Version 4.0

OFFICE of information technology services

Information Security Policy Manual

Security and Privacy Policies for Information Systems, ITS, and Supported Agencies'

its.idaho.gov

Integrity • Teamwork • Service

ITS members embody the core values of integrity, teamwork, and service. Here are ways those values are expressed in our conduct…

Integrity

Being honest – with ourselves and others. Doing what is right – especially when it's hard or unpopular. Making tough decisions. Being a good steward of the time and money entrusted to us. Taking responsibility. Holding ourselves and our teams to high standards. Doing what we say we will do. Giving every task its due attention.

Teamwork

Recognizing others as important and valuing what they contribute. Being respectful. Lending a hand. Avoiding gossip. Filling in gaps to serve our customers. Seeing individual contributions as part of a whole. Being flexible and open minded. Taking criticism as an opportunity to improve. Reaching out to other teams, other divisions, and other agencies to do good things.

Service

Being part of something bigger. Recognizing Idaho citizens as the ultimate customer. Earning their trust. Maintaining a positive attitude. Improving our systems, our processes, our people, and ourselves. Putting requirements above preferences. Treating others with courtesy, dignity, and respect.

ITS' Mission

We connect citizens with their government.

ITS Chief Information Security Officer's Mission

To protect Idaho's cyber infrastructure through standardized best practices, strategic partnerships, and collective defense.

Intent

The intent of this manual is to establish policies that fully comply with the most recent revision of various contractual and regulatory requirements.

This manual contains policies for the Idaho Office of Information Technology Services (ITS) and supported customers with respect to the security of our electronic information and supported information systems. The purpose of this document is to set forth expectations of practice and behavior to protect all state data and information technology infrastructure. Executive Leadership has approved the enclosed policies and standards and is fully committed to their enforcement. ITS leadership will ensure all ITS staff will follow these policies and standards. Some aspects of this manual are still under review and development and are subject to change.

The ITS Chief Information Security Officer (CISO) disseminates this manual to facilitate a review of the included policies and standards by the ITS Executive Leadership, at least annually.

All policies contained herein apply to anyone working on behalf of ITS including, but not limited to, employees, officers, agents, contractors, consultants, vendors, interns, or any other person performing work for ITS or for any individual, partnership, corporation, or other entity providing goods or services to ITS that will have access to the electronic information and supported information systems of ITS. No exceptions to these policies are permitted unless approved by the ITS Administrator. Any questions related to this document should be directed to your manager or the ITS CISO.

ITS' supported information systems, whether owned or contracted, will be configured to meet the requirements set forth in these policies. Agreements that involve a third party accessing or managing ITS supported information systems must comply with all the requirements specified in these policies.

Administrator Name	ALBERTO GONZALEZ
Administrator Signature	
Date	7/11/2025

Table of Contents

BLANK

Acknowledgements

In preparing “ITS Information Security Policy Manual v 3.0” I wish to acknowledge my indebtedness to the wholehearted cooperation, guidance, constructive suggestions, and encouragement of my two colleagues Matt Aslett and Sam Montiel.

Sincerest thanks are also due to Executive Leadership for trusting in my abilities and allowing me the space to make this manual what it is.

Elizabeth Knox
Policy and Programs Officer

ITS CISO GRC

Matt Aslett
Chief Compliance Officer

Terry Conway
Compliance Officer

Executive Leadership

Alberto Gonzalez
Administrator / Chief Information Officer

Jason Pierce
Deputy Administrator / Chief Information Officer

Jerred Edgar
Chief Information Security Officer

About this Policy Manual

Overview

The Information Technology Services (ITS) Information Security Policy Manual provides definitive information on the prescribed measures used to establish and enforce the cybersecurity program at ITS.

ITS is committed to protecting its employees, partners, customers, and ITS from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every vendor that interacts with State Data and/or supported information systems. Therefore, it is the responsibility of all personnel to be aware of and adhere to ITS' cybersecurity requirements.

Protecting State Data and supported information systems (system/s) that collect, process, and maintain this data is of critical importance. To reduce risk, security and privacy measures must be implemented to guard against unauthorized access, alteration, disclosure, or destruction of data and supported information systems. This includes protection against accidental loss or destruction. Therefore, the security of supported information systems must include policies and safeguards to offset threats, as well as policies to ensure the confidentiality, availability, integrity, and safety:

CONFIDENTIALITY – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.

INTEGRITY – Integrity addresses the concern that State Data has not been modified or deleted in an unauthorized and undetected manner.

AVAILABILITY – Availability addresses ensuring timely and reliable access to and use of information.

SAFETY – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

Purpose

The purpose of the ITS Information Security Policy Manual is to prescribe a comprehensive framework for:

- ✓ Creating a NIST based Information Security Management System
- ✓ Protecting the confidentiality, integrity, and availability of Idaho data and supported information systems
- ✓ Protecting ITS, its employees, and customers from illicit use of State Data and supported information systems
- ✓ Ensuring the effectiveness of security policies over Idaho data and supported information systems that support ITS' operations
- ✓ Recognizing the highly networked nature of the current computing environment and provide effective agency-wide management and oversight of those related cybersecurity risks
- ✓ Providing for the development, review, and maintenance of minimum-security policies required to protect ITS' data and supported information systems

The formation of this information security manual is driven by many factors, with the key factor being risk. These policies set ground rules under which ITS operates and safeguards Idaho data and supported information systems to both reduce risk and minimize the effect of potential incidents.

The policies in this document, including their related standards, procedures, and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides

due care to ensure ITS users understand their day-to-day cybersecurity responsibilities and the threats that could impact ITS.

Implementing consistent security policies across the agency will help ITS comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity, and availability of State Data.

Scope and Applicability

The policies in this manual apply to all State Data, supported information systems, activities, and assets owned, leased, controlled, or used by ITS, its agents, contractors, or other business partners on behalf of ITS. These policies apply to all ITS employees, contractors, sub-contractors, and their respective facilities supporting ITS business operations, wherever State Data is stored or processed, including any third-party contracted by ITS to handle, process, transmit, store, or dispose of State Data.

Some policies apply specifically to persons with a specific job function/role (e.g., a System Administrator); otherwise, all personnel supporting ITS business functions must comply with the policies.

Cybersecurity Roles and Responsibilities provides a description of ITS user roles and responsibilities, in regard to cybersecurity.

These policies do not supersede any other applicable law or stricter agency directive or existing labor management agreement in effect as of the effective date of this policy.

ITS reserves the right to revoke, change, or supplement these policies at any time without prior notice. Such changes must be effective immediately upon approval by management, unless otherwise stated.

Policy Overview

To ensure an acceptable level of cybersecurity risk, ITS is required to design, implement, and maintain a coherent set of policies, standards, procedures, and guidelines to manage risks to State Data and supported information systems.

ITS users are required to protect and ensure the Confidentiality, Integrity, and Availability of State Data and supported information systems, regardless of how data is created, distributed, or stored.

- Security policies will be tailored accordingly so that cost-effective policies can be applied commensurate with the risk and sensitivity of the data and supported information system
- Security policies must be designed and maintained to ensure compliance with all legal requirements

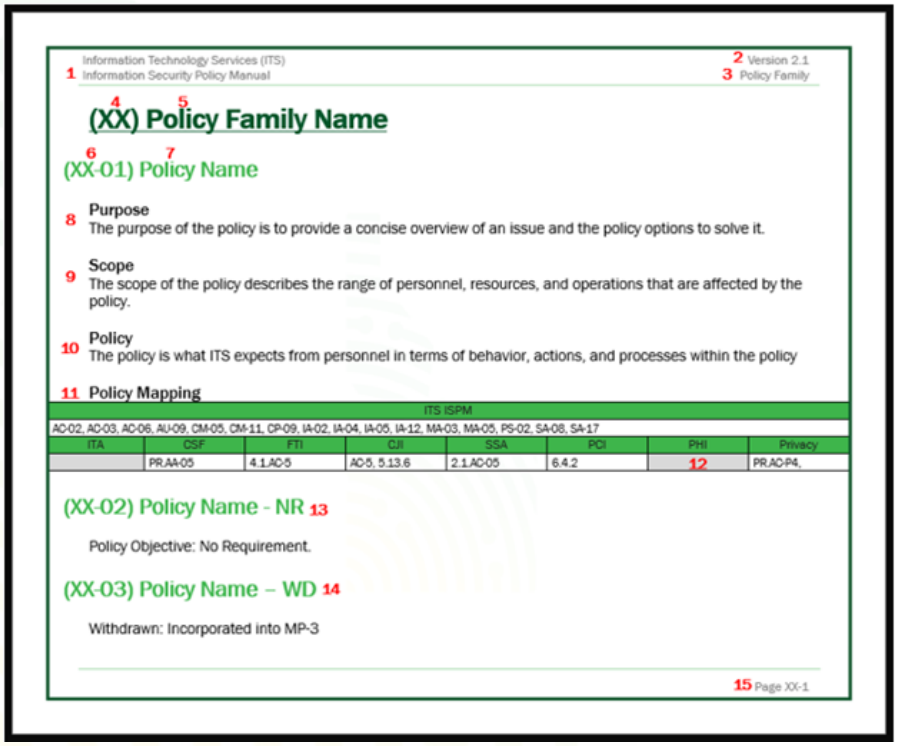
Security and privacy policies in this manual have a well-defined organization and structure. Policies are organized into twenty (20) control/policy families. The control/policy families are defined by NIST SP 800-53 r5. A two-character identifier uniquely identifies each control/policy family (e.g., PS for Personnel Security). Each family contains policies that are related to the specific title of the family. Security and privacy policies may involve aspects of policy, oversight, supervision, manual processes, and automated mechanisms that are implemented by supported information systems or actions by individuals. Table 1 lists the security and privacy policies families and their associated family identifiers.

Table 1 Security and Privacy Policy Families

ID	Family	ID	Family
AC	Access Control	PL	Planning
AT	Awareness and Training	PM	Program Management
AU	Audit and Accountability	PS	Personnel Security
CA	Assessment, Authorization, Monitoring	PT	PII Processing and Transparency
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Service Acquisition
IA	Identification and Authentication	SC	System and Communication Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	SR	Supply Chain Risk Management
MP	Media Protection	ITS.P	ITS Policies
PE	Physical and Environmental Protections	S	ITS Standards

Figure 1 Policy Structure

1. Name of manual
2. Version number
3. Name of policy family
4. Family identifier
5. Policy family name
6. Policy identifier
7. Policy name
8. Policy purpose
9. Who/what policy applies to
10. What ITS must do
11. Compliance mapping
12. Cell that are gray = no requirements
13. No requirement
14. Withdrawn
15. Page number with family identifier



Policy Mapping Guide

ITS ISPM	ITS Information Security Policy Manual 3.0
ITA	Idaho Technology Authority - Policies/Standards/Guidelines
CSF	NIST Cybersecurity Framework
FTI	IRS Publication 1075
CJI	FBI Criminal Justice Information Services Security Policy
SSA	Social Security Administration Technical System Security Requirements
PCI	Payment Card Industry Data Security Standard
PHI	Implementing the Health Insurance Portability and Accountability Act Security Rule
Privacy	NIST Privacy Framework

Violations

Any ITS user found to have violated any policy, standard, or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Additional information can be found in Enforcement and Penalties.

Updates

- **Announcement of Updates**: Updates to the ITS Information Security Policy Manual will be communicated to employees via management updates or Communications.
- **Record of Changes**: All changes/updates to the manual will be documented in the Record of Changes to highlight the pertinent changes from the previous policies and standards.
- **Administrative Changes**: Minor, non-substantive changes (such as formatting or grammatical corrections) can be made without requiring executive approval. These changes are indicated by a *minor version increment* (e.g., "Version 1.0 to 1.1").
- **Major Changes**: Significant changes, such as revisions to core policies or standards, require executive approval and are reflected by a *major version increment* (e.g., "Version 1.0 to 2.0").

Policy Manual Assistance

If you find an error, have questions, or there is a policy that may cause operational challenges, please screenshot issue within the manual and email to GRC@its.idaho.gov with ISPM in the subject line.

Cybersecurity Roles and Responsibilities

The defined roles and responsibilities below are the general requirements for cybersecurity policies within ITS. There may be slight differences between this list and what is documented within an agency's SLA with ITS. If this occurs, the SLA will have precedence over this document. The roles and responsibilities include, but are not limited to:

Role	Responsibilities	Policies
3rd Party	• The third party must exercise care, skill, and diligence when handling information or supported information systems from the principal or the agencies that fall within scope • The third party must take all steps to protect the principal's interests regarding the organization, reputation, and security of the entrusted information and information systems • The third party must not place their duties as an agent in conflict with their own interests and the interests or mission of the organization and agencies	PS-07, P.ITS-01
ITS	• Establish policies and procedures for managing the assignment of classification levels within the agency • Ensure that information belonging to different classification levels be logically separated or protected at the highest impact level of the systems associated information • If using another agency's information or information assets, observe and maintain the appropriate security for the classification levels assigned by other agency's information owner • Provide training to information owners and information handlers on this policy and handling procedures associated with all information classification levels	XX-1, AC-05, AC-06, AC-14, AC-19, AC-20, AT-02, AT-03, AU-02, AU-09, CA-08, CA-09, CM-02, CM-012, CP-03, CP-04, CP-06, CP-07, IA-03, IA-08, IA-12, MA-02, MP-02, MP-04, MP-05, MP-06, MP-07, PE-02, PE-03, PE-04, PE-05, PE-06, PE-08, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-17, PM-04, PS-07, PS-08, PS-09, PT-02, RA-02, SA-09, SC-07, P.ITS-01, S.PE-02, S.PE-03, S.PL-01d, S.PS-03
All State personnel	• Follow policies as outlined in this manual • Reading and signing the ITS Rules of Behavior and Non-disclosure agreement	AC-02, AC-03, AC-19, AT-02, AT-03, AT-04, CM-12, CM-13, CP-03, IA-11, IR-02, IR-06, MP-03, MP-04, MP-05, MP-06, PE-02, PE-03, PE-04, PE-05, PL-02, PL-04, PS-06, SI-12, P.ITS-01, S.PL-01, S.PS-02
Application Development (AppDev)	• Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices	AC-03, SA-03, SA-10, SA-11, SA-15, SC-08, SC-18, SI-10, SI-11
Business Operations (BusOps)	• Collaborating with relevant parties to create a budget • Overseeing money handling, accounting, and bank processes • Employing means to control company costs • Generating financial reports	CM-08, PM-05, SA-03, SA-04, SR-02, SR-03, SR-06, SR-09, SR-10, SR-11,
Configuration Control Board (CCB)	• Ensuring security is considered when changes to ITS networks • Offers multiple perspectives necessary to ensure proper decision-making • Reviewing and prioritizing requested changes, monitoring the change process, and providing managerial feedback • Covers all changes related to the service lifecycle, including emergency changes	CM-03

Role	Responsibilities	Policies
Chief Compliance Officer (CCO)	• Oversees the State of Idaho's Compliance Program, functioning as an independent and objective body that reviews and evaluates compliance issues/concerns within the State • Ensures agencies, management, and employees follow the rules and regulations of regulatory agencies, that agency policies and procedures are being followed, and that behavior in the agencies meets the company's Rules of Behavior	AU-16, CA-02, PM-08
Chief Information Officer (CIO)	• Accountable for the effective implementation of IT management responsibilities • Strategic planning for all IT management functions • Assessing agency IT workforce needs and developing strategies and plans for meeting those needs	CA-06, CP-02, MA-02, PM-23
Chief Information Security Officer (CISO)	• Ensuring that the ITS Security Program is communicated and understood by all users accessing ITS supported information systems • Overseeing personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained • Incident response reporting / issues Point of Contact (POC) • Policies and Procedures • Security awareness • Risk, Vulnerability, and testing coordination • Participate in coordinator forums and training	XX-1, AC-02, AC-17, AC-19, AC-21, AT-02, AT-06, CA-02, CA-03, CA-05, CA-06, CA-07, CM-03, CM-06, CM-09, CP-04, IR-02, IR-03, IR-04, IR-05, IR-06, IR-07, IR-08, MA-03, MA-05, PL-02, PL-04, PL-08, PL-09, PM-03, PM-06, PM-08, PM-09, PM-10, PM-11, PM-13, PM-14, PM-15, PM-16, PM-21, PM-23, PS-07, PS-09, RA-02, RA-05, RA-09, SA-02, SA-08, SA-09, SA-10, SC-04, SC-35, SI-04, SI-05, SI-11, SI-12, SR-02, SR-03,
Chief Operating Officer (COO)	• Contribute operations information and recommendations to strategic plans and reviews; prepare and complete action plans; implement production, productivity, quality, and customer-service standards; resolve problems; complete audits; identify trends • Define the way ITS manages software and hardware	CM-09, CM-11, CP-02, CP-08, CP-09, CP-10, IA-04, MA-06, PL-04, PL-10, PL-11, PM-08, PM-10, PM-11, PM-23, PS-06, SC-04
Chief Technology Officer (CTO)	• Define and execute the agency's tech vision and align it with business goals • Manage and guide the technology team to foster innovation and productivity • Oversee the creation of scalable, secure, and innovative products or services • Ensure reliable, secure, and scalable tech infrastructure and data protection • Report tech progress and risks to executives and key stakeholders	CM-03, CM-10, PL-02, PL-08, PM-03, PM-05, PM-07, PM-08, SA-02, SA-03, SA-04, SA-05, SA-08, SA-09, SA-15, SA-22, SR-02, SR-03, SR-06, SR-09, SR-10, SR-11
Computer Security Incident Response Team (CSIRT)	• Detecting and taking immediate action upon incidents • Training to give the appropriate responses for new threats • Informing related departments about new technologies, policies, and changes in protocols after security incidents • Maintaining internal communications and supervising operations during and after significant incidents • Creating and updating the incident response plan (IRP)	IR-03, IR-04, IR-05, IR-06, IR-07, IR-08, IR-09, SI-04, SI-05
Communications Manager	• Developing communication strategies • Overseeing internal and external communications • Ensuring consistent messaging • Managing media relations and social media presence	AC-22, PM-20, PM-27

Role	Responsibilities	Policies
Database Administrators (DBA)	• Perform tests and evaluations regularly to ensure data security, privacy, and integrity	SC-28
Enterprise Architect (EA)	• Align IT strategies with agency goals and develop long-term roadmaps • Define enterprise architecture standards and ensure governance • Evaluate and integrate appropriate technologies across systems • Work with business and IT teams to align technology with needs • Identify IT risks and ensure systems meet regulatory standards	SA-03, SA-04, SA-05, SA-08, SA-15, SA-22, CM-10, PL-02, PL-08, PM-07, SR-02, SR-03, SR-06,
Executive Leadership Team (ELT)	• Establishes ITS requirements • Assigns senior individuals to necessary roles	AT-06, CA-07, PM-02, PM-19, PM-27, PM-29, S.PS-03
Facilities	• Any physical location where personnel perform work on the behalf of ITS without regard to the ownership of the physical property. This term includes alternate sites where ITS has approved for the personnel to work (e.g., a private residence).	PE-02, PE-03, PE-04, PE-05, PE-06, PE-08, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16
Governance, Risk and Compliance (GRC)	• Governance: Set rules and make sure teams follow them • Risk: Spot problems early and plan how to handle them • Compliance: Make sure agencies follows laws and standards	XX-01, PM-23
Hosting Team (Hosting)	• Application and Middleware Management • Support for websites and client/server applications	IA-09, SC-03, SC-08,
Human Resources (HR)	• Recruitment of candidates • Training and development • Policies of the workplace • Performance reviews and promotion of the employee	AT-02, AT-03, AT-04, IA-12, PL-04, PS-02, PS-03, PS-04, PS-08, PS-09, P.ITS-02
Infrastructure Team	• Plan, organize and coordinate the activities of the computer infrastructure department • Ensure that all computer networks, supported information systems, and servers are all up and running • Ensue that the IT infrastructure runs smoothly by scheduling repair work when necessary • Develop new computer infrastructures if needed through conducting feasibility studies and making plans	AC-02, AC-03, AC-04, AC-07, AC-17, AU-04, AU-08, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, IA-02, IA-04, IA-05, MP-07, SC-03, SC-10, SC-12, SC-13, SC-17, SC-20, SC-21, SC-22, SC-28, SC-32, SC-39, SC-45, SI-02, SI-07, SI-16,
ITS Management	• Ensuring that personnel under their direct report complete all required IT security training and activities, including privacy and role-based training within the mandated time limit	AC-04, AC-05, AC-06, AC-19, AU-06, CM-05, IR-08, MP-02, PE-02, PE-04, PE-17, PS-02, PS-03, PS-04, PS-05, PS-08, PS-09, SA-15,
Network Operations (NetOps)	• Responsible for network infrastructure configuration design, implementation, maintenance, evaluation, and testing, change processes, and security • Firewall management	AC-04, AC-18, AU-03, AU-09, CM-08, SC-03, SC-05, SC-07, SC-10, SC-32, SC-40,
Policy Officer	• Performing analysis and research for policies • Monitoring, managing, and inspecting the implementation of policies	CA-02, PL-09,
Privacy Manager	• Develop and maintain an accurate accounting of disclosures • Monitor PII disclosures • Review latest privacy laws and how they affect ITS • Identifying and assessing risks that may affect the confidentiality of protected information • Establish and lead a privacy program for ITS consistent with applicable laws • Serve as the information privacy liaison for users of technology systems	PM-18, PM-20, PM-21, PM-23, PM-26, PM-27, PT-02, PT-03, PT-05, PT-07, RA-02, RA-08,

Role	Responsibilities	Policies
Risk Officer	• Evaluating potential risk to ITS • Conducts risk assessments, collecting and analyzing documentation, statistics, reports, and market trends • Design processes to eliminate or mitigate potential risks • Quantitatively and qualitatively assessing risks to prioritize management strategies • Recommends and implements risk management solutions • Drafts and presents risk reports and proposals to executive leadership	PM-09, PM-29, PS-02, RA-03, RA-07, SA-09,
Security Operations (SecOps)	• Maintain the ongoing security posture of an organization. It consists of the monitoring, maintenance, and management of the security aspects of the IT estate, its people, and its processes • Patching vulnerable systems • Develop and enforce security policies, standards, and procedures necessary for safeguarding state data	AC-17, AC-19, AC-23, AU-02, AU-03, AU-05, AU-06, AU-07, AU-09, AU-10, AU-11, AU-12, AU-13, CM-08, IA-07, MA-04, MP-07, RA-05, SC-03, SC-05, SC-07, SC-08, SC-10, SI-03, SI-04, SI-07, SI-08, SI-11, SI-16, SR-09, SR-10, SR-11,
Service Desk	• Identify and diagnose issues and problems • Categorize and record reported queries and provide solutions • Advise users on appropriate course of action • Escalate, if needed, unresolved problems to a higher level of support • Account creation	AC-02, IA-02, IR-06, PM-05, PS-04, PS-05, SC-06, SA-02, S.SC-01
System Administrator (SysAdmin)	• Install and update hardware and software • Maintain and configure network servers and computer supported information systems • Integrate automation procedures and processes • Run diagnostics and troubleshoot errors • Lead service desk efforts • Provide training and documentation to staff regarding new IT infrastructure	AU-02, AU-05, AU-09, SA-10, SA-11, SC-03, SC-32, SI-03,
Threat Hunter Team (THT)	• Search for cyber threats and risks hiding inside the data before attacks occur • Gather as much information on threat behavior, goals, and methods as possible • Organize and analyze the collected data to determine trends in the security environment of the organization • Make predictions for the future and eliminate the current vulnerabilities	AC-02, AC-23, PM-12, RA-10, SI-10, SR-09, SR-10, SR-11,
Unified Endpoint Management (UEM)	• Unified Endpoint Management • Responsible for management of all end user computing devices. Laptops, Desktops, Tablets, Mobile Phones, Etc. • Responsible for Image creation and application deployment packages	SC-06, SC-15, SI-02, S.SC-01,
VoIP Team	• Troubleshooting VoIP network issues • Collaborate with BusOps for port orders and E911 management for VoIP site • Complete VoIP SAR requests (Add, Remove Users, Devices and Directory Numbers) • Manage and update Call Flow to match the Business needs of the customer	SC-15

ITS Information Security Policies

(AC) Access Control Family

(AC-01) Access Control Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish and enforce access control policies and procedures to regulate permissions, protect sensitive resources, and mitigate security risks associated with unauthorized access or privilege misuse.

Scope
The policy applies to the Chief Information Security Officer (CISO), Cyber Governance Team (CGT), agencies with a low, moderate, or high baseline, and all access control policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the access control policy and procedures. The CISO along with CGT must:

(a) Develop, document, and disseminate to State personnel with access control responsibilities:
   1. An State level access control policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the access control policies and the associated access control family policies

(b) Review and update the current access control:
   1. Policies annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data
   2. Procedures annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data

Policy Mapping

ITS ISPM							
IA-01, PM-09, PM-24, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03, PR.AA-01, PR.AA-05	4.1.AC-1	AC-1	2.1.AC-01	8.1, 8.4	164.312(a)(a)	PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CT.PO-P2, CT.PO-P3, PR.AC-P3, PR.AC-P4

(AC-02) Account Management

Purpose
The purpose of the policy is to ensure organizations manage user accounts effectively, including creation, modification, and termination, to prevent unauthorized access.

Scope

The policy applies to the Service Desk, Chief Information Security Officer (CISO), Infrastructure Team, ITS Managers, and ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy restricts personnel access to data and systems appropriate to their duties and responsibilities. The CISO and Service Desk are responsible for ensuring proper user identification and authentication management for all standard and privileged users on all systems. The CISO and Service Desk must:

(a) Define and document the types of accounts allowed and specifically prohibited for use within the System; see (S.AC-03) ITS User Accounts
(b) Assign account managers
(c) Require conditions for group and role membership
(d) Specify:
    1. Authorized users of the System
    2. Group and role membership
    3. Access authorizations (i.e., privileges) and other attributes (as required) for each account
(e) Require approvals by the System owner or designated representative for requests to create accounts
(f) Create, enable, modify, disable, and remove accounts in accordance with ITS policy
(g) Monitor the use of accounts
(h) Notify account managers and designated agency officials within one (1) day when:
    1. Accounts are no longer required
    2. Users are terminated or transferred
    3. System usage or need-to-know changes for an individual
(i) Authorize access to the System based on:
    1. A valid access authorization
    2. Intended System usage
    3. Under the authority to re-disclosed FTI under the provisions of IRC § 6103
(j) Review accounts for compliance with account management requirements:
    1. Annually for standard user accounts
    2. Semi-annually for privileged accounts
(k) Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group
(l) Align account management processes with personnel termination and transfer processes
(m) *Automated System Account Management*: Support the management of system accounts using automated mechanisms
(n) *Automated Temporary and Emergency Account Management*: Automatically disable and remove temporary and emergency accounts within two (2) business days
(o) *Disable accounts* within one (1) week when the account:
    1. Has expired
    2. Is no longer associated with a user or individual
    3. Is in violation of ITS policy
    4. Has been inactive for:
        i. Ninety (90) days for non-privileged accounts
        ii. Sixty (60) days for privileged accounts
    5. Delete accounts within ninety (90) days after accounts have been disabled
(p) *Automated Audit Actions*: Automatically audit account creation, modification, enabling, disabling and removal actions
(q) *Inactivity Logout*: Require users to log out when users expect inactivity longer than four (4) hours
(r) *Privileged User Accounts*:
    1. Establish and administer privileged user accounts in accordance with a role-based access scheme; an attribute-based access scheme
    2. Monitor privileged role or attribute assignments
    3. Monitor changes to roles or attributes
    4. Revoke access when privileged role or attribute assignments are no longer appropriate

(s) *Restrictions on use of Shared and Group Accounts*: Only permit the use of shared and group accounts that meet ITS-defined conditions for establishing shared and group accounts

(t) *Account Monitoring for Atypical Usage*:

1. Monitor System accounts for ITS-defined atypical usage
2. Report atypical usage of System accounts to ITS Threat Hunter Team

(u) *Disable Accounts for High-Risk Individuals*: Disable accounts of users within thirty (30) minutes but no later than one (1) day of discovery of direct threats to the confidentiality, integrity, or availability of State Data

Policy Mapping

ITS ISPM							
AC-03, AC-05, AC-06, AC-17, AC-18, AC-20, AC-24, AU-02, AU-12, CM-05, IA-02, IA-04, IA-05, IA-08, MA-03, MA-05, PE-02, PL-04, PS-02, PS-04, PS-05, PS-07, PT-02, PT-03, SC-7, SC-12, SC-13, SC-27, S.AC-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4502, P4590, S6010	PR.AA-01, PR.AA-05, PR.DS-10, DE.CM-01, DE.CM-03	4.1.AC-2	AC-2	2.1.AC-02	8.1.3-8.1.5, 8.2.2, 8.2.6, 8.5, 8.5.1, 8.6, 8.7,	164.312(d), 164.312(a)(2)(iii), 164.308(a)(4(ii)(A) and (B) and (C)	CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4

(AC-03) Access Enforcement

Purpose

The purpose of the policy is to ensure organizations enforce access control policies to restrict system access based on predefined authorization rules.

Scope

The policy applies to the Infrastructure Team, Application Development (AppDev), all State personnel and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the Infrastructure Team and all Systems where State Data is Handled to:

(a) Enforce approved authorizations for logical access to State Data and System resources in accordance with applicable access control policies

(b) Limit access to Systems and State Data to only those individuals whose job requires such access

(c) On custom-developed applications and web pages, AppDev is required to enforce rules to require inputs to be prescreened to prevent the content from being unintentionally interpreted as commands

(d) Enforce a role-based access control over defined subjects and objects and access based upon the need to utilize State Data

(e) Enforce a role-based access control over users and Systems that have access to State Data, and control access based upon ITS

(f) *Release Data Outside of the System Only if*:

1. The receiving System handling State Data meets the requirements within the ITS Information Security Policy Manual
2. ITS-defined controls, ITS Information Security Manual, FedRAMP ATO are used to validate the appropriateness of the information designated for release

(g) *Restrict Access to Specific Information Types:* Restrict access to data repositories containing State Data

(h) *Individual Access*: Provide automated or manual processes to enable individuals to have access to elements of their PII

(i) *IRS-Defined*: Users having accounts with administrator access privileges may access those accounts only from ITS owned or authorized Systems

Policy Mapping

ITS ISPM							
AC-02, AC-04, AC-05, AC-06, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-02, AT-03, AU-09, CA-09, CM-05, CM-11, IA-02, IA-05, IA-06, IA-07, IA-11, MA-03, MA-04, MA-05, MP-04, PM-02, PS-03, PT-02, PT-03, SA-17, SC-02, SC-03, SC-04, SC-12, SC-13, SC-28, SC-31, SC-34, SI-04, SI-08.							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1030	PR.AA-05, PR.DS-10, PR.IR-01	4.1.AC-3	AC-3	2.1.AC-03	7.1, 7.1.1-7.1.4, 7.2, 7.2.1, 7.2.3	164.308(a)(4(i) and (ii)	PB, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2

(AC-04) Information Flow Enforcement

Purpose
The purpose of the policy is to ensure organizations regulate the flow of information within and between systems to prevent unauthorized data transmission.

Scope
The policy applies to Network Operations (NetOps), Infrastructure Team, ITS Management, and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires NetOps, Infrastructure Team, and the System to enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing State Data from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from the agency-controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers).

Policy Mapping

ITS ISPM							
AC-03, AC-06, AC-16, AC-17, AC-19, AC-21, AU-10, CA-03, CA-09, CM-07, PL-09, PM-24, SA-17, SC-04, SC-07, SC-16, SC-31							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4501, P4570	ID.AM-03, PR.DS-10, PR.IR-01, DE.CM-09	4.1.AC-4	AC-4, 5.10.1		1.1.3, 1.1.6, 1.1.7, 1.3.1, - 1.3.7		CT.DM-P2, PR.AC-P5, PR.DS-P5

(AC-05) Separation of Duties

Purpose
The purpose of the policy is to ensure organizations implement role-based access restrictions to minimize conflicts of interest and reduce security risks.

Scope
The policy applies to ITS Management and State personnel with authorized access to ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires ITS Management in locations that Handle State Data to:

(a) Identify and document separate duties of individuals to prevent malevolent activity without collusion
(b) Define System access authorizations to support separation of duties

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-06, AU-09, CM-05, CM-11, CP-09, IA-02, IA-04, IA-05, IA-12, MA-03, MA-05, PS-02, SA-08, SA-17							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-05	4.1.AC-5	AC-5, 5.13.6	2.1.AC-05	6.4.2		PR.AC-P4, PR.DS-P5

(AC-06) Least Privilege

Purpose

The purpose of the policy is to ensure organizations grant users only the minimum necessary access to perform their job functions.

Scope

The policy applies to ITS Management and State personnel with authorized access to ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires ITS to:

(a) Employ the "principle of least privilege," allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned agency tasks

(b) *Authorize Access to Security Functions*: Authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions to:

1. Explicitly authorize access to security functions deployed in hardware, software, and firmware
2. Security-relevant information in hardware, software, and firmware

(c) *Non-Privileged Access for Non-Security Functions*: Require users of system accounts (or roles) with access to security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions

(d) *Privileged Accounts*: Restrict privileged accounts on the system to privileged users

(e) Privileged Access by Non-Organizational Users: Prohibit privileged access to the System by non-agency users

(f) *Review of User Privileges*:

1. Annually the privileges assigned to ITS-Defined roles or classes of users to validate the need for such privileges
2. Reassign or remove privileges, if necessary, to correctly reflect ITS' mission/business needs

(g) *Privileged Levels for Code Execution*: Prevent the following software from executing at higher privilege levels than users executing the software: ITS-defined software (This should be tracked in the agency's POAM)

(h) *Log Use of Privileged Functions*: Log the execution of privileged functions

(i) *Prohibit Non-Privileged Users from Executing Privileged Function*: Prevent non-privileged users from executing privileged functions

(j) *IRS-Defined*: Prohibit accounts with administrative privileges (including local administrator rights) from web browsing and other internet connections outside of the local protected boundary unless such risk is accepted in writing by the agency's CISO

(k) *IRS-Defined*: Block accounts with administrative privileges (including local administrator rights) from access to email unless such risk is accepted in writing by the agency's CISO

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-05, AC-16, CM-05, CM-11, PL-02, PM-12, SA-08, SA-15, SA-17, SC-38							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy

P4501, P4502	PR.AA-05	4.1.AC-6	AC-6, 5.13.6	2.1.AC-06	7.1, 7.1.2,		PR.AC-P4, PR.DS-P5

(AC-07) Unsuccessful Logon Attempts

Purpose
The purpose of the policy is to ensure organizations monitor and limit failed login attempts to mitigate unauthorized access risks.

Scope
The policy applies to the Infrastructure Team and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled) that enforce authentication.

Policy
ITS policy requires the Infrastructure Team to:

(a) Enforce a limit of three (3) consecutive invalid logon attempts by a user during a 120-minute period

(b) Automatically lock the account for fifteen (15) minutes; or until released by an administrator; delays next logon prompt when the maximum number of unsuccessful attempts is exceeded

(c) *Purge or Wipe Mobile Devices*: Purge or wipe information from mobile devices based on agency-defined purging or wiping requirements and techniques after ten (10) consecutive, unsuccessful device login attempts:

1. ITS owned devices – ALL data will be purged regardless of who's data is on the device
2. Personally owned devices – Every attempt will be made to purge only State Data

Policy Mapping

ITS ISPM							
AC-02, AC-09, AU-02, AU-06, IA-05							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4550, S2140, G540	PR.AA-03	4.1.AC-7	AC-7	2.1.AC-07	8.3.4		

(AC-08) System Use Notification

Purpose
The purpose of the policy is to ensure organizations provide system use notifications to inform users of security policies and monitoring practices.

Scope
The policy applies to all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires System use notifications to be presented to users. Systems that contain State Data must:

(a) Display a warning banner to users before granting access to the System that provides privacy and security notices consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance and states that:

1. Users are accessing a U.S. Government System
2. System usage may be monitored, recorded, and subject to audit
3. Unauthorized use of the System is prohibited and subject to criminal and civil penalties
4. Use of the System indicates consent to monitoring and recording

(b) Retain the warning banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the System

(c) For publicly accessible Systems:
1. Display System use information warning banner before granting further access to the publicly accessible system
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such Systems that generally prohibit those activities
3. Include a description of the authorized uses of the System

(d) *IRS-defined*: The warning banner must be applied at the application, database, operating system, and network device levels for all systems that receive, process, store, or transmit FTI

For sample warning banners see (S.AC-01) System Use Notification

Policy Mapping

ITS ISPM							
AC-14, PL-04, SI-04, S.AC-01							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.1.AC-8	AC-8	2.1.AC-08			CM.AW-P1

(AC-09) Previous Logon Notification – NR

Policy Objective: No Requirement.

(AC-10) Concurrent Session Control – NR

Policy Objective: No Requirement.

Policy Mapping

ITS ISPM							
SC-23							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-05						PR.AC-P5

(AC-11) Device Lock

Purpose
The purpose of the policy is to ensure organizations automatically lock inactive sessions to protect sensitive information from unauthorized viewing.

Scope
The policy applies to all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires:

(a) Systems to prevent further access to the System by initiating a device lock after fifteen (15) minutes of inactivity; requiring the user to initiate a device lock before leaving the System unattended

(b) Systems to retain the device lock until the user re-establishes access using established identification and authentication procedures

(c) *Pattern-Hiding Displays*: Systems to conceal, via the device lock, information previously visible on the display with a publicly viewable image

(d) Users to lock their system when they stop working and move away from the immediate vicinity of the system

Policy Mapping

ITS ISPM							
AC-02, AC-07, IA-11, PL-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.1.AC-11	5.5.AC-11	2.1.AC-11	8.1.8		

(AC-12) Session Termination

Purpose
The purpose of the policy is to ensure organizations enforce automatic session termination after a defined period of inactivity to reduce security risks.

Scope
The policy applies to logical sessions on supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires Systems to be configured to:

(a) Automatically terminate a user session after thirty (30) minutes of inactivity

(b) *User-Initiated Logouts*: Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to Systems that Handle State Data

Policy Mapping

ITS ISPM							
SC-10, SC-23							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-03	4.1.AC-12	5.5.AC-12		8.1.8, 12.3.8	164.312(a)(b)(iii)	PR.PT-P3

(AC-13) Supervision and Review – Access Control – WD

Withdrawn: Incorporated into AC-02 and AU-06

(AC-14) Permitted Actions w/o Identification or Authentication

Purpose
The purpose of the policy is to ensure organizations define and restrict system actions that can be performed without authentication.

Scope
The policy applies to all ITS supported information systems (System/s) in which it has been determined that no identification or authentication is required.

Policy
ITS policy prohibits System configurations that do not require identification or authentication, without a documented and justifiable business requirement. When situations arise in which ITS determines that no identification or authentication is required ITS must:

(a) Identify specific user actions that can be performed on the System without identification or authentication

(b) Document and provide supporting rationale in the security plan, IRS SSR (or other requirement) for the System, user actions not requiring identification and authentication

Policy Mapping

ITS ISPM							
AC-08, IA-02, PL-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-01	4.1.AC-14	5.5.AC-14				PR.AC-P4, PR.AC-P6

(AC-15) Automated Marking – WD

Withdrawn: Incorporated into MP-03

(AC-16) Security and Privacy Attributes – NR

Policy Objective: No Requirement.

(AC-17) Remote Access

Purpose

The purpose of the policy is to ensure organizations regulate remote access to systems to prevent unauthorized external connections.

Scope

The policy applies to the Chief Information Security Officer (CISO), Security Operations (SecOps), Infrastructure Team, and the access of data classified as Level 2 and higher (State Data) or supported information systems (System/s) by personnel (or processes acting on behalf of personnel) via non-ITS controlled networks regardless of method (e.g., dial-up, broadband, and wireless). The policy does not apply to resources designed for public access such as web servers.

Policy

ITS policy assigns responsibility to CISO, Infrastructure Team, and SecOps for:

(a) Establishing and documenting usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed

(b) Authorizing each type of remote access to the System prior to allowing such connections

(c) *Monitoring and Control*: Employing automated mechanisms to monitor and control remote access methods

(d) *Protection of Confidentiality and Integrity Using Encryption*: Implementing cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions

(e) *Managed Access Control Points*: Routing remote access through authorized and managed network access control points

(f) *Privileged Commands and Access*:

1. Authorizing the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for compelling operational needs
2. Documenting the rationale for remote access in the security plan for the System

(g) *Disconnect or Disable Access*: Providing the capability to disconnect or disable remote access to the System within fifteen (15) minutes

(h) Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. Sessions must be monitored at all times by an authorized escort
2. Escorts must be familiar with the System/area in which the work is being performed
3. Escorts must have the ability to end the session at any time
4. Remote administrative personnel connections must be via an encrypted (FIPS 140-2 certified) path

5. Remote administrative personnel must be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an advanced authentication (AA) solution or during the session via active teleconference with the escort throughout the session
6. Enabling only during the time period needed and disabled when not in use

(i) Incorporating multi-factor authentication for all remote access (both user and privileged accounts, including third-party access for support or maintenance)

(j) Automatically disconnect remote sessions after fifteen (15) minutes of inactivity

(k) Authorizing remote users/teleworkers to connect to the internal network only if the following criteria for the remote system are met:

1. Software patch status is current
2. Anti-malware software is enabled and current

(l) *PCI-Defined*: Prohibiting personnel accessing cardholder data via remote sessions from copying, moving, and storing cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-04, AC-18, AC-19, AC-20, CA-03, CM-10, IA-02, IA-03, IA-08, MA-04, PE-17, PL-02, PL-04, SC-10, SC-12, SC-13, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4502	PR.AA-05	4.1.AC-17	5.5.AC-17	2.1.AC-17	8.4.3, 12.3.8, 12.3.9, 12.3.10		PR.AC-P3, PR.PT-P3

(AC-18) Wireless Access

Purpose

The purpose of the policy is to ensure organizations manage wireless access to prevent unauthorized network intrusions.

Scope

The policy applies to Network Operations (NetOps) and the use of technologies that do not require a physical connection (e.g., microwave, UHF/VHF radio, 802.11x, Bluetooth, Near Field Communications, etc.).

Policy

This policy requires ITS to:

(a) Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access

(b) Authorize each type of wireless access to the system prior to allowing such connections

(c) *Authentication and Encryption*: Protect wireless access to the system using authentication of both users and devices and encryption

(d) *Disable Wireless Networking*: Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment

(e) *Disable Unauthorized Connections*: Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment

(f) *Restrict Configurations by Users*: Identify and explicitly authorize users allowed to independently configure wireless networking capabilities

(g) NetOps is required to attempt to confine the wireless transmission boundary to within the geographic confines of ITS' facilities through:

1. Proper placement of wireless access points (WAPs)
2. Limiting the output/transmission power of the WAPs

(h) *IRS-Defined*: Guest wireless networks operated by or on behalf of ITS, data center, or vendor managed facilities must be completely logically separate from all other secured internal networks

(i) *IRS-Defined*: Monitor for unauthorized wireless access to the system and enforce requirements for wireless connections to the system
(j) *IRS-Defined*: Employ security mechanisms for wireless networks consistent with the sensitivity of the data to be transmitted. FIPS 140 validated encryption must be employed in all wireless networks used to access data classified Level 2 and higher and/or manage a Level 2 and higher environment
(k) *IRS-Defined*: Perform both attach monitoring and vulnerability monitoring on the wireless network to support WLAN security
(l) Ensure wireless networks use industry-recognized leading practices to implement strong encryption for authentication and transmission, commensurate with the sensitivity of the data being transmitted
(m) *IRS-defined* Additional requirements for protecting FTI on wireless networks are provided in Pub1075 Nov2021 Section 3.3.6, Network Boundary and Infrastructure

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-17, AC-19, CA-09, CM-07, IA-02, IA-03, IA-08, PL-04, SC-40, SC-43, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P3020, P4540, P4570, S3530, G530	PR.AA-05	4.1.AC-18	5.5.AC-18, 5.13.1, 5.13.1.1, 5.13.1.3, 5.13.1.4		11.1.1		PR.PT-P3

(AC-19) Access Control for Mobile Devices

Purpose
The purpose of the policy is to ensure organizations enforce security controls on mobile devices to protect sensitive data.

Scope
The policy applies to all State personnel, ITS Management, the Chief Information Security Officer (CISO), Security Operations (SecOps), data classified as Level 2 and higher (State Data) and supported mobile devices (devices) that are portable by an individual, designed to operate without the need of a physical connection to a network, possess local data storage and a self-contained power source. Mobile devices include, but are not limited to: laptop computers, smart phones, personal digital assistants (PDAs), any other existing or future mobile computing or storage device.

Policy
ITS policy requires the implementation of a centralized mobile device management (MDM) solution to authenticate and manage the configuration of supported mobile devices prior to allowing access to the internal network. Devices owned and supported by ITS **and** personally owned devices must meet the terms set out in (S.AC-02) Mobile Device Requirements.

ITS must:
(a) Establish configuration requirements, connection requirements, and implementation guidance for ITS-controlled mobile devices, to include when such devices are outside of controlled areas
(b) Authorize the connection of devices to ITS systems
(c) Restrict access to State Data by:
    1. Prohibiting the use of unclassified devices in facilities containing systems handling State Data unless specifically permitted by the ITS CISO
    2. Enforcing the following restrictions on individuals permitted by the ITS CISO to use unclassified devices in facilities containing systems processing, storing, or transmitting State Data:
        i. Connection of unclassified devices to classified systems is prohibited
        ii. Connection of unclassified devices to unclassified systems requires approval from the ITS CISO
        iii. Use of internal or external modems or wireless interfaces within the unclassified devices is prohibited

iv. Unclassified devices and the information stored on those devices are subject to random reviews and inspections by the ITS CISO and SecOps, and if classified information is found, the incident handling policy is followed

(d) Restrict the connection of classified devices to classified systems in accordance with the (MP) Media Protection Family

(e) Employ full-device encryption using the latest FIPS 140 validated encryption on areas where State Data resides to protect the confidentiality and integrity of information on ITS-owned mobile devices and mobile devices that are part of bring your own device (BYOD) implementation. Plan of actions and milestones (POAM) findings must be documented and tracked when no such encryption technology solutions are available to address a specific device

(f) *IRS-Defined*: Additional requirements on protecting FTI accessed by mobile systems are provided in Section 3.3.4 Mobile Devices, Section 2.C.7 Offshore Operations, and on the Office of Safeguards website

Policy Mapping

ITS ISPM							
AC-03, AC-04, AC-07, AC-11, AC-17, AC-18, AC020, CA-09, CM-02, CM-06, IA-02, IA-03, MP-02, MP-04, MP-05, MP-07, PL-04, SC-07, SC-34, SC-43, SI-03, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1060, P4540, P4550, S3530, S2140, G540, G550	PR.AA-05	4.1.AC-19	5.5.AC-19, 5.13.1.2.1, 5.13.1.2.2, 5.13.1.4, 5.13.2, 5.13.3, 5.13.7.2.1, 5.13.7.3				PR.AC-P3

(AC-20) Use of External Systems

Purpose

The purpose of the policy is to ensure organizations establish policies for accessing external systems to mitigate security risks.

Scope

The policy applies to the intended use of external information systems, or non-agency-owned equipment, this includes any technology used to receive, process, store, access, protect and/or transmit (Handle) data classified as Level 2 and higher (State Data) that is not owned and managed by:

- ITS or ITS' mobile device management system
- One of ITS' approved contractors or subcontractors (e.g., print vendors, collections agencies, etc.)
- One of the agency's constituent counties

Examples of external information systems include but are not limited to:

- Personally owned systems (desktops, laptops, mobile devices)
- Devices owned and managed by agency stakeholders that do not have proper approvals to Handle State Data

Policy

This policy establishes the requirements to use external information systems. ITS must:

(a) Establish terms and conditions, consistent with the trust relationships established with organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

1. Access the system from external systems
2. Process, store, or transmit ITS-controlled information using external systems

(b) Prohibit the use of non-ITS managed external systems

(c) *Limits on Authorized Use*: Permit authorized individuals to use an external system to access the system or Handle State Data only after:

1. Verification of the implementation of controls on the external system as specified in ITS' security and privacy policies and security and privacy plans
2. Retention of approved system connection or processing agreements with the organizational entity hosting the external system

(d) *Portable Storage Devices – Restricted Use*: Restrict the use of ITS-controlled portable storage devices by authorized individuals on external information systems using ITS-defined policy

(e) *Non-Organizationally Owned Systems – Restricted Use*: Restrict the use of non-ITS owned systems or system components to Handle State Data using the policies outlined within this manual

(f) *Portable Storage Devices – Prohibited Use*: Prohibit the use of ITS-controlled portable storage devices by authorized individuals on external systems

(g) Prohibit the use of personally owned systems to access any state domain unless:
1. Approved by the ITS CISO
2. ITS established and documented the specific terms and conditions for personally owned systems
3. The personally owned device is controlled in accordance with the requirements in (AC-19)
4. The user signs and agrees to the terms set out in (S.AC-02) Mobile Device Requirements

(h) Prohibit the ability for personnel or contractors to use non-ITS sanctioned devices to connect to the cloud infrastructure

(i) *(IRS-defined)* Approval by ITS CISO is required for connection of non-ITS furnished, contractor-owned devices, or personally owned devices (including USB-connected portable storage and mobile devices) to ITS-owned systems or networks handling FTI Data (This requirement does not apply to networks and systems intended for use by the public)

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-17, AC-19, CA-03, PL-02, PL-04, SA-09, SC-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4550, S2140, G540	ID.AM-02, ID.AM-04	4.1.AC-20	5.5.AC-20				PR.AC-P3

(AC-21) Data Sharing

Purpose
The purpose of the policy is to ensure organizations control data sharing to prevent unauthorized data exposure.

Scope
The policy applies to the Chief Information Security Officer (CISO) and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the sharing or re-disclosure of State Data to only authorized personnel. While it is the user's responsibility to exercise sound judgment if information should be shared, the ITS CISO must:

(a) Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for information sharing circumstances where user discretion is required

(b) Employ attribute-based access control or manual processes as defined in information exchange agreements to assist users in making information sharing/collaboration decisions (e.g., sharing or redisclosure of State Data is strictly prohibited to only authorized personnel)

(c) *(IRS-Defined)* For FTI, authorization is defined in Internal Revenue Code 26 U.S.C. § Section 6103 – Confidentiality and disclosure of returns and return information and approved by the IRS Office of Safeguards

Policy Mapping

ITS ISPM							
AC-03, AC-04, AC-16, PT-02, PT-07, RA-03, SC-15							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.1.AC-21	5.5.AC-21, 5.1.1, 5.1.1.1 - 5.1.1.6, 5.1.1.8				CT.DM-P2, PR.PO-P6

(AC-22) Publicly Accessible Content

Purpose
The purpose of the policy is to ensure organizations manage publicly accessible content to prevent unauthorized modifications.

Scope
The policy applies to the Communication Manager and all ITS supported information systems (System/s) that may receive, process, store, access, protect, and/or transmit (Handle) data classified as Level 1 and higher (State Data) and publicly accessible Systems.

Policy
ITS policy requires the Communication Manager to:

(a) Designate individuals authorized to make information publicly accessible
(b) Train the authorized individuals to ensure that publicly accessible information does not contain nonpublic information
(c) Review the proposed content of information prior to posting onto the publicly accessible System to ensure that nonpublic information is not included
(d) Review the content on the publicly accessible System for nonpublic information at a minimum quarterly and remove such information, if discovered

Policy Mapping

ITS ISPM							
AC-03, AT-02, AT-03, AU-13							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P5040		4.1.AC-22	5.5.AC-22, 5.10.1.1.6				

(AC-23) Data Mining Protection

Purpose
The purpose of the policy is to ensure organizations implement safeguards against unauthorized data mining activities.

Scope
The policy applies to Security Operations (SecOps), Threat Hunter Team (THT), and all ITS supported information systems (System/s) that may receive, process, store, access, protect, and/or transmit (Handle) data classified as Level 1 and higher (State Data).

Policy
ITS policy requires SecOps and THT to employ ITS-defined data mining prevention and detection techniques for ITS-defined data storage objects to detect and protect against unauthorized data mining.

Policy Mapping

ITS ISPM

PM-12, PT-02

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.1.AC-23					CT.DP-P1, CT.DP-P2, CT.DP-P3

(AC-24) Access Control Decisions – NR

Policy Objective: No Requirement.

(AC-25) Reference Monitor – NR

Policy Objective: No Requirement.

(AT) Awareness and Training Family

(AT-01) Security Awareness and Training Policies and Procedures

Purpose
The purpose of the policy is to ensure – Ensure organizations establish and maintain a formal policy and procedures for security awareness and training to promote a culture of cybersecurity.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all awareness and training family policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the awareness and training policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to all State personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted State Data:
   1. An State level security and privacy awareness and training policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the awareness and training policies and the associated awareness and training family policies

(b) Review and update the current awareness and training:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4130, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.2.AT-1	5.2.AT-1	2.3.AT-1	12.6		PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6

(AT-02) Literacy Training and Awareness

Purpose
The purpose of the policy is to ensure organizations provide security and privacy literacy training to all system users to enhance their ability to recognize and mitigate threats.

Scope
The policy applies to Human Resources (HR), the Chief Information Security Officer (CISO), and all State personnel that access ITS supported information systems (System/s) that may receive, process, store, access, protect, and/or transmit (Handle) data classified as Level 1 and higher (State Data).

Policy

ITS policy requires, prior to granting authorized personnel access to State Data and Systems, personnel to certify their understanding of ITS' security policies and procedures for safeguarding information. Personnel may not access Systems and State Data unless certification, or recertification, has been completed. HR, in consultation with CISO, must develop and document a security awareness and training program and disseminate the program to all Systems users. ITS must:

(a) Provide security and privacy literacy training to System users (including managers, senior executives, and contractors):
   1. As part of initial training for new users prior to accessing State Data
   2. When required by System changes, following assessment or audit findings, within thirty (30) days of any security or privacy incidents, or changes to applicable laws, executive orders, directives, regulations, polices, standards, and guidelines
   3. Annually thereafter

(b) Employ the following techniques to increase the security and privacy awareness of System users:
   1. Display posters
   2. Offering supplies inscribed with security and privacy reminders
   3. Displaying logon screen messages
   4. Generating email advisories or notices from ITS officials
   5. Conducting awareness events

(c) Update literacy training and awareness content annually and following System changes

(d) Incorporate lessons learned from internal or external security or privacy incidents into literacy training and awareness techniques

(e) *Practical Exercises*: Provide practical exercises in literacy training that simulate events and incidents

(f) Train users and provide means to ensure workstations are adequately protected from theft, particularly regarding laptops acting as workstations

(g) Distribute security and privacy awareness reminders/updates to all users at least quarterly

(h) Conduct phishing email simulation exercises on at least a quarterly

(i) Training and certification must include the following provisions:
   1. Include security awareness training on recognizing and reporting potential indicators of insider threat. Insider threat training should bring awareness of the potential for personnel to use insider knowledge of sensitive ITS information to perform malicious actions, which could include the unauthorized access or re-disclosure of data
   2. For data classified as FTI:
      i. Then per IRS 1075 IRC 6103(p)(4)(D)(6.3)
      ii. Personnel must be advised of the penalty provisions of IRCs 7431, 7213, and 7213A
   3. The incident response policy and procedure for reporting unauthorized disclosures and data breaches
   4. Personnel must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements. It must also contain a statement that the employee understands they must report possible improper inspection or disclosure of FTI, including breaches and security incidents to the NCDOR Disclosure Officer
   5. Training certification and recertification must be documented and placed in ITS files for review and retained for at least five (5) years
   6. Provide literacy training on recognizing:
      i. And reporting potential indicators of insider threats
      ii. And reporting potential and actual instances of social engineering and social mining
      iii. Suspicious communications and anomalous behavior in organizational Systems using ITS-defined indicators or malicious code

Policy Mapping

ITS ISPM							
AC-03, AC-17, AC-22, AT-03, AT-04, CP-03, IA-04, IR-02, IR-07, IR-09, PL-04, PM-13, PM-21, PS-07, PT-02, SA-08, SA-16							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy

P4505, P4590, S6010	PR.AT-01	4.2.AT-2	5.2.AT-2	2.3.AT-2	12.6.1	164.308(a)(5)(i), 164.308(a)(5)(ii)(A)	PB, GV.AT-P1

(AT-03) Role-Based Security Training

Purpose

The purpose of the policy is to ensure organizations deliver specialized security and privacy training tailored to personnel roles to strengthen their ability to fulfill security responsibilities.

Scope

The policy applies to Human Resources (HR) and all State personnel to include contractors that have access to supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS to determine the appropriate content of role-based training based on the assigned roles and responsibilities of individuals and the specific security requirements ITS and the Systems to which personnel have authorized access. ITS must:

(a) Provide role-based security and privacy training to personnel with the roles and responsibilities defined in (S.AT-01) Role-Based Training Content:
   1. Before authorizing access to the System, State Data, or performing assigned duties
   2. Annually
   3. When required by System changes

(b) Update role-based training content annually and following System changes

(c) Incorporate lessons learned from internal or external security or privacy incidents into role-based training

Policy Mapping

ITS ISPM							
AC-03, AC-17, AC-22, AT-02, AT-04, CP-03, IR-02, IR-07, IR-09, IR-10, PL-04, PM-13, PM-23, PS-07, PS-09, SA-03, SA-08, SA-11, SA-16, SR-05, SR-06, SR-11, S.AT-01							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4505	PR.AT-01, PR.AT-02	4.2AT-3	5.2.AT-3	2.3.AT-3	6.5, 9.9.3, 12.6.1, 12.10.4		PB, GV.AT-P1, GV.AT-P2, GV.AT-P3, GV.AT-P4

(AT-04) Security Training Records

Purpose

The purpose of the policy is to ensure organizations maintain documented records of security and privacy training, enabling accountability, compliance verification, and continuous improvement of training programs.

Scope

The policy applies to Human Resources (HR) and all State personnel that have access to supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires HR to:

(a) Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training

(b) Retain individual training records for five (5) years

(c) Have State personnel acknowledge in writing or electronically, at least annually, that they have read and understand ITS' cybersecurity policies

Policy Mapping

ITS ISPM							
AT-02, AT-03, CP-03, IR-02, PM-14, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.2.AT-4	5.2.AT-4	2.3.AT-4	12.6.2		PB

(AT-05) Contacts with Security Groups and Associations – WD

Withdrawn: Incorporated into PM-15.

(AT-06) Training Feedback

Purpose

The purpose of the policy is to ensure organizations collect and analyze feedback on training programs to improve awareness and effectiveness.

Scope

The policy applies to Executive Leadership and the Chief Information Security Officer (CISO).

Policy

This policy establishes the requirement to provide feedback on agency awareness and role-based training results to Executive Leadership and the CISO office. Training results, especially failures of personnel in critical roles, can be indicative of a potentially serious problem. Training feedback supports the evaluation and update of agency training described in AT-02(b) and AT-03(b).

Policy Mapping

ITS ISPM							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.2.AT-6	3.2.10				

(AU) Audit and Accountability Family

(AU-01) Audit and Accountability Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish and maintain audit and accountability policies and procedures to support security and compliance objectives.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all audit and accountability family policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the audit and accountability policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel with audit and accountability responsibilities:
   1. An State level audit and accountability policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the audit and accountability family policies and the associated audit and accountability family policies

(b) Review and update the current audit and accountability:
   1. Policies annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data
   2. Procedures annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.3.AU-1	5.4.AU-1	2.2.AU-1	10.1	164.312(b)	PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CT.DM-P8

(AU-02) Audit Events

Purpose
The purpose of the policy is to ensure organizations identify, log, and retain security-relevant events to support audit functions and forensic analysis.

Scope
The policy applies to Security Operations (SecOps), System Administrators (SysAdmin), and all ITS supported information systems (System/s) that contain data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires logging of events that are significant and relevant to the security of Systems and the privacy of individuals. To support monitoring and auditing needs ITS must:

(a) Identify the types of events that the System is capable of logging in support of the audit function: See (S.AU-01) Event Logging
(b) Coordinate the event logging function with other ITS entities (i.e., ITS GRC) requiring audit-related information to enhance mutual support and to guide and inform the selection of auditable events
(c) Specify the following event types for logging within the System: See (S.AU-01) Event Logging
(d) Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents
(e) Review and update the audited events at a minimum, annually
(f) Legal Issues – The media and System combined must be able to show, to the court's criteria of acceptance, that the objects, documents, records, or information:
    1. Are authentic (are a true and accurate copy of the original)
    2. Was made near to the time of the event in question
    3. Was created and maintained as a regular course of business
    4. Was created with input procedures that are documented and defined and can be verified by proven tests for accuracy

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-06, AC-07, AC-08, AC-16, AC-17, AU-03, AU-04, AU-05, AU-06, AU-07, AU-11, AU-12, CM-03, CM-05, CM-06, CM-13, IA-03, MA-04, MP-04, PE-03, PM-21, PT-02, PT-07, RA-08, SA-08, SC-07, SC-18, SI-03, SI-04, SI-07, SI-10, SI-11, S.AU-01							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1030, P4501, P4502	PR.PS-04	4.3.AU-2	5.4.AU-2	2.2.AU-2	10.2.1		PB, CT.DM-P8

(AU-03) Content of Audit Records

Purpose

The purpose of the policy is to ensure organizations capture sufficient details in audit records to facilitate event correlation and security investigations.

Scope

The policy applies to Network Operations (NetOps), Security Operations (SecOps), and all ITS supported information systems (System/s) that contain data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires NetOps and SecOps to:

(a) Ensure that audit records contain information that establishes the following:
    1. What type of event occurred
    2. When the event occurred
    3. Where the event occurred
    4. Source of the event
    5. Outcome of the event
    6. Identity of any individuals, subjects, or objects/entities associated with the event
    7. Session, connection, transaction, and activity duration
    8. Source and destination addresses
    9. Object or filename involved
    10. Number of bytes received, and bytes sent (for client-server transactions) in the audit records for audit events identified by type, location, or subject
    11. *(FBI-Defined)* The III portion of the log must clearly identify:
        i. The operator
        ii. The authorized receiving agency

iii. The requestor
iv. The secondary recipient

12. Details that facilitate the reconstruction of events if:
    i. Unauthorized activity occurs or is suspected
    ii. A malfunction occurs or is suspected

(b) *Limit Personally Identifiable Information (PII) Elements*: PII contained in audit records to the following elements identified in the privacy risk assessment: ITS-defined elements

Policy Mapping

ITS ISPM							
AU-02, AU-08, AU-12, AU-14, MA-04, PL-09, SA-08, SI-07, SI-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.PS-04	4.3.AU-3	5.4.AU-3	2.2.AU-3	10.3, 10.3.1-10.3.6		PB, CT.DM-P8, CT.DP-P2

(AU-04) Audit Log Storage Capacity

Purpose
The purpose of the policy is to ensure organizations allocate adequate storage capacity for audit logs to meet retention and analysis requirements.

Scope
The policy applies to the Infrastructure Team and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the Infrastructure Team to:

(a) Allocate sufficient audit record storage capacity to retain audit records for the required audit retention requirements in (S.SI-01) Retention Schedule to handle security incidents and compliance mandates

(b) Configure auditing to reduce the likelihood of such capacity being exceeded

Policy Mapping

ITS ISPM							
AU-02, AU-05, AU-06, AU-07, AU-09, AU-11, AU-12, AU-14, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.3.AU-4	5.4.AU-4		10.7		PR.DS-P4

(AU-05) Response to Audit Processing Failures

Purpose
The purpose of the policy is to ensure organizations detect, report, and respond to audit logging failures to maintain system integrity and accountability.

Scope
The policy applies to the Security Operations (SecOps), System Administrators (SysAdmin), and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires Systems to:

(a) Alert State personnel with audit and accountability responsibilities, SysAdmins, and NetOps within one (1) hour in the event of an audit logging process failure
(b) Take the following additional actions:
    1. Monitor System operational status using operating System or System audit logs and verify functions and performance of the System. Logs must be able to identify where System process failures have taken place and provide information relative to corrective actions to be taken by the SysAdmin
    2. Restart all audit logging processes and verify System(s) are logging properly
    3. If logs are not available, shut down the System
(c) *Storage Capacity Warning*: Provide a warning to the SecOps within twenty-four (24) hours when allocated audit record storage volume reaches (75%) of repository maximum audit record storage capacity
(d) SecOps is responsible for managing a 24x7x365 alerting process for critical Systems

Policy Mapping

ITS ISPM							
AU-02, AU-04, AU-07, AU-09, AU-11, AU-12, AU-14, SI-04, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.3.AU-5	5.4.AU-5				

(AU-06) Audit Review, Analysis, and Reporting

Purpose
The purpose of the policy is to ensure ITS regularly review and analyze audit records to detect anomalies, investigate incidents, and generate reports that support security monitoring and compliance.

Scope
The policy applies to Security Operations (SecOps), ITS Management, and the logs being collected from all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires SecOps to:
(a) Review and analyze System audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity
(b) Report findings in accordance with incident handling procedures in:
    1. ITA Policy P4590 – Cybersecurity Incident and Breach Response Management and Reporting
    2. ITA Standard S6010 – Cybersecurity Incident and Breach Response Management and Reporting
    3. If the finding involves a potential unauthorized disclosure of FTI, ITS must also contact:
        i. The appropriate IRS special agent-in-charge
        ii. The Treasury Inspector General for Tax Administration (TIGTA)
        iii. The IRS Office of Safeguards
(c) Adjust the level of audit review, analysis, and reporting within the System when there is a change in risk to operations, assets, individuals, or other agencies based on credible sources of information
(d) *Automated Process Integration*: Integrate audit record review, analysis, and reporting processes using automated mechanisms to support ITS processes for investigation and response to suspicious activities
(e) *Correlate Audit Record Repositories*: Analyze and correlate audit records across different repositories to gain ITS wide situational awareness
(f) *Permitted Actions*: Specify the permitted actions for each role or users associate with the review, analysis, and reporting of audit record information
(g) *Correlation with Information from Nontechnical Sources*: Correlate information from nontechnical sources with audit record information to enhance ITS wide situational awareness

(h) Develop processes for the timely detection and reporting of failures of critical security control Systems. Reference ITS Standard (S.AU-02) Critical Security Control Systems

(i) Responding to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:

1. Restoring security functions
2. Identifying and documenting the duration (date and time start to end) of the security failure
3. Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
4. Identifying and addressing any security issues that arose during the failure
5. Performing a risk assessment to determine whether further actions are required because of the security failure
6. Implementing controls to prevent cause of failure from reoccurring
7. Resuming monitoring of security controls

(j) In consultation with ITS Management:

1. Determine normal time-of-day and duration usage for System accounts
2. Monitor for atypical usage of System accounts
3. Report of atypical usage in accordance with incident escalation procedures

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-05, AC-06, AC-07, AC-17, AU-07, AU-16, CA-02, CA-07, CM-02, CM-05, CM-06, CM-10, CM-11, IA-02, IA-03, IA-05, IA-08, IR-05, MA-04, MP-04, PE-03, PE-06, RA-05, SA-08, SC-07, SI-03, SI-04, SI-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4570, P4590, S6010	PR.PS-04, DE.AE-02, DE.AE-03	4.3.AU-6	5.4.AU-6	2.2.AU-6	10.6, 10.6.1, 10.6.2, 10.6.3		ID.DE-P5, CT.DM-P8

(AU-07) Audit Record Reduction and Report Generation

Purpose

The purpose of the policy is to provide organizations with the capability to filter, summarize, and generate reports from audit records without altering their original content or time ordering, supporting efficient security monitoring and incident investigations.

Scope

The policy applies to Security Operations (SecOps), and the logs being collected for ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires SecOps to implement a security information and event management (SIEM) to provide the capability to process audit records for events of interest based on the content of specific audit record fields defined in (S.AU-01) Event Logging and generate reports that allow SecOps to review potentially significant issues and/or incidents on the System generating the event. The System must provide an audit reduction and report generation capability that:

(a) Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents

(b) Does not alter the original content or time ordering of audit records

Policy Mapping

ITS ISPM							
AC-02, AU-02, AU-03, AU-04, AU-05, AU-06, AU-12, AU-16, CM-05, IA-05, IR-04, PM-12, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.PS-04, RS.AN-03, RS.AN-06, RS.AN-07	4.3.AU-7	5.4.AU-7	2.2.AU-7			CT.DM-P8

(AU-08) Time Stamps

Purpose
The purpose of the policy is to ensure organizations use reliable time sources to generate accurate timestamps for audit records to support event correlation.

Scope
The policy applies to Infrastructure Team and the logs being collected for ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires Infrastructure Team to configure Systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time:

(a) Systems have the correct and consistent time
(b) Time data is protected
(c) Time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Mountain Standard Time (MST)
(d) Compare and synchronize the internal information system clocks to an enterprise-wide authoritative time source. Where possible, synchronize enterprise time source to an external source (e.g., NIST, Naval Observatory)
(e) The official NIST or USNO Internet Time Service required to use for system time synchronization include, but are not limited to:
    1. Time.nist.gov 192.43.244.18 [primary]
    2. Time-nw.nist.gov 131.107.13.100 [alternate]

Policy Mapping

ITS ISPM							
AU-03, AU-12, AU-14, SC-45							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.3.AU-8	5.4.AU-8		10.4, 10.4.1-10.4.3		

(AU-09) Protection of Audit Information

Purpose
The purpose of the policy is to ensure organizations safeguard audit records from unauthorized access, modification, and deletion, preserving their integrity for security monitoring, incident investigation, and compliance.

Scope
The policy applies to Security Operations (SecOps), Network Operations (NetOps), System Administrators (SysAdmins) and to the logs being collected for ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to restrict the ability to access and execute audit logging tools to only authorized individuals. SecOps must:

(a) Protect audit information and audit tools from unauthorized access, modification, and deletion

(b) Alert the CISO upon detection of unauthorized access, modification, or deletion of audit information
(c) *Access by Subset of Privileged Users*: Authorize access to management of audit logging functionality to only authorized SysAdmins
(d) Restrict access to the management of audit functionality to users who have:
1. A valid business justification
2. Received security awareness training equal with the level of risk from having privileged access
3. Demonstrated technical competence specific to the environment where access is being granted
4. System and NetOps must not have the ability to modify or delete audit log entries

Policy Mapping

ITS ISPM							
AC-03, AC-06, AU-06, AU-11, AU-14, AU-15, MP-02, MP-04, PE-02, PE-03, PE-06, SA-08, SC-08, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4502, P4505	PR.DS-10	4.3.AU-9	5.4.AU-9	2.2.AU-9	10.5, 10.5.1-10.5.5	164.312(c)(a)	

(AU-10) Non-Repudiation

Purpose
The purpose of the policy is to ensure organizations provide irrefutable evidence that individuals or processes have performed specific actions, preventing denial of responsibility and supporting accountability through mechanisms like digital signatures and message receipts.

Scope
The policy applies to Security Operations (SecOps) and the logs being collected for ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires SecOps to be able to provide irrefutable evidence that an individual (or process acting on behalf of an individual) has created information, sent and received messages, and approved information.

Policy Mapping

ITS ISPM							
AU-09, PM-12, SA-08, SC-08, SC-12, SC-13, SC-16, SC-17, SC-23							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1030					10.5.5	164.312(c)(b)	PB

(AU-11) Audit Record Retention

Purpose
The purpose of the policy is to ensure organizations retain audit records for a defined period to support incident investigations, regulatory compliance, and operational needs.

Scope
The policy applies to Security Operations (SecOps)and the logs being collected for ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires SecOps to retain audit records for the time period defined in (S.SI-01) Retention Schedule to provide support for after-the-fact investigations of incidents and to meet regulatory and agency information retention requirements. Logs must be retained according to ITS' record retention schedule:

(a) For Systems where State Data is Handled log entries must be:
   1. Immediately available for a minimum of ninety (90) days (online)
   2. Available for time specified in (S.SI-01) Retention Schedule (online or offline storage)

(b) All logs must be exportable or transferable in an automated fashion

(c) Once logs are offloaded to an ITS-approved log collector, the local logs may be removed from the reporting System or application

Policy Mapping

ITS ISPM							
AU-02, AU-04, AU-05, AU-06, AU-09, AU-14, MP-06, RA-05, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1030	PR.PS-04	4.3.AU-11	5.4.AU-11	2.2.AU-11	10.7		

(AU-12) Audit Record Generation

Purpose

The purpose of the policy is to ensure organizations generate audit records for defined security events, allowing personnel to monitor activities, investigate incidents, and maintain accountability.

Scope

The policy applies to Security Operations (SecOps) and logs being collected for ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires SecOps to:

(a) Provide audit record generation capability for the event types the System is capable of auditing as defined in AU-02(f) on all Systems where State Data is Handled

(b) Allow State personnel with audit record generation responsibilities, State personnel with information security and privacy responsibilities, and System/network administrators to select the event types that are to be logged by specific components of the System

(c) Generate audit records for the event types defined in AU-02(f) that include the audit record content defined in AU-03

(d) *System-wide and Time-correlated Audit Trail*: Compile audit records from Systems that Handle State Data into a System-wide logical audit trail that is time-correlated to within ITS-defined level of tolerance for the relationship between time stamps of individual records in the audit trail

Policy Mapping

ITS ISPM							
AC-06, AC-17, AU-02, AU-03, AU-04, AU-05, AU-06, AU-07, AU-14, CM-05, MA-04, MP-04, PM-12, SA-08, SC-18, SI-03, SI-04, SI-07, SI-10							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.PS-04, DE.CM-01, DE.CM-03, DE.CM-09	4.3.AU-12	5.4.AU-12	2.2.AU-12			CT.DM-P6, CT.DM-P8

(AU-13) Monitoring for Information Disclosure

Purpose

The purpose of the policy is to ensure organizations actively monitor open-source information and external sites for unauthorized disclosure of sensitive data, enabling timely detection, notification, and corrective actions.

Scope

The policy applies to Security Operations (SecOps) and the logs being collected for ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires SecOps to:

(a) Monitor open-source information daily for evidence of unauthorized disclosure of agency information
(b) If an information disclosure is discovered follow ITS' Incident Response Plan
(c) *Unauthorized Replication of Information*: Employ discovery techniques, processes, and tools to determine if external entities are replicating agency information in an unauthorized manner

Policy Mapping

ITS ISPM							
AC-22, PE-03, PM-12, RA-05, SC-07, SI-20							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4150, P4590, S6010	PR.DS-10, DE.CM-03				12.5.5		CT.DM-P8, PR.DS-P5

(AU-14) Session Audit – NR

Policy Objective: No Requirement.

(AU-15) Alternate Audit Capability – WD

Withdrawn: Incorporated into AU-05

(AU-16) Cross-Organizational Audit Logging

Purpose

The purpose of the policy is to ensure organizations coordinate audit information sharing across external entities when logs are transmitted beyond organizational boundaries, supporting accountability, identity preservation, and compliance.

Scope

The policy applies to the Chief Compliance Officer (CCO) and external agencies, outsourced data centers, or cloud providers who store, transmit or process (Handle) data classified as Level 1 and higher (State Data). The provider must be held accountable to protect and share audit information with ITS through the contract.

Policy

ITS policy assigns responsibility to the CCO to:

(a) Employ ITS-defined methods for coordinating ITS-defined audit information among external organizations when audit information is transmitted across agency boundaries
(b) *Identity Preservation*: Preserve the identity of individuals in cross-organizational audit trails
(c) *Sharing of Audit Information*: Provide cross-organizational audit information to ITS-defined organizations based on ITS-defined cross-organizational sharing agreements

Policy Mapping

ITS ISPM							
AU-03, AU-06, AU-07, CA-03, PT-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1080, P4120	PR.DS-02	4.3.AU-16					CT.DM-P8, CT.DP-P1, CT.DP-P3

(CA) Assessment, Authorization, and Monitoring Family

(CA-01) Assessment, Authorization, and Monitoring Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish, document, and disseminate policies and procedures for assessment, authorization, and monitoring to maintain compliance and operational integrity.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all security and privacy assessment, authorization, and monitoring policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
1. An State level security and privacy assessment, authorization, and monitoring policy that:
   i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
   ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
2. Procedures to facilitate the implementation of the security and privacy assessment, authorization, and monitoring policies and the associated security and privacy assessment, authorization, and monitoring family policies

(b) Review and update the current security and privacy assessment, authorization, and monitoring:
1. Policies annually, following changes in ITS' System operating environment and when security incidents occur
2. Procedures annually, following changes to ITS' System operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.4.CA-1	CA-1				PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6

(CA-02) Policy Assessments

Purpose
The purpose of the policy is to ensure organizations conduct regular assessments of security and privacy controls to evaluate effectiveness and identify areas for improvement.

Scope
The policy applies to the Chief Information Security Officer (CISO), and Chief Compliance Officer (CCO), and Policy Officer.

Policy

ITS policy requires policy assessments to be conducted on implemented policies as documented in security and privacy plans, to meet information security and privacy requirements, identify weaknesses, and deficiencies in the system design, development process, provide essential information needed to make risk-based decisions as part of authorization processes, and comply with vulnerability mitigation procedures. The Policy Officer must:

(a) Select the appropriate assessor or assessment team for the type of assessment to be conducted
(b) Develop a policy assessment plan that describes the scope of the assessment including:
    1. Policy and policy enhancements under assessment
    2. Assessment procedures to be used to determine policy effectiveness
    3. Assessment environment, assessment team, and assessment roles and responsibilities
(c) Ensure the policy assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment
(d) Assess the policies in the system and its environment of operation annually to determine the extent to which the policies are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements
(e) Produce a policy assessment report that document the results of the assessment
(f) Provide the results of the policy assessment to the CISO and CCO
(g) *Independent Assessors*: Employ independent assessors or assessment teams to conduct policy assessments

Policy Mapping

ITS ISPM							
AC-20, CA-05, CA-06, CA-07, PM-09, RA-05, RA-10, SA-11, SC-38, SI-03, SI-12, SR-02, SR-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4130, P4520	ID.RA-01, ID.IM-01, ID.IM-02, ID.IM-03	4.4.CA-2	CA-2	2.12.CA-2			PB, ID.DE-P5, GV.MT-P3, CT.DM-P9, PR.PO-P5

(CA-03) Information Exchange

Purpose

The purpose of the policy is to ensure organizations establish policies and controls for securely sharing information across systems, users, and external entities, preventing unauthorized access, data leakage, and integrity violations.

Scope

The policy applies to the Chief Information Security Officer (CISO) and information exchanges between two (2) or more systems.

Policy

ITS policy requires the CISO to determine the risk associated with system information exchange and the policies needed for appropriate risk mitigation and document these connections through interconnected security agreements. The CISO must:

(a) Approve and manage the exchange of information between the system and other systems using interconnected security agreements (ISAs)
(b) Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated
(c) Review and update the agreements on an annual basis or when responsibilities or signatories change
(d) *SSA-Defined*: Document an ITS specific data flow diagram that shows how SSA data is transmitted to ITS

Policy Mapping

ITS ISPM							
AC-04, AC-20, AU-16, CA-06, IA-03, IR-04, PL-02, PT-07, RA-03, SA-09, SC-07, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4550, P4570, S2140, G540	ID.AM-03, PR.DS-01, PR.DS-02, PR.DS-10	4.4.CA-3	CA-3	2.12.CA-3			

(CA-04) Security Certification – WD

Policy Objective: Withdrawn: Incorporated into CA-02.

(CA-05) Plan of Action and Milestones

Purpose

The purpose of the policy is to ensure organizations document and track remediation efforts for security and privacy weaknesses identified during assessments, audits, or continuous monitoring activities.

Scope

The policy applies to the Chief Information Security Officer (CISO) and any known weakness or deficiency identified for all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires remedial actions to be documented in a plan of action and milestones (POAM), or some other ITS-approved method. The CISO must:

(a) Develop a POAM for the System to document the planned remediation actions of ITS to correct weaknesses or deficiencies noted during the assessment of the policies and to reduce or eliminate known vulnerabilities in the System

(b) Update existing POAMs quarterly, at a minimum, based on the findings from policy assessments, independent audits or reviews, and continuous monitoring activities

(c) Ensure that the individual and/or office responsible for correcting each weakness is identified in the appropriate POAM

(d) Enter all new weaknesses into appropriate POAMs within two (2) months for weaknesses identified during assessments

Policy Mapping

ITS ISPM							
CA-02, CA-07, PM-04, PM-09, RA-07, SI-02, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.IM-01, ID.IM0-2, ID.IM-03	4.4.CA-5	CA-5				PB, ID.RA-P5, GV.MT-P4

(CA-06) Authorization

Purpose

The purpose of the policy ensures organizations formally authorize information systems before operational use, assessing security risks and compliance to maintain accountability and protect sensitive data.

Scope

The policy applies to the Chief Information Officer (CIO), Chief Information Security Officer (CISO), and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires all new technology platforms be approved by the CIO and CISO prior to the introduction of the new System into production environments. All new Systems must:

(a) Be reviewed by the CISO for common policies available for inheritance by ITS Systems
(b) Ensure that the CIO and CISO for the System, before commencing operations:
    1. Accepts the use of common policies inherited by the System
    2. Authorizes the System to operate
(c) Ensure that the CISO for common policies authorizes the use of those controls for inheritance by ITS Systems
(d) Update the authorizations whenever there is a significant change to the System, or every three (3) years, whichever occurs first

Policy Mapping

ITS ISPM							
CA-02, CA-03, CA-07, PM-09, PM-10, RA-03, SA-10, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.4.CA-6	CA-6		12.3.1		PB

(CA-07) Continuous Monitoring

Purpose

The purpose of the policy is to ensure organizations implement ongoing security and privacy monitoring to detect vulnerabilities, assess control effectiveness, and support risk-based decision-making.

Scope

The policy applies to the Chief Information Security Officer (CISO) and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy assigns the CISO the responsibility to develop a System-level continuous monitoring strategy and implement continuous monitoring in accordance with ITS' continuous monitoring strategy that includes:

(a) Establishing ITS-defined metrics to be monitored annually, at a minimum
(b) Establishing ITS-defined frequency (no less than annually) for monitoring and ITS-defined frequencies (no less than annually) for ongoing assessment of security and privacy control effectiveness
(c) Ongoing policy assessments in accordance with the continuous monitoring strategy
(d) Ongoing monitoring of System and ITS-defined metrics in accordance with the continuous monitoring strategy
(e) Correlation and analysis of information generated policy assessments and monitoring
(f) Response actions to address results of the analysis of policy assessments and monitoring information
(g) Reporting the security and privacy status of the System to Executive Leadership annually
(h) *Independent Assessment*: Employing independent assessors or assessment teams to monitor the policies in the System on an ongoing basis
(i) *Risk Monitoring*: Ensuring risk monitoring is an integral part of the continuous monitoring strategy that includes the following:
    1. Effectiveness monitoring
    2. Compliance monitoring
    3. Change monitoring

Policy Mapping

ITS ISPM

AC-02, AC-06, AC-17, AT-04, AU-06, AU-13, CA-02, CA-05, CA-06, CM-03, CM-04, CM-06, CM-11, IA-05, IR-05, MA-02, MA-03, MA-04, PE-03, PE-06, PE-14, PE-16, PE-20, PL-02, PM-04, PM-06, PM-09, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-07, PT-07, RA-03, RA-05, RA-07, RA-10, SA-08, SA-09, SA-11, SC-05, SC-07, SC-18, SC-38, SC-43, SI-03, SI-04, SI-12, SR-06							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4150	ID.RA-01, ID.RA-07, ID.IM-01, ID.IM-02, ID.IM-03, DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-06, DE.CM-09, DE.AE-02, DE.AE-03	4.4.CA-7	5.4.3,	2.12.CA-7	10.6, 10.6.1, 10.6.2		PB, ID.DE-P5, GV.MT-P1, GV.MT-P3, CT.DM-P9, PR.PO-P5, PR.PO-P6

(CA-08) Penetration Testing

Purpose

The purpose of the policy is to ensure is to ensure organizations conduct controlled security testing to identify vulnerabilities, assess system defenses, and validate the effectiveness of security controls.

Scope

The policy applies to ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS to conduct penetration testing every three (3) years on the ITS environment. External and internal penetration testing must include the following:

(a) Based on industry-accepted penetration testing approaches (e.g., *NIST SP 800-115*)
(b) Coverage for the entire Cardholder Data Environment (CDE) perimeter and critical Systems
(c) Testing from both inside and outside the network
(d) Testing to validate any segmentation and scope-reduction controls
(e) Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in PCI DSS Requirement 6.5
(f) Defines network-layer penetration tests to include components that support network functions as well as operating Systems
(g) Reviews and considerations of threats and vulnerabilities experienced in the last twelve (12) months
(h) Specifies retention of penetration testing results and remediation activities results
(i) Internal and external testing that occurs at least annually and after any significant infrastructure or application upgrade or modification (such as an operating System upgrade, a sub-network added to the environment, or a web server added to the environment)
(j) Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections

Policy Mapping

ITS ISPM							
RA-05, RA-10, SA-11, SR-05, SR-06							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-01, ID.IM-01, ID.IM-02, ID.IM-03	4.4.CA-8			11.3-11.3.3		PR.PO-P5

(CA-09) Internal System Connections

Purpose

The purpose of the policy is to ensure organizations authorize, document, and review internal system connections to maintain security, privacy, and operational integrity.

Scope

This policy applies to both internal (intra) and external connections to supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS to:

(a) Authorize internal connections of System or classes of components to the System (ITS may authorize internal connections for a class of components with common characteristics and/or configurations Instead of authorizing each individual internal connection)

(b) Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated

(c) Terminate internal System connections after ITS-defined conditions

(d) Review annually the continued need for each internal connection

(e) *Compliance Checks*: Perform security and privacy compliance checks on constituent System components prior to the establishment of the internal connection

(f) For critical Systems, all internal connections must be documented and authorized

Policy Mapping

ITS ISPM							
AC-03, AC-04, AC-18, AC-19, CM-02, IA-03, SC-07, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-03	4.4.CA-9	5.7.1.1, 5.7.1.2, 5.7.2		1.1.2,1.1.3		

(CM) Configuration Management Family

(CM-01) Configuration Management Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish, document, and disseminate configuration management policies and procedures to maintain system integrity and compliance

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all security and privacy configuration management policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the configuration management policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level configuration management policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the configuration management policies and the associated configuration management family policies

(b) Review and update the current configuration management:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PS-08, SA-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03, PR.PS-01	4.5.CM-1	5.7.CM-1				PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P1

(CM-02) Baseline Configuration

Purpose
The purpose of the policy is to ensure organizations establish, document, and maintain a secure baseline configuration for their information systems. This control helps prevent unauthorized changes, supports system integrity, and ensures consistency across deployments.

Scope
The policy applies to the Infrastructure Team and all ITS supported information systems (System/s) with a low moderate, or high baseline.

Policy

ITS policy requires the Infrastructure Team to:

(a) Develop, document, and maintain a current baseline configuration of Systems and System components (e.g., software packages, version numbers, and patch information)

(b) Review and update the baseline configuration of the System:
1. At a minimum annually
2. When required due to reorganizations, refreshes, etc.
3. When System components are installed, changed, modified, or upgraded
4. When changes occur that may have potential impact to security controls

(c) *Automation Support for Accuracy and Currency*: Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the System using automated mechanisms

(d) *Retention of Previous Configurations*: Retain at least three (3) previous versions of the baseline configurations of the System to support rollback

(e) *Development and Test Environments*: Maintain and manage baseline configurations for development and test environments separately from its production baseline configurations

(f) *Configure Systems and Components for High-risk Areas*: For Systems, components, or devices used in high-risk areas:
1. ITS must:
   i. Issue Systems, System components or devices with hardened configurations to individuals traveling to locations that State of Idaho Agencies deems to be of significant risk
   ii. Apply additional, ITS-defined security safeguards to validate the security of the device(s) when the individual(s) return
2. Users are required to:
   i. Physically examine their mobile devices upon return from travel to locations of concern for signs of physical or logical tampering
   ii. Immediately report any possible tampering to ITS
3. Infrastructure Team must verify that running and start up configuration files are:
   i. Synchronized with the correct build
   ii. The same secure configurations

(g) Ensure all devices connect to a managed organizational network at regular intervals to receive configuration changes, anti-virus updates, and security patch updates

(h) *IRS-Defined*: ITS must use SCSEMs provided on the Office of Safeguards website to ensure secure configurations of all agency information technology and communication Systems receiving, processing, storing, accessing, protecting and/or transmitting FTI

(i) *FBI-Defined*: Develop, document, and maintain a current and complete topological drawing depicting the interconnectivity of ITS' network to CJI systems and services. Review and update the topological drawing of the system:
1. At a minimum annually
2. When required due to security-relevant changes to the system and/or security incidents occur
3. When system components are installed or upgraded

Policy Mapping

ITS ISPM							
AC-19, AU-06, CA-09, CM-01, CM-03, CM-05, CM-06, CM-08, CM-09, CP-09, CP-10, CP-12, MA-02, PL-08, PM-05, SA-08, SA-10, SA-15, SC-18							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
S2140, P3030, G950	PR.PS-01	4.5.CM-2	5.7.CM-2		1.1.1, 1.2.2, 6.4.1 - 6.4.4		CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.DS-P7

(CM-03) Configuration Change Control

Purpose

The purpose of the policy is to ensure organizations systematically manage changes to system configurations, including software updates, security patches, and operational modifications.

Scope
The policy applies to the Configuration Control Board, Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Configuration Control Board (CCB), Infrastructure Team, and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to establish a Change Control Board (CCB) The CCB are responsible for:

(a) Determining the types of changes to Systems that are configuration controlled
(b) Reviewing proposed configuration-controlled changes and approve or disapprove such changes with explicit consideration for security impact analyses
(c) Documenting configuration change decisions
(d) Implementing approved configuration-controlled changes
(e) Retaining records of configuration-controlled changes to the System for the life of the System
(f) Auditing and reviewing activities associated with configuration-controlled changes
(g) Coordinating and providing oversight for configuration change control activities through a configuration control board that convenes when configuration changes occur
(h) *Testing, Validation, and Documentation of Changes*: Testing, validating, and documenting changes to the System before implementing the changes on the operational System
(i) Infrastructure Team is prohibited from implementing a change without first obtaining pre-approval from the CCB and notifying all affected parties prior to the implementation of the change
(j) ITS' CISO personnel are required to represent cybersecurity topics as a representative of ITS' CCB
(k) After-System changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the System

Policy Mapping

ITS ISPM							
CA-07, CM-02, CM-04, CM-05, CM-06, CM-09, CM-11, IA-03, MA-02, PE-16, PT-06, RA-08, SA-08, SA-10, SC-28, SC-34, SC-37, SI-02, SI-03, SI-04, SI-07, SI-10, SR-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-07, PR.PS-01, DE.CM-01, DE.CM-09	4.5.CM-3	5.7.CM-3		6.4.5, 6.4.6		CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2

(CM-04) Impact Analysis

Purpose
The purpose of the policy is to ensure organizations assess the potential security and privacy risks associated with changes to their information systems.

Scope
The policy applies to the Infrastructure Team and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the Infrastructure Team, from a test environment, to:

(a) Analyze changes to the System to determine potential security and privacy impacts prior to change implementation

(b) *Verification of Controls*: After System changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the System

Policy Mapping

ITS ISPM							
CA-07, CM-03, CM-08, CM-09, MA-02, RA-03, RA-05, RA-08, SA-05, SA-08, SA-10, SI-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-07, PR.PS-01	4.5.CM-4	CM-04		6.4, 6.4.5, 6.4.5.1-6.4.5.4		PB, GV.MT-P1, GV.MT-P5, CT.DM-P9, PR.PO-P1, PR.PO-P2

(CM-05) Access Restrictions for Change

Purpose

The purpose of the policy is to ensure organizations define, document, approve, and enforce physical and logical access restrictions for system changes.

Scope

The policy applies to the Infrastructure Team, ITS Management, and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the Infrastructure Team to:

(a) Define, document, approve, and enforce physical and logical access restrictions associated with changes to the System

(b) *Privilege Limitation for Production and Operations*:

1. Limit privileges to change System components and System-related information within a production or operational environment
2. Review and reevaluate privileges semi-annually

(c) *Limit Library Privileges*: Limit privileges to change software archived within software libraries

(d) Configure Systems to prevent the installation of software and hardware components by non-administrators through limiting the actions that users can perform

(e) Configure Systems to enforce access restrictions and support auditing of the enforcement actions

(f) When dictated by a compensating control, develop, and implement a two-person rule for implementing changes to sensitive System components and System-level information

(g) With consultation from ITS Management:

1. Identify incompatible business roles
2. Limits privileges to change System components and System-related information within a production or operational environment
3. Implement steps to remediate incompatible business roles
4. Perform reviews, based on ITS' access permission review requirements

(h) *IRS-Defined*: Restrict administration of configurations to only authorized administrators

(i) *IRS-Defined*: Verify the authenticity and integrity of Basic Input/Output System (BIOS) or Unified Extensible Firmware Interface (UEFI) updates to ensure that the BIOS or UEFI is protected from modification out of the secure update process

Policy Mapping

ITS ISPM							
AC-03, AC-05, AC-06, CM-09, PE-03, SC-28, SC-34, SC-37, SI-02, SI-10							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4502	PR.PS-01	4.5.CM-5	5.7.CM-5		6.4.2, 6.4.4		PR.PO-P1

(CM-06) Configuration Settings

Purpose
The purpose of the policy is to establish and enforce security and privacy controls by defining, documenting, and maintaining secure configurations for information systems to mitigate risks and ensure compliance.

Scope
The policy applies to Infrastructure Team, Chief Information Security Officer (CISO), and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the Infrastructure Team with consultation from the CISO to:

(a) Establish and document configuration settings for components employed within the System that reflect the most restrictive mode consistent with operational requirements using established best practices and guidelines
(b) Implement approved configuration settings
(c) Identify, document, and approve any deviations from established configuration settings for Systems that receive, process, store, or transmit State Data based on explicit operational requirements
(d) Monitor and control changes to the configuration settings in accordance with agency-related policies and procedures

Policy Mapping

ITS ISPM							
AC-03, AC-19, AU-02, AU-06, CA-09, CM-02, CM-03, CM-05, CM-07, CM-11, CP-07, CP-09, CP-10, IA-03, IA-05, PL-08, PL-09, RA-05, SA-04, SA-05, SA-08, SA-09, SC-18, SC-28, SC-43, SI-02, SI-04, SI-06							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.PS-01, DE.CM-09	4.5.CM-6	5.7.CM-6				CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DP-P4, PR.PO-P1

(CM-07) Least Functionality

Purpose
The purpose of the policy is to ensure systems provide only the essential capabilities needed for their mission, restricting unnecessary functions, ports, protocols, software, and services to minimize security risks.

Scope
The policy applies to Infrastructure Team and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires all Systems to be configured with only essential capabilities. ITS utilizes the “principle of least privilege,” which states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary. The Infrastructure Team is required to:

(a) Configure the System to provide only mission essential capabilities
(b) Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services:
    1. Those not needed to conduct business
    2. Maintenance ports when not in use

3. File Transfer Protocol (FTP)

(c) *Periodic Review*:
1. Review the System annually to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services
2. Disable or remove identified functions, ports, protocols, and services within the information System deemed to be unnecessary and/or nonsecure

(d) *Authorized software – Allow by exception*:
1. Identify software programs authorized to execute on the System
2. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the System
3. Review and update the list of authorized software programs at a minimum annually

(e) *Prohibiting the use of unauthorized hardware*:
1. Identify ITS-defined hardware components authorized for System
2. Prohibit the use or connection of unauthorized hardware components
3. Review and update the list of authorized hardware components annually

(f) Periodically scan the state network to detect and remove any unauthorized or unlicensed software

Policy Mapping

ITS ISPM							
AC-03, AC-04, CM-02, CM-05, CM-06, CM-11, RA-05, SA-04, SA-05, SA-08, SA-09, SA-15, SC-02, SC-03, SC-07, SC-37, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4501, P4502, P4520, P4570	PR.PS-01, PR.PS-03, PR.PS-05	4.5.CM-7	5.7.CM-7		7.1.1 - 7.1.4, 7.2.2		PR.PO-P1, PR.PT-P2

(CM-08) System Component Inventory

Purpose
The purpose of the policy is to ensure organizations develop and maintain an accurate inventory of system components, including hardware, software, and firmware.

Scope
The policy applies to Business Operations (BusOps), Infrastructure Team, Network Operations (NetOps), Security Operations (SecOps), and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires BusOps, Infrastructure Team, and NetOps to:

(a) Develop, document, and maintain an inventory of System components that:
1. Accurately reflects the System
2. Includes all components within the System
3. Does not include duplicate accounting of components or components assigned to any other Systems
4. Is at the level of granularity deemed necessary for tracking and reporting
5. Includes the following information to achieve System component accountability: for example, hardware inventory specifications, software license information, software version numbers, component owners and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location
6. Information deemed necessary to achieve effective System component accountability

(b) Review and update the System component inventory at a minimum annually

(c) *Updates During Installation and Removal*: Update the inventory of System components as part of component installations, removals, and System updates

(d) *Automated unauthorized component detection*:

1. Detect the presence of unauthorized hardware, software, and firmware components within the System using automated mechanisms at all times
2. Take the following actions when unauthorized components are detected:
   i. Disable network access by such components
   ii. Isolate the components
   iii. Notify the CISO and CIO

Policy Mapping

ITS ISPM							
CM-02, CM-07, CM-09, CM-10, CM-11, CM-13, CP-02, CP-09, MA-02, MA-06, PE-20, PL-09, PM-05, SA-04, SA-05, SI-02, SR-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-01, ID.AM-02, PR.PS-01	4.5.CM-8	5.7.CM-8		2.4	164.310(d)(b)(iii)	ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3

(CM-09) Configuration Management Plan

Purpose

The purpose of the policy is to ensure organizations develop, document, and implement a structured approach to managing system configurations.

Scope

The policy applies to the Chief Operating Officer (COO), Chief Information Security Officer (CISO), and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the COO in conjunction with the CISO to develop, document, and implement a configuration management plan for all Systems that:

(a) Addresses roles, responsibilities, and configuration management processes and procedures
(b) Establishes a process for identifying configuration items throughout the System Development Lifecycle (SDLC) and for managing the configuration of the configuration items
(c) Defines the configuration items for the System and places the configuration items under configuration management
(d) Is reviewed and approved by the CIO and CISO
(e) Protects the configuration management plan from unauthorized disclosure and modification

Policy Mapping

ITS ISPM							
CM-02, CM-03, CM-04, CM-05, CM-08, PL-02, RA-08, SA-10, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-08, PR.PS-01	4.5.CM-9	5.7.CM-9		6.4		CT.PO-P2, PR.PO-P1

(CM-10) Software Usage Restrictions

Purpose

The purpose of the policy is to ensure organizations enforce policies governing the use of software and associated documentation, preventing unauthorized distribution, copyright violations, and security risks.

Scope

The policy applies to all software that is on the State network, the Chief Technology Officer (CTO), and Enterprise Architect (EA).

Policy

ITS policy assigns responsibility for software licensing to the CTO and EA, they must:

(a) Use software and associated documentation in accordance with contract agreements and applicable copyright laws
(b) Track the use of software and associated documentation protected by quantity licenses to control copying and distribution
(c) Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work
(d) *Open-source Software*: Only use open-source software that is legally licensed, approved for use by the CISO and adhere to a secure configuration baseline checklist from the U.S. Government or industry

Policy Mapping

ITS ISPM							
AC-17, AU-06, CM-07, CM-08, PM-30, SC-07, P.ITS-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.PS-01, DE.CM-03, DE.CM-09	4.5.CM-10	5.7.CM-10				

(CM-11) User-Installed Software

Purpose

The purpose of the policy is to ensure organizations establish policies governing software installation by users, enforce restrictions through procedural or automated methods, and monitor compliance to prevent unauthorized or malicious software installations.

Scope

The policy applies to the Chief Operating Officer (COO) and software that is installed by personnel outside of IT Operations.

Policy

ITS policy requires end-user software installation to be prohibited, and compliance monitored, through automated methods when practical. The COO must:

(a) Establish policies governing the installation of software by users
(b) Enforce software installation policies through procedural methods, automated methods, or both
(c) Monitor policy compliance at a minimum annually
(d) *FBI-Defined*: Monitor policy compliance through automated methods at least weekly

Policy Mapping

ITS ISPM							
AC-03, AU-06, CM-02, CM-03, CM-05, CM-06, CM-07, CM-08, PL-04, SI-04, SI-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.PS-01, PR.PS-02, DE.CM-03, DE.CM-09	4.5.CM-11	5.7.CM-11				

(CM-12) Information Location

Purpose

The purpose of the policy is to ensure organizations identify and document the physical and logical locations of information assets, supporting security, privacy, and compliance requirements.

Scope
The policy applies to all State personnel and all data classified as Level 1 and higher (State Data) that is received, processed, stored, accessed, protected, and/or transmitted (Handled) by ITS supported information systems (System/s).

Policy
This policy establishes that ITS must identify where data and associated information reside in the System components that compose agency Systems; and how information is being processed so that information flow can be understood, and adequate protection and policy management provided for such information and System components. ITS must:

(a) Identify and document the location of State Data and the specific System components on which the information is processed and stored
(b) Identify and document the users who have access to the System and System components where the State Data is Handled
(c) Document changes to the location (i.e., System or System components) where State Data is Handled
(d) *Automated Tools to Support Information Location*: Use automated tools to identify State Data on System components to ensure controls are in place to protect State Data and individual privacy

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-04, AC-06, AC-23, CM-08, PM-05, RA-02, SA-04, SA-08, SA-17, SC-04, SC-16, SC-28, SI-04, SI-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-07	4.5.CM-12	5.7.CM-12				ID.IM-P1, ID.IM-P7

(CM-13) Data Action Mapping

Purpose
The purpose of the policy is to ensure organizations develop and document a structured map of system data actions, particularly those involving personally identifiable information (PII).

Scope
The policy applies to all State personnel and all data classified as Level 2 and higher (State Data) that is received, processed, stored, accessed, protected, and/or transmitted (Handled) by ITS supported information systems (System/s).

Policy
This policy requires ITS to develop and document a map of system data actions.

Policy Mapping

ITS ISPM							
AC-03, CM-04, CM-12, PM-05, PM-27, PT-02, PT-03, RA-03, RA-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-07, ID.AM-08	4.5.CM-13					ID.IM-P1 ID.IM-P2, ID.IM-P3, ID.IM-P4, ID.IM-P5, ID.IM-P6, ID.IM-P7, ID.IM-P8, ID.RA-P1, ID.RA-P3, GV.MT-P1

(CM-14) Signed Components

Purpose

The purpose of the policy is to ensure organizations prevent the installation of software and firmware components unless they have been digitally signed using a certificate that is recognized and approved by the organization.

Scope

The policy applies to all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy prohibits the installation of ITS-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by ITS.

Policy Mapping

ITS ISPM							
CM-07, SC-12, SC-13, SI-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.5.CM-14					

(CP) Contingency Planning Family

(CP-01) Contingency Planning Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish, document, and disseminate contingency planning policies and procedures to maintain operational resilience.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all security and privacy contingency planning policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the contingency planning policy and procedures. The CISO along with must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level security and privacy contingency planning policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the security and privacy contingency planning policies and the associated security and privacy contingency planning family policies

(b) Review and update the current security and privacy contingency planning:
   1. Policies annually, following changes to ITS' system operating environment, when security incidents occur, or training simulations or exercises
   2. Procedures annually, following changes to ITS' system operating environment, when security incidents occur, or training simulations or exercises

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P2020, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, GV.SC-08, ID.IM-01, ID.IM-02, ID.IM-03, PR.IR-03	4.6.CP-1	5.18.CP-1			164.308(a)(7)(i) | 164.308(a)(7)(ii)	GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P7

(CP-02) Contingency Plan

Purpose
The purpose of the policy is to ensure organizations develop and implement a structured plan to maintain essential mission and business functions during system disruptions, compromises, or failures.

Scope
The policy applies to the Chief Information Officer (CIO), Chief Operating Officer (COO), and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the COO to establish, and implement, procedures to enable the continuation of critical business processes while operating in other than normal conditions. The COO must:

(a) Develop a contingency plan that:
1. Identifies essential missions and business functions and associated contingency requirements
2. Provides recovery objectives, restoration priorities, and metrics
3. Addresses contingency roles, responsibilities, assigned individuals with contact information
4. Addresses maintaining essential missions and business functions despite a System disruption, compromise, or failure
5. Addresses eventual, full System restoration without deterioration of the security safeguards originally planned and implemented
6. Addresses the sharing of contingency information
7. Is reviewed and approved by the CIO

(b) Distribute copies of the contingency plan to key contingency personnel, at a minimum
(c) Coordinate contingency planning activities with incident handling activities
(d) Review the contingency plan for the System annually
(e) Update the contingency plan to address changes to the organization, Systems, or environment of operation and problems encountered during contingency plan implementation, execution, or testing
(f) Communicate contingency plan changes to key contingency personnel
(g) Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training
(h) Protect the contingency plan from unauthorized disclosure and modification
(i) *Coordinate with Related Plans*: Coordinate contingency plan development with organizational elements responsible for related plans
(j) *Resume Mission and Business Functions*: Plan for the resumption of essential mission and business functions within an ITS-defined specified time-period of contingency plan activation
(k) *Identify Critical Assets*: Identify critical System assets supporting essential mission and business functions

Policy Mapping

ITS ISPM
CP-03, CP-04, CP-06, CP-07, CP-08, CP-09, CP-10, CP-11, CP-13, IR-04, IR-06, IR-08, IR-09, MA-06, MP-02, MP-04, MP-05, PL-02, PM-08, PM-11, SA-15, SA-20, SC-07, SC-23, SI-12

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2020, P4590, S6010	GV.OC-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04, PR.IR-02, PR.IR-03, RC.RP-03, RC.CO-04	4.6.CP-2	5.18.CP-2	2.4.CP-2		164.308(a)(7)(ii)(C) 164.312(a)(b)(ii)	GV.PO-P3, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4

(CP-03) Contingency Training

Purpose

The purpose of the policy is to ensure organizations provide training to personnel with contingency roles and responsibilities.

Scope

The policy applies to all State personnel identified in the contingency plan with responsibilities.

Policy

This policy requires ITS to:

(a) Provide contingency training to System users consistent with assigned roles and responsibilities:
1. Within thirty (30) days of assuming a contingency role and responsibility
2. When required by System changes

3. Annually thereafter

(b) Review and update contingency training content annually and following:

1. Contingency plan testing
2. Actual contingency (lessons learned)
3. Assessment or audit findings
4. Security incidents or breaches involving State Data
5. Changes in laws, executive orders, directives, regulations, policies, standards, and guidelines

Policy Mapping

ITS ISPM							
AT-02, AT-03, AT-04, CP-02, CP-04, CP-08, IR-02, IR-04, IR-09							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2020	PR.IR-03	4.6.CP-3	5.18.CP-3				GV.AT-P3

(CP-04) Contingency Plan Testing

Purpose

The purpose of the policy is to ensure organizations evaluate the effectiveness of their contingency plans and the readiness of personnel to execute them during system disruptions or emergencies.

Scope

The policy applies to the Chief Information Security Officer (CISO) and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS to conduct testing based on the requirements in ITS' contingency plan and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations.

The CISO must:

(a) Test the contingency plan for Systems at a minimum, annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan in accordance with:

1. NIST SP 800-84 Guide to Test, Training, and Exercise Process for IT Plans and Capabilities
2. NIST SP-34 Contingency Planning Guide for Federal Information Systems and other applicable guidance
3. ITS-defined tests and exercises

(b) Review the contingency plan test results

(c) Initiate corrective actions, if needed

(d) *Coordinate with Related Plans*: Coordinates contingency plan testing with organizational elements responsible for related plans

Policy Mapping

ITS ISPM							
AT-03, CP-02, CP-03, CP-08, CP-09, IR-03, IR-04, PL-02, PM-14, SR-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2020	ID.IM-02, PR.IR-03, RC.RP, RC.RP-03	4.6.CP-4	5.18.CP-4			164.308(a)(7)(ii)(D)	PR.PO-P3, PR.PO-P5, PR.PO-P8

(CP-05) Contingency Plan Update – WD

Policy Objective: Withdrawn: Incorporated into CP-02

(CP-06) Alternate Storage Site

Purpose
The purpose of the policy is to ensure organizations establish geographically distinct storage locations to maintain duplicate copies of critical information and data.

Scope
The policy applies to all backup information on supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to:

(a) Establish an alternative storage site, including necessary agreements to permit the storage and retrieval of System backup information

(b) Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site

(c) *Separation from Primary Site*: Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats

(d) *Recovery Time and Recovery Point Objectives*: Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives

(e) *Accessibility*: Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions

(f) *IRS-Defined*: If the System backup information contains data classified as Federal Tax Information (FTI), ensure that the alternative storage site provides information security safeguards that meet the IRS Publication 1075 November 2021 revision Section 2.B.6 Media Off-Site Storage Requirements

Policy Mapping

ITS ISPM							
CP-02, CP-07, CP-08, CP-09, CP-10, MP-04, MP-05, PE-03, SC-36, SI-13							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2020	PR.DS-11, PR.IR-03, PR.IR-04		5.18.CP-6			164.310(a)(b)(i)	PR.PO-P3

(CP-07) Alternate Processing Site

Purpose
The purpose of the policy is to ensure organizations establish geographically distinct processing sites to maintain essential mission and business functions during disruptions or failures at the primary site.

Scope
The policy applies to all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to:

(a) Establish an alternative processing site, including necessary agreements to permit the transfer and resumption of Systems for essential missions/business functions within the recovery period identified for the System (See CP-02) when the primary processing capabilities are unavailable

(b) Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the ITS-defined time period for transfer and resumption

(c) Provide controls at the alternate processing site that are equivalent to those at the primary site

(d) *Separation from Primary Site*: Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats
(e) *Accessibility*: Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions
(f) *Priority of Service*: Develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives)

Policy Mapping

ITS ISPM							
CP-02, CP-06, CP-08, CP-09, CP-10, MA-06, PE-03, PE-11, PE-12, PE-17, SC-36, SI-13							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2020	PR.IR-03, PR.IR-04		5.18.CP-7				PR.PO-P7, PR.PT-P4

(CP-08) Telecommunications Services

Purpose
The purpose of the policy is to ensure organizations establish alternate telecommunications services to maintain essential mission and business functions during disruptions to primary services.

Scope
The policy applies to the Chief Operating Officer (COO) and all State of Idaho telecommunications infrastructure.

Policy
This policy requires the COO to:

(a) Establish alternate telecommunications services, including necessary Service Level Agreement (SLA) to permit the resumption of critical communication Systems for essential mission and business functions within SLA defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage site
(b) *Priority of Service Provisions*:
    1. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives)
    2. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier
(c) *Single Points of Failure*: Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services

Policy Mapping

ITS ISPM							
CP-02, CP-06, CP-07, CP-11, SC-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2020, P3010	PR.IR-03, PR.IR-04		5.18.CP-8				PR.PT-P3, PR.PT-P4

(CP-09) System Backup

Purpose
The purpose of the policy is to ensure organizations conduct regular backups of critical system information, including user-level data, system-level data, and system documentation.

Scope
The policy applies to Chief Operating Officer (COO) and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the COO to:

(a) Conduct backups of user-level information contained in the System documentation, including security-related documentation, weekly
(b) Conduct backups of System-level information contained in the System weekly
(c) Conduct backups of System documentation, including security- and privacy- related documentation weekly
(d) Protect the confidentiality, integrity, and availability of backup information
(e) Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information
(f) *Testing for Reliability and Integrity*: Test backup information annually to verify media reliability and information integrity
(g) *Cryptographic Protection*: Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of State Data
(h) *IRS-Defined*: If the backup contains data classified as Federal Tax Information, the confidentiality of backup information at storage locations will be protected pursuant to Internal Revenue Code § 6103 Confidentiality and Disclosure of Returns requirements

Policy Mapping

ITS ISPM							
CP-02, CP-06, CP-10, MP-04, MP-05, SC-08, SC-12, SC-13, SI-04, SI-13							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2020	PR.DS-01, PR.DS-10, PR.DS-11, PR.IR-03, RC.RP-03	4.6.CP-9	5.18.CP-9			164.308(a)(7)(ii)(A)	PR.PO-P3

(CP-10) System Recovery and Reconstruction

Purpose
The purpose of the policy is to ensure organizations can recover and restore their systems to a known, secure state after disruptions, compromises, or failures.

Scope
The policy applies to Chief Operating Officer (COO) and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires the COO to:

(a) Provide for the recovery and reconstitution of the System to a known state within ITS-defined time period consistent with recovery time and recovery point objectives after a disruption, compromise, or failure
(b) *Transaction Recovery*: Implement transaction recovery for Systems that are transaction-based

Policy Mapping

ITS ISPM
AC-17, AU-06, CM-07, CM-08, PM-30, SC-07

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2020	PR.IR-03, RC.RP, RC.RP-01, RC.RP-02, RC.RP-05	4.6.CP-10	5.18.CP.10				PR.PO-P7

(CP-11) Alternate Communications Protocols – NR

Policy Objective: No Requirement.

(CP-12) Safe Mode – NR

Policy Objective: No Requirement.

(CP-13) Alternative Security Mechanisms – NR

Policy Objective: No Requirement.

(IA) Identification and Authentication Family

(IA-01) Identification and Authentication Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish, document, and disseminate identification and authentication policies and procedures to maintain secure access control.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all security and privacy identification and authentication policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the identification and authentication policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level security and privacy identification and authentication policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the security and privacy identification and authentication policies and the associated security and privacy identification and authentication family policies

(b) Review and update the current security and privacy identification and authentication:
   1. Policies annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data
   2. Procedures annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data

Policy Mapping

ITS ISPM							
AC-01, PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03, PR.AA-01	4.7.IA-1	5.6.IA-1		8.1		GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.AC-P1, PR.AC-P6

(IA-02) Identification and Authentication (Organizational Users)

Purpose
The purpose of the policy is to ensure organizations uniquely identify and authenticate users accessing their information systems.

Scope
The policy applies to the Service Desk, Infrastructure Team, State personnel, and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires:

(a) Service Desk to uniquely identify and authenticate personnel and associate that unique identification with processes acting on behalf of those users

(b) Implement multifactor authentication for:

1. Network access to privileged and non-privileged accounts
2. Local access to privileged and non-privileged accounts
3. Remote access to privileged and non-privileged accounts such that:
   i. One of the factors is provided by a device separate from the System gaining access
   ii. The device meets Authenticator Assurance Level 2 (AAL) per NIST SP 800-63-3

(c) *Access to Accounts – Replay Resistant*: Implement replay-resistant authentication mechanisms for network access to privileged accounts

(d) *Acceptance of PIV Credentials*: Accepts and electronically verifies Personal Identity Verification (PIV) compliant credentials

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-04, AC-14, AC-17, AC-18, AU-01, AU-06, IA-04, IA-05, IA-08, MA-04, MA-05, PE-02, PL-04, SA-04, SA-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4502, G560	PR.AA-01, PR.AA-03	4.7.IA-2	5.6.IA-2, 5.13.7.1, 5.13.7.2	2.5.IA-2	8.1.1, 8.2, 8.3, 8.3.1, 8.3.2		PR.AC-P1, PR.AC-P6

(IA-03) Device Identification and Authentication

Purpose

The purpose of the policy is to ensure organizations uniquely identify and authenticate devices before establishing connections, whether local, remote, or network-based.

Scope

The policy applies to all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires ITS to:

(a) Uniquely identify and authenticate devices before establishing a remote or network connection

(b) *Cryptographic Bidirectional Authentication*: Authenticate all devices before establishing remote network connection using bidirectional authentication that is cryptographically based

Policy Mapping

ITS ISPM							
AC-17, AC-18, AC-19, AU-06, CA-03, CA-09, IA-04, IA-05, IA-09, IA-11, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-01, PR.AA-03	4.7.IA-3	5.6.IA-3, 5.13.7.1, 5.13.7.2.1, 5.13.7.3				PR.AC-P1, PR.AC-P6

(IA-04) Identifier Management

Purpose

The purpose of the policy is to ensure organizations manage the lifecycle of identifiers (e.g., usernames, IDs) assigned to users, devices, or processes.

Scope

The policy applies to the Chief Operating Officer (COO), the Infrastructure Team, and all ITS supported information system (System/s) identifiers. Common device identifiers include, for example, media access control (MAC), Internet protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared System accounts (e.g., guest, and anonymous accounts).

Policy

ITS policy requires the Infrastructure Team to:

(a) Manage System identifiers by:
   1. Receiving authorization from the COO to assign or create an individual, group, role, service, device identifier, or account
   2. Selecting an identifier that identifies an individual, group, role, service, or device, in a manner, consistent with ITS-defined guidelines
   3. Assigning the identifier to the intended individual, group, role, service, or device, in a manner, consistent with ITS-defined guidelines
   4. Preventing reuse of identifiers indefinitely

(b) *Identify User Status*: Manage individual identifiers by uniquely identifying each individual with ITS-defined characteristics identifying individual status (e.g., Contractor)

(c) Archive inactive or terminated user credentials

(d) Develop and document the process for validating System users who request reinstatement of user credentials for those suspended or revoked

(e) Disable:
   1. Identifiers after ninety (90) days of inactivity
   2. Privileged accounts after sixty (60) days of inactivity
   3. Identifiers or accounts after an employee has separated

(f) Change default vendor-set or factory-set administrator accounts prior to implementation (e.g., during installation or immediately after installation)

Policy Mapping

ITS ISPM							
AC-05, IA-02, IA-03, IA-05, IA-08, IA-09, IA-12, MA-04, PE-02, PE-03, PE-04, PL-04, PM-12, PS-03, PS-04, PS-05, SC-37							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-01	4.7.IA-4	5.6.IA-4		8.1.1	164.312(a)(b)(i)	CT.DP-P2, PR.AC-P1, PR.AC-P6

(IA-05) Authenticator Management

Purpose

The purpose of the policy is to ensure organizations manage the lifecycle of authenticators, such as passwords, cryptographic devices, biometrics, and certificates.

Scope

The policy applies to the Infrastructure Team and all ITS supported information systems (System/s) authenticators.

Policy

ITS policy requires the Infrastructure Team to:

(a) Manage System authenticators by:
   1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator
   2. Establishing initial authenticator content for authenticators defined by ITS. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length)
   3. Ensuring that authenticators have sufficient strength of mechanism for their intended use

4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators
5. Changing default authenticators prior to first use
6. Changing or refreshing authenticators defined in standard
7. Protecting authenticator content from unauthorized disclosure and modification
8. Requiring individuals to take, and having devices implement, specific controls to protect authenticators
9. Changing authenticators for group/role accounts when membership to those account changes

(b) *Password-Based Authentication*:

1. Maintain a list of commonly used, expected, or compromised passwords and update the list every three (3) years and when ITS passwords are suspended to have been compromised directly or indirectly
2. Verify, when users create or update passwords, that the passwords are not found on the list of commonly used, expected, or compromised passwords in IA-05(b)
3. Transmit passwords only over cryptographically protected channels
4. Store passwords using an approved salted key derivation function, preferably using a key hash
5. Require immediate selection of a new password upon account recovery
6. Allow user selection of long passwords and passphrases, including spaces and all printable characters
7. Employ automated tools to assist the user in selecting strong password authenticators
8. Enforce the composition and complexity rules in ITS standard (S.IA-01) Authentication Requirements

(c) Authentication with password, multifactor, or public key-based follow (S.IA-01) Authentication Requirements

(d) *Change Authenticators Prior to Delivery*: Require developers/installers of System components to provide unique authenticators or change default authenticators prior to delivery/installation

(e) *Protection of Authenticators*: Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access

(f) *No Embedded Unencrypted Static Authenticators*: Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage

(g) *Biometric Authentication Performance*: For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements defined in NIST SP 800-63

Policy Mapping

ITS ISPM							
AC-03, AC-06, CM-06, IA-02, IA-04, IA-07, IA-08, IA-09, MA-04, PE-02, PL-04, SC-12, SC-13							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4503, S6030	PR.AA-01, PR.AA-03	4.7.IA-5	5.6.IA-5, 5.13.1.1	2.5.IA-5	8.2.1 - 8.2.6, 8.3.1, 8.3.2, 8.6	164.308(a)(5)(ii)(D)	PR.AC-P1, PR.AC-P6

(IA-06) Authenticator Feedback

Purpose

The purpose of the policy is to ensure organizations prevent information systems from providing feedback during authentication that could be exploited by attackers.

Scope

The policy applies to all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires all Systems to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Policy Mapping

ITS ISPM							
AC-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-01	4.7.IA-6	5.6.IA-6				

(IA-07) Cryptographic Module Authentication

Purpose
The purpose of the policy is to ensure organizations implement mechanisms to authenticate access to cryptographic modules.

Scope
The policy applies to Security Operations (SecOps) and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires SecOps to implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.

All electronic transmissions of FTI must be encrypted using FIPS 140-2 validated cryptographic modules. A product does not meet the FIPS 140-2 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information.

Policy Mapping

ITS ISPM							
AC-03, IA-05, SA-04, SC-12, SC-13							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-01, PR.AA-03	4.7.IA-7	5.6.IA-7, 5.10.1.2.1, 5.10.1.2.2				PR.AC-P1

(IA-08) Identification and Authentication (Non-Organizational Users)

Purpose
The purpose of the policy is to ensure organizations uniquely identify and authenticate non-organizational users (or processes acting on their behalf) before granting access to information systems.

Scope
The policy applies to all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires ITS to:

(a) Uniquely identify and authenticate non-agency personnel or processes acting on behalf of non-personnel (i.e., personnel are strictly prohibited from sharing accounts)

(b) *Acceptance of External Credentials*:

1. Accept only external authenticators that are NIST-compliant
2. Document and maintain a list of accepted external authenticators

(c) *Use of Defined Profiles*: Conform to the following profiles for identity management: NIST, FICAM-issued profiles, Security Assertion Markup Language (SAML), or OpenID Connect

(d) *IRS-Defined*: Deploy identification and authentication technology consistent with the results of the e-authentication risk analysis

Policy Mapping

ITS ISPM							
AC-02, AC-06, AC-14, AC-17, AC-18, AU-06, IA-02, IA-04, IA-05, IA-10, IA-11, MA-04, RA-03, SA-04, SC-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-01, PR.AA-03	4.7.IA-8	5.6.IA-8				CT.DP-P1, CT.DP-P3, PR.AC-P1, PR.AC-P6

(IA-09) Service Identification and Authentication

Purpose
The purpose of the policy is to ensure organizations uniquely identify and authenticate services before granting access to information systems.

Scope
The policy applies to the Hosting Team and web applications using digital certificates and services or applications that query a database.

Policy
ITS policy requires the Hosting Team to uniquely identify and authenticate ITS-defined system services and applications before establishing communications with devices, users, or other services or applications.

Policy Mapping

ITS ISPM							
IA-03, IA-04, IA-05, SC-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-01, PR.AA-03	4.7.IA-9					PR.AC-P1, PR.AC-P6

(IA-10) Adaptive Authentication – NR

Policy Objective: No Requirement.

(IA-11) Re-Authentication

Purpose
The purpose of the policy is to ensure organizations implement session-based authentication rules to strengthen access controls.

Scope
The policy applies to all State personnel and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires personnel to re-authenticate when:

(a) Systems have reached inactivity time limits or other circumstances that would cause a user to be logged out of their System

(b) Roles, authenticators, or credentials change
(c) Security categories of Systems change
(d) Execution of privileged functions occur
(e) Every twelve (12) hours

Policy Mapping

ITS ISPM							
AC-03, AC-11, IA-02, IA-03, IA-04, IA-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-01, PR.AA-03	4.7.IA-11	5.6.IA-11		8.1.8		PR.AC-P1, PR.AC-P6

(IA-12) Identity Proofing

Purpose
The purpose of the policy is to ensure organizations verify user identities through proofing mechanisms to establish legitimate access.

Scope
The policy applies to Human Resources (HR), new hires, and any person being issued credentials for accessing a supported information systems (System/s).

Policy
ITS policy requires the collection, validation, and verification of a user's identity information prior to issuing credentials for accessing a System. ITS must:

(a) Identity proof users that require accounts for logical access to Systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines
(b) Resolve user identities to a unique individual
(c) Collect, validate, and verify identity evidence
(d) *Supervisor Authorization*: Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization
(e) *Identity Evidence*: Require evidence of individual identification be presented to the registration authority
(f) *Identity Evidence Validation and Verification*: Require that the presented identity evidence be validated and verified through NIST SP 800-63 compliant methods of validation and verification
(g) *Address Confirmation*: Require that a registration code or notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record

Policy Mapping

ITS ISPM							
AC-05, IA-01, IA-02, IA-03, IA-04, IA-05, IA-06, IA-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-02	4.7.IA-12	5.6.IA-12				PR.AC-P1, PR.AC-P6

(IR) Incident Response Family

(IR-01) Incident Response Policies and Procedure

Purpose
The purpose of the policy is to ensure organizations establish and maintain incident response policies and procedures to guide effective incident management.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all security and privacy incident response policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the incident response policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to all State personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted State Data:
   1. An State level incident response policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the security and privacy incident response policies and the associated security and privacy incident response family policies

(b) Review and update the current incident response:
   1. Policies annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data
   2. Procedures annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4110, P4140, P4590, S6010	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, GV.SC-08, ID.IM-01, ID.IM-02, ID.IM-03, PR.IR-03, RC.RP-04	4.8.IR-1	5.3.IR-1	2.6.IR-1	11.1.2, 12.5.3, 12.10	164.308(a)(6)(i)	PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CM.AW-P7, PR.PO-P7

(IR-02) Incident Response Training

Purpose
The purpose of the policy is to ensure organizations provide training to personnel to prepare them for incident response activities.

Scope

The policy applies to the Chief Information Security Officer (CISO) and all State personnel who access the state network.

Policy

ITS policy requires the CISO to:

(a) Provide incident response training to users consistent with assigned roles and responsibilities:
   1. Within thirty (30) days of assuming an incident response role or responsibility or acquiring system access
   2. When required by system changes
   3. Annually thereafter

(b) Review and update incident response training content annually and following any security incidents involving unauthorized access to State Data or system used to handle State Data

(c) *Simulated Events*: Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations

(d) *Breach*: Provide incident response training on how to identify and respond to a breach, including ITS' process for reporting a breach

Policy Mapping

ITS ISPM							
AT-02, AT-03, AT-04, CP-03, IR-03, IR-04, IR-08, IR-09							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010	PR.IR-03	4.8.IR-2	5.3.IR-2	2.6.IR-2	12.10.4,		PB, GV.AT-P3, CM.AW-P7

(IR-03) Incident Response Testing

Purpose

The purpose of the policy is to ensure organizations test their incident response capabilities to validate effectiveness and readiness.

Scope

The policy applies to the Chief Information Security Officer (CISO), Computer Security Incident Response Team (CSIRT), and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the CISO and CSIRT to perform annual tests and/or exercises of its incident response capability to formally determine incident response effectiveness and make corrections, based on any deficiencies. The CSIRT must:

(a) Test the effectiveness of the incident response capability for the System annually using tabletop exercises at least annually

(b) *Coordination with Related Plans*: Coordinate incident response testing with agency elements responsible for related plans

(c) *Continuous Improvement*: Use qualitative and quantitative from testing to:
   1. Determine the effectiveness of incident response processes
   2. Continuously improve incident response processes
   3. Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format

(d) Include all personnel with significant Incident response capabilities, including those responsible for maintaining consolidated data centers and off-site storage, must be included in the tabletop exercise

(e) Produce an after-action report to improve the existing processes, procedures, and policies

Policy Mapping

ITS ISPM							
CP-03, CP-04, IR-02, IR-04, IR-08, PM-14							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.IM-02, PR.IR-03	4.8.IR-3	5.3.IR-3		12.10.2		PB, PR.PO-P5, PR.PO-P8

(IR-04) Incident Handling

Purpose

The purpose of the policy is to ensure organizations implement processes to handle incidents effectively and minimize impact.

Scope

The policy applies to the Chief Information Security Officer (CISO), Computer Security Incident Response Team (CSIRT), supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled), and the Incident Response process.

Policy

ITS policy requires the CSIRT:

(a) Implement an incident handling capability for incidents with the incident response plan and includes preparation, detection, analysis, containment, eradication, and recovery

(b) Coordinate incident handling activities with contingency planning activities

(c) Incorporate lessons learned from ongoing incident handling activities into Incident Response procedures, training, and testing/exercises, and implement the resulting changes accordingly

(d) Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across ITS

(e) *Automated Incident Handling Process*: Support the incident handling process using automated mechanisms

(f) *Insider Threats*: Implement an incident handling capability for incidents involving insider threats

(g) *Correlation with External Organizations*: Coordinate with contractors, data centers, counties, and other agencies to correlate and share incidents involving data classified as Level 2 and higher to achieve a cross-organization perspective on incident awareness and more effective incident responses

Policy Mapping

ITS ISPM							
AC-19, AU-06, AU-07, CM-06, CP-02, CP-03, CP-04, IR-02, IR-03, IR-06, IR-08, PE-06, PL-02, PM-12, SA-08, SC-05, SC-07, SI-03, SI-04, SI-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010	ID.IM-01, ID.IM-02, ID.IM-03, PR.IR-03, DE.AE-02, DE.AE-03, DE.AE-06, DE.AE-08, RS.MA, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02, RC.RP-01, RC.RP-02, RC.RP-06, RC.CO-03, RC.CO-04	4.8.IR-4	5.3.IR-4, 5.13.5	2.6.IR-4	12.10.1, 12.10.3, 12.10.5, 12.10.6		PB, GV.MT-P6, CM.AW-P7

(IR-05) Incident Monitoring

Purpose
The purpose of the policy is to ensure organizations monitor systems to detect and respond to incidents promptly.

Scope
The policy applies to the Chief Information Security Officer (CISO), Computer Security Incident Response Team (CSIRT), and all security incidents and breaches.

Policy
ITS policy requires the CSIRT to track and document all security incidents and breaches.

Policy Mapping

ITS ISPM							
AU-06, AU-07, IR-08, PE-06, PM-05, SC-05, SC-07, SI-03, SI-04, SI-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010	PR.IR-03, DE.AE-03, RS.MA-02, RS.MA-03, RS.MA-04	4.8.IR-5	5.3.IR-5		12.5.2, 12.10.5		PB

(IR-06) Incident Reporting

Purpose
The purpose of the policy is to ensure organizations report incidents to appropriate stakeholders in a timely manner.

Scope
The policy applies to the Chief Information Security Officer (CISO), Computer Security Incident Response Team (CSIRT), Service Desk, all State personnel, supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled), and all Security Incidents and Breaches.

Policy
ITS policy requires:

(a) All State personnel to report suspected security incidents to the Service Desk immediately but not to exceed one (1) hour after discovery

(b) The CSIRT:

1. Report incident information to mandated personnel/agencies within defined timelines
2. Report incidents using automated mechanisms
3. Report System vulnerabilities associated with reported incidents to designated agency personnel

(c) The CISO to provide incident information to the provider of the product or service and other agencies involved in the supply chain or supply chain governance for Systems or System components related to the incident

Policy Mapping

ITS ISPM							
CM-06, CP-02, IR-04, IR-05, IR-08, IR-09							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010	PR.IR-03, RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-06, RS.AN-07, RS.CO-	4.8.IR-6	5.3.IR-6		12.10.1	164.308(a)(6)(ii)	PB, CM.AW-P7

	02, RS.CO-03, RC.CO-03						

(IR-07) Incident Response Assistance

Purpose
The purpose of the policy is to ensure ITS provides incident response support and/or resources.

Scope
The policy applies to the Chief Information Security Officer (CISO), Computer Security Incident Response Team (CSIRT), and all security incidents and breaches.

Policy
ITS policy requires CISO to:

(a) Provide an incident response support resource, integral to ITS' incident response capability, which offers advice and assistance to users of the system for the handling and reporting of incidents

(b) Automation Support for Availability of Information and Support: Increase the availability of incident response information and support using automated mechanisms

(c) Coordinate with external providers:

1. Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability
2. Identify ITS' CSIRT to the external providers

Policy Mapping

ITS ISPM							
AT-02, AT-03, IR-04, IR-06, IR-08, PM-22, PM-26, SA-09, SI-18							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010	PR.IR-03, RS.MA, RS.MA-01, RS.MA-04, RS.CO-02, RS.CO-03	4.8.IR-7	5.3.IR-7				PB, CM.AW-P8, PR.PO-P7

(IR-08) Incident Response Plan

Purpose
The purpose of the policy is to ensure that there is a documented incident response plan (IRP).

Scope
The policy applies to ITS Management, the Chief Information Security Officer (CISO), Computer Security Incident Response Team (CSIRT), and all security incidents and breaches.

Policy
ITS policy requires the CISO and CSIRT to:

(a) Develop an incident response plan that:

1. Provides ITS with a roadmap for implementing its incident response capability
2. Describes the structure and organization of the incident response capability
3. Provides a high-level approach for how the incident response capability fits into the overall organization
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions
5. Defines reportable incidents
6. Provides metrics for measuring the incident response capability within the organization

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability
8. Addresses the sharing of incident information
9. Is reviewed and approved by designated agency officials at a minimum on an annual basis
10. Explicitly designates responsibility for incident response to ITS' CSIRT

(b) Distribute copies of the incident response plan to authorized incident response personnel and agency personnel with access to State Data

(c) Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing

(d) Communicate incident response plan changes to authorized incident response personnel and agency personnel with access to State Data

(e) Protect the incident response plan from unauthorized disclosure and modification

(f) Breaches: Include the following in the Incident Response Plan for breaches involving personally identifiable information:

1. A process to determine when notice to individuals or other organizations, including oversight organizations, is needed
2. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms
3. Identification of applicable privacy requirements

Policy Mapping

ITS ISPM							
AC-02, CP-02, CP-04, IR-04, IR-07, IR-09, PE-06, PL-02, SA-15, SI-12, SR-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010	ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04, PR.IR-03, DE.AE-03, DE.AE-08, RS.MA, RS.MA-01, RS.MA-05, RS.AN-08, RC.RP-01, RC.RP-02, RC.RP-04, RC.RP-06	4.8.IR-8	5.3.IR-8, 5.13.5	2.6.IR-8	12.8.3, 12.10, 12.10.1-12.10.6	164.308(a)(6)(ii)	PB, CM.AW-P7, PR.PO-P5, PR.PO-P6, PR.PO-P7

(IR-09) Information Spillage Response

Purpose

The purpose of the policy is to ensure ITS responds to information spillage.

Scope

The policy applies to the Computer Security Incident Response Team (CSIRT), and information spillage.

Policy

This policy requires CSIRT to respond to information spillage by:

(a) Assigning designated incident response agency personnel with responsibility for responding to information spills

(b) Identifying the specific information involved in the system contamination

(c) Alerting designated agency officials of the information spill using a method of communication not associated with the spill

(d) Isolating the contaminated system or system component

(e) Eradicating the information from the contaminated system or component

(f) Identifying other systems or system components that may have been subsequently contaminated

(g) Performing the following additional actions: Report incident information to personnel/agencies within defined timelines

Policy Mapping

ITS ISPM							
CP-02, IR-06, PM-26, PM-27, PT-02, PT-03, PT-07, RA-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-03, RS.MA	4.8.IR-9			12.10, 12.10.1-12.10.6		PR.PO-P7

(IR-10) Integrated Information Security Analysis – WD

Withdrawn: Moved to IR-04

(MA) Maintenance Family

(MA-01) Maintenance Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish, disseminate, and periodically review maintenance policies and procedures to support operational security.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all security and privacy maintenance policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the maintenance policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level security maintenance policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the security and privacy maintenance policies and the associated security and privacy maintenance family policies

(b) Review and update the current security and privacy maintenance:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.9.MA-1	5.16.MA-1			164.310(a)(b)(iv)	GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, ,GV.MT-P6 PR.MA-P1

(MA-02) Controlled Maintenance

Purpose
The purpose of the policy is to ensure organizations perform scheduled and controlled maintenance to prevent unauthorized access or risks during maintenance activities.

Scope
The policy applies to the Chief Information Officer (CIO) and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS to:

(a) Schedule, document, and review records of maintenance, repairs, and replacements on System components in accordance with manufacturer or vendor specifications and/or ITS requirements
(b) Approve and monitor all maintenance activities, whether performed on site or remotely and whether the System or System components are serviced on site or removed to another location
(c) Require the CIO to explicitly approve the removal of the System or System components from ITS facilities for off-site maintenance, repair, or replacement
(d) Sanitize Systems to remove all State Data from associated media prior to removal from ITS facilities for off-site maintenance, repair, or replacement
(e) Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions
(f) Include the following information in ITS' maintenance records:
    1. Component name
    2. Component serial number
    3. Date and time of maintenance
    4. Name of individual performing the maintenance including escort if required
    5. A description of the maintenance performed
    6. A list of equipment removed or replaced (including identification numbers, if applicable)

Policy Mapping

ITS ISPM							
CM-02, CM-03, CM-04, CM-05, CM-08, MA-04, MP-06, PE-16, SI-02, SR-03, SR-04, SR-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2030	ID.AM-08	4.9.MA-2	5.16.MA-2				PR.MA-P1

(MA-03) Maintenance Tools

Purpose

The purpose of the policy is to ensure organizations restrict the use of maintenance tools to prevent unauthorized access and protect data integrity during maintenance operations.

Scope

The policy applies to the Chief Information Security Officer (CISO) and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the CISO to:

(a) Approve, control, and monitor the use of System maintenance tools
(b) Review previously approved System maintenance tools on at least an annual basis
(c) *Inspect Tools*: Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications
(d) *Inspect Media*: Check media containing diagnostic and test programs for malicious code before the media are used in the System
(e) *Prevent the removal of maintenance equipment containing State Data by*:
    1. Verifying that there is no State Data on contained on the equipment
    2. Sanitizing or destroying the equipment
    3. Retaining the equipment within the facility
    4. Obtaining an exemption from a designated agency official(s) explicitly authorizing removal of the equipment from the facility
(f) *Restricted Tool Use*: Restrict the use of maintenance tools to authorized personnel only
(g) *Execution with Privilege*: Monitor the use of maintenance tools that execute with increased privilege

Policy Mapping

ITS ISPM							
MA-02, PE-16							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.PS-02	4.9.MA-3	5.16.MA-3				PR.MA-P1

(MA-04) Nonlocal Maintenance

Purpose
The purpose of the policy is to ensure organizations manage remote maintenance processes securely, avoiding risks associated with external access.

Scope
The policy applies to Security Operations (SecOps) and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires SecOps to:

(a) Approve and monitor nonlocal maintenance and diagnostic activities
(b) Allow the use of nonlocal maintenance and diagnostic tools only as consistent with ITS policy and documented in the security plan for the System
(c) Employ strong authenticator in the establishment of nonlocal maintenance and diagnostic sessions
(d) Maintain records for nonlocal maintenance and diagnostic activities
(e) Terminates session and network connections when nonlocal maintenance is completed
(f) *Logging and review*:
    1. Log events defined in AU-02(a) for nonlocal maintenance and diagnostic sessions
    2. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior
(g) *Authentication and Separation of Maintenance Sessions*: Protect nonlocal maintenance sessions by:
    1. Employing multifactor authentication consistent with NIST 800-63 Digital Identity Guidelines requirements
    2. Separating the maintenance sessions from other network sessions with the System by either:
        i. Physically separated communications paths
        ii. Logically separated communication paths
(h) *Cryptographic Protection*: Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: virtual private network (VPN) connection
(i) *Disconnect Verification*: Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-06, AC-17, AU-2, AU-03, IA-02, IA-04, IA-05, IA-08, MA-02, MA-05, PL-02, SC-07, SC-10							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.9.MA-4	5.16.MA-4		9.9.3		PR.MA-P2

(MA-05) Maintenance Personnel

Purpose
The purpose of the policy is to ensure organizations authorize maintenance personnel, verifying their qualifications to maintain system integrity.

Scope
The policy applies to the Chief Information Security Officer (CISO) and any personnel performing maintenance on ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the CISO to:

(a) Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel

(b) Verify the non-escorted personnel performing maintenance on the System possess the required access authorizations

(c) Designate State personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations

(d) *Non-System Maintenance*: Ensure that non-escorted personnel performing maintenance activities not directly associated with the System but in the physical proximity of the System, have required access authorizations

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-05, AC-06, IA-02, IA-08, MA-04, MP-02, PE-02, PE-03, PS-07, RA-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.9.MA-5	5.16.MA-5				PR.MA-P1

(MA-06) Timely Maintenance

Purpose
The purpose of the policy is to ensure organizations perform maintenance promptly to mitigate vulnerabilities and maintain system reliability.

Scope
The policy applies to the Chief Operating Officer (COO) and to all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the COO to obtain maintenance support and/or spare parts for security critical information System components and/or key information technology components within the recovery time objective/recovery point objective (RTO/RPO) timelines and maximum tolerable downtime (MTD) parameters agreed upon in the information Systems Information System Contingency Plan (ISCP).

Policy Mapping

ITS ISPM							
CM-08, CP-02, CP-07, RA-07, SA-15, SI-13, SR-02, SR-03, SR-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-08	4.9.MA-6	5.16.MA-6	8.6			PR.MA-P1

(MA-07) Field Maintenance – NR

Policy Objective: No Requirement.

(MP) Media Protection Family

(MP-01) Media Protection Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations develop, document, and implement media protection policies and procedures to safeguard sensitive information throughout its lifecycle.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all security and privacy media protection policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the media protection policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level media protection policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the security and privacy media protection policies and the associated security and privacy media protection family policies

(b) Review and update the current security and privacy media protection:
   1. Policies annually and following any security incidents involving digital and/or non-digital media
   2. Procedures annually and following any security incidents involving digital and/or non-digital media

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.10.MP-1	5.8.MP-1		9.5, 9.6	164.308(a)(4)(ii)(B)	PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PT-P1

(MP-02) Media Access

Purpose
The purpose of the policy is to ensure organizations restrict access to media containing sensitive information to authorized individuals to prevent unauthorized access or disclosure.

Scope
The policy applies ITS Management and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires ITS Management to restrict access to digital and non-digital media to only authorized individuals. State Data cannot be accessed by State employees, agents, representatives, contractors, or subcontractors located outside of the legal jurisdictional boundary of the United States (outside of the US, its territories, embassies, or military installations).

Policy Mapping

ITS ISPM							
AC-19, AU-09, CP-02, CP-09, CP-10, MA-05, MP-04, MP-06, PE-02, PE-03, SC-12, SC-13, SC-34, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1030		4.10.MP-2	5.8.MP-2	2.7.MP-2	9.7, 9.7.1	164.308(a)(4)(ii)(C)	PR.DS-P1, PR.PT-P1

(MP-03) Media Marking

Purpose

The purpose of the policy is to ensure organizations mark media containing sensitive information with appropriate labeling to indicate required handling or protection levels.

Scope

The policy applies to all State personnel and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires all State personnel to label media with the most restrictive data classification as is stored on the media.

(a) Mark System media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information. Any media that contains data classified as:
   1. High Risk:
      i. Contains Federal Tax Information (FTI) must be labeled as "FTI"
      ii. Does not contain FTI must be labeled "Level 3"
   2. Medium Risk, must be labeled "Level 2"
   3. Low Risk, must be labeled "Level 1"

(b) Exempt digital and non-digital media containing FTI or CJI from marking if the media remain within physically secure locations or ITS controlled areas

Refer to section (S.MP-01d) Classification Labeling requirements.

Policy Mapping

ITS ISPM							
AC-16, CP-09, MP-05, PE-22, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
G505, P4120, P4130		4.10.MP-3			9.6.1		PR.DS-P1, PR.PT-P1

(MP-04) Media Storage

Purpose

The purpose of the policy is to ensure organizations securely store media to prevent unauthorized access, loss, or damage during storage.

Scope

The policy applies to all State personnel and all ITS media that may store data classified as Level 1 and higher (State Data).

Policy

This policy requires State personnel to:

(a) Physically control and securely store digital and non-digital media containing State Data within physically secure locations or controlled areas and encrypt State Data on digital
(b) Protect system media types defined in MP-04(a) until the media are destroyed or sanitized using approved equipment, techniques, and procedures
(c) Ensure systems containing State Data are located, operated, and maintained by personnel physically located within the United States (this prohibits foreign remote maintenance, foreign call centers, help desks and the like)
(d) Conduct media inventories at least annually
(e) *IRS-Defined*: Data classified as Federal Tax Information, see IRS Publication 1075 Revision November 2021 - Section 2.B, Secure Storage—IRC 6103(p)(4)(B), on additional secure storage requirements

Refer to section (S.MP-01) Classifications requirements.

Policy Mapping

ITS ISPM							
AC-19, CP-02, CP-06, CP-09, CP-10, MP-02, MP-07, PE-03, PL-02, SC-12, SC-13, SC-28, SC-34, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
G550, P4130		4.10.MP-4	5.8.MP-4		9.5.1, 9.6.1, 9.6.2, 9.7.1	164.310(d)(b)(iv	PR.DS-P1, PR.PT-P1

(MP-05) Media Transport

Purpose

The purpose of the policy is to ensure organizations securely transport media to protect sensitive information during transit.

Scope

The policy applies to all State personnel and all ITS supported information systems (System/s) that may store data classified as Level 1 and higher (State Data).

Policy

ITS policy requires State personnel to:

(a) Protect and control digital and/or non-digital media containing State Data during transport outside controlled areas using agency defined safeguards in accordance with:
    1. (MP-04) Media Storage control requirements
    2. (SC-28) Protection of Data at Rest control requirements
(b) Maintain accountability for System media during transport outside of controlled areas
(c) Document activities with the transport of System media
(d) Restrict the activities associated with the transport of System media to authorized personnel
(e) *Custodians*: Employ an identified custodian during transport of System media outside of controlled areas
(f) Ensure State Data is not received, processed, stored, accessed, or transmitted to Systems located outside of the United States
(g) *IRS-Defined*: For FTI, See Section 2.B.4, FTI in Transit, for information on transmittals and media transport requirements

Refer to section (S.MP-01e) Data Transfer or Communication for proper requirements.

Policy Mapping

ITS ISPM							
AC-07, AC-19, CP-02, CP-09, MP-03, MP-04, PE-16, PL-02, SC-12, SC-13, SC-28, SC-34							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.10.MP-5	5.8.MP-5		9.6.1 - 9.6.3	164.310(d)(a)	PR.DS-P1, PR.PT-P1

(MP-06) Media Sanitization

Purpose

The purpose of the policy is to ensure organizations sanitize or destroy media containing sensitive information prior to disposal or reuse to prevent data leakage.

Scope

The policy applies to all State personnel and all system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include: digital media found in scanners, copiers, printers, notebook computers, workstations, network components, mobile devices; and non-digital media such as paper and microfilm.

Policy

This policy requires ITS to prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. ITS must:

(a) Sanitize digital and non-digital media containing State Data prior to disposal, release out of organizational control, or release for reuse using NIST 800-88, Guidelines for Media Sanitization approved sanitization techniques and procedures

(b) Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information

(c) *Review, Approve, Track, Document, and Verify*: Review, approve, track, document, and verify media sanitization and disposal actions

(d) Clear or purge any sensitive data from the system BIOS or UEFI before a computer system is disposed of and leaves the agency. Reset the BIOS or UEFI to the manufacturer's default profile, to ensure the removal of sensitive settings such as passwords or keys

(e) Media provided by foreign visitors (end users) may only be loaded into a standalone agency system. The system must remain standalone until such time as it is sanitized. Additionally, no other media loaded into the standalone system can be loaded into a non-standalone agency system until sanitized

(f) Assign one individual or department responsible for coordinating data disposal and reuse of equipment

(g) Train staff members on the security risks associated with the reuse of equipment that stored or processed sensitive information

(h) Destroy system media that cannot be sanitized, as follows:

1. Physical media (printouts and other physical media) must be disposed of by one of the following authorized means which includes thorough burning or shredding:
    i. When burning the data, the material must be burned in an incinerator that produces enough heat to burn the entire bundle, or the bundle must be separated to ensure that all pages are incinerated
    ii. When shredding the data, destroy paper using crosscut shredders which produce particles that are 1mm x 5mm (.04in. x .2in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 2.4mm (3/32in.) security screen
2. Electronic media (hard drives, tape cartridge, CDs, printer ribbons, flash drives, printer, and copier hard drives, etc.) must be disposed of by one of the following authorized means:

i. Overwriting (at least 3 times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located
ii. Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are weak and cannot effectively degauss magnetic media
iii. Destruction – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled

Refer to section (S.MP-01f) Disposal Methods and (S.MP-01g) Media Sanitation for proper requirements.

Policy Mapping

ITS ISPM							
AC-07, AC-19, CP-02, CP-09, MP-03, MP-04, PE-16, PL-02, SC-12, SC-13, SC-28, SC-34							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4530, G550, G540, S2140		4.10.MP-6	5.8.MP-6	2.7.MP-6	9.8, 9.8.1, 9.8.2	164.310(d)(b)(i), 164.310(d)(b)(ii)	PB, CT.PO-P2, CT.DM-P5, PR.DS-P1, PR.DS-P3

(MP-07) Media Use

Purpose
The purpose of the policy is to ensure organizations use media in approved environments to maintain the integrity and security of sensitive information.

Scope
The policy applies to Infrastructure Team, Security Operations (SecOps), and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to:
(a) Prohibit the use of personally owned media on agency Systems or System components
(b) Prohibit the use of portable storage devices in agency Systems when such devices have no identifiable owner
(c) *IRS-Defined*: Develop policy to disable all portable storage devices except for those required for explicit business need, which must be restricted to specific workstations or laptops. In the absence of an agency-developed and issued policy, the default policy is:
1. That the connection of non-agency portable storage devices is disallowed
2. Technical controls are implemented to enforce (e.g., implement data loss prevention software to limit the use of removeable media to known devices, blacklist USB-storage, prevent the mounting of USB storage, deny all access to all removable storage classes)

Policy Mapping

ITS ISPM							
AC-19, AC-20, PL-04, PM-12, SC-34, SC-41							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.10.MP-7	5.8.MP-7				PR.DS-P1, PR.PT-P1

(MP-08) Media Downgrading – NR

Policy Objective: No Requirement.

(PE) Physical and Environmental Protection Family

(PE-01) Physical and Environmental Protection Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish and maintain comprehensive physical and environmental protection policies and procedures.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all security and privacy physical and environmental protection policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level physical and environmental protection policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the security and privacy physical and environmental protection policies and the associated security and privacy physical and environmental protection family policies

(b) Review and update the current security and privacy physical and environmental protection:
   1. Policies annually and following any physical, environmental, or security related incidents involving State Data or systems used to handle State Data
   2. Procedures annually and following any physical, environmental, or security related incidents involving State Data or systems used to handle State Data

(c) Develop policy and procedures as needed to address their specific building access systems (e.g., restriction of physical access, identification and authentication and audit logging), that are critical to the security of a facility

(d) Develop and implement a clean desk policy for the protection of State Data (e.g., paper output, electronic storage media) to preclude unauthorized disclosures, see (S.PE-04) Clean Desk

(e) Designate restricted IT areas that house IT assets such as, but not limited to, mainframes, servers, controlled interface equipment, associated peripherals, and communications equipment

Policy Mapping

ITS ISPM							
AT-03, PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.11.PE-1	5.9.PE-1		9.1	164.310(a)(a)	GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P4, PR.AC-P2

(PE-02) Physical Access Authorizations

Purpose
The purpose of the policy is to ensure organizations authorize and document access to facilities housing systems.

Scope
The policy applies to ITS Management, all State personnel and facilities, and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled)

Policy
This policy requires ITS to enforce physical access authorizations to Systems in addition to the physical access controls for the facility where State Data is Handled by:

(a) Developing, approving, and maintaining a list of personnel with authorized access to ITS facilities where the System resides
(b) Issuing authorization credentials for facility access
(c) Reviewing the access list detailing authorized ITS facility access by individuals at least annually
(d) Removing individuals from the facility access list when access is no longer required

Policy Mapping

ITS ISPM							
AT-03, AU-09, IA-04, MA-05, MP-02, PE-03, PE-04, PE-05, PE-08, PM-12, PS-03, PS-04, PS-05, PS-06							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-06	4.11.PE-2	5.9.PE-2		9.2, 9.3, 9.4, 9.4.1	164.310(a)(b)(ii), 164.310(a)(b)(iii)	PR.AC-P2, PR.AC-P6

(PE-03) Physical Access Control

Purpose
The purpose of the policy is to ensure organizations enforce access controls at entry and exit points to secure facilities.

Scope
The policy applies to all State personnel and facilities that have supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to:

(a) Enforce physical access authorizations at entry/exit points to facilities where Systems that Handle State Data by:
    1. Verifying individual access authorizations before granting access to the facility
    2. Controlling ingress and egress to the facility using ITS-defined physical access control Systems or devices
(b) Maintain physical access audit logs ITS-defined entry/exit points
(c) Control access to areas within the facility designated as publicly accessible by implementing the following controls: ITS-defined physical access controls
(d) Escort visitors and control visitor activity in accordance with agency policies (e.g., personnel and physical security
(e) Secure keys, combinations, and other physical access devices
(f) Inventory ITS-defined physical access devices every twelve (12) months
(g) Change combinations and keys when:
    1. Keys are lost
    2. If combinations are compromised
    3. When individuals are transferred or terminated
    4. At least annually
(h) Issue visitors a physical token (e.g., a badge or access device) that:
    1. Identifies the visitors as not onsite personnel
    2. Must be surrendered before leaving the facility or at the date of expiration

3. Expires through automated or visual means (e.g., different color for each day)

(i) *Facility and Systems*: Perform security checks at a minimum daily at the physical perimeter of the facility or supported information System for exfiltration of information or removal of System components

(j) If the above conditions cannot be met, refer to the requirements listed in PE-17

Policy Mapping

ITS ISPM							
AT-03, AU-2, AU-06, AU-09, AU-13, CP-10, IA-03, IA-08, MA-05, MP-02, MP-04, PE-02, PE-04, PE-05, PE-08, PS-02, PS-03, PS-06, PS-07, RA-03, SC-28, SI-04, SR-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-06, DE.CM-02	4.11.PE-3	5.9.PE-3	2.9.PE-3	9.1, 9.1.1, 9.1.2, 9.2, 9.4.2, 9.4.3, 9.5, 9.5.1, 9.6	164.310(a)(b)(iv)	PR.AC-P2

(PE-04) Access Control for Transmission

Purpose

The purpose of the policy is to ensure organizations protect transmission lines within facilities from unauthorized access.

Scope

The policy applies to ITS Management and all State personnel and facilities that have supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS Management to control physical access to information System distribution and transmission lines within ITS facilities using physical security safeguards.

Policy Mapping

ITS ISPM							
AT-03, IA-04, MP-02, MP-04, PE-02, PE-03, PE-05, PE-09, SC-07, SC-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-06	4.11.PE-4	5.9.PE-4		9.1.2, 9.1.3		PR.AC-P2

(PE-05) Access Control for Output Systems

Purpose

The purpose of the policy is to ensure organizations secure output devices to prevent unauthorized access to sensitive information..

Scope

The policy applies to all State personnel and facilities.

Policy

This policy requires ITS to control physical access to output from output devices (e.g., monitors, printers, and audio devices) to prevent unauthorized individuals from obtaining the output.

Policy Mapping

ITS ISPM							
PE-02, PE-03, PE-04, PE-18							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-06	4.11.PE-5	5.9.PE-5				PR.AC-P2

(PE-06) Monitoring Physical Access

Purpose
The purpose of the policy is to ensure organizations monitor and review physical access to facilities to detect and respond to security incidents.

Scope
The policy applies to all ITS facilities where supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to:

(a) Monitor physical access to the facility where the System resides to detect and respond to physical security incidents
(b) Review physical access logs at a minimum monthly and upon occurrence of a potential indication of an event
(c) Coordinate results of reviews and investigations with the organizational incident response capability
(d) *Intrusion Alarms and Surveillance Equipment*: Monitor physical access to the facility where the System resides using physical intrusion alarms and surveillance equipment
(e) *IRS-Defined*: For FTI, See Section 2.B.3, Restricted Area Access, for additional information

Policy Mapping

ITS ISPM							
PE-02, PE-03, PE-04, PE-18							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010	PR.AA-06, DE.CM-02	4.11.PE-6	5.9.PE-6	2.9.PE-6			PR.AC-P2

(PE-07) Visitor Control – WD

Policy Objective: Withdrawn: Incorporated into PE-02 and PE-03

(PE-08) Visitor Access Records

Purpose
The purpose of the policy is to ensure organizations maintain and review visitor access records to identify anomalies.

Scope
The policy applies to all ITS facilities where supported information systems (System/s) reside.

Policy
This policy requires ITS to:

(a) Maintain visitor access records to the facility where Systems reside for five (5) years
(b) Review visitor access records at least monthly
(c) Report anomalies in visitor access records to agency defined personnel
(d) *Limit Personally Identifiable Information Elements*: Limit personally identifiable information (PII) contained in visitor access records to the minimum PII necessary to achieve the purpose for which it is collected

(e) *IRS-Defined*: For FTI, See Section 2.B.3.2, Authorized Access List (AAL) for visitor access requirements

Policy Mapping

ITS ISPM							
PE-02, PE-03, PE-06							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.AA-06	4.11.PE-8	5.9.PE-8		9.4.4		PB, CT.DP-P2, PR.AC-P2

(PE-09) Power Equipment and Cabling

Purpose
The purpose of the policy is to ensure organizations protect power equipment and cabling from damage or destruction.

Scope
The policy applies to Network Operation (NetOps) and all ITS supported information systems (System/s) and facilities where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires NetOps to protect power equipment and power cabling for the System from damage and destruction.

Policy Mapping

ITS ISPM							
PE-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-02		5.9.PE-9				PR.AC-P2

(PE-10) Emergency Shutoff

Purpose
The purpose of the policy is to ensure organizations provide the capability to quickly shut off power to systems or components during emergencies, while protecting the shutoff mechanisms from unauthorized activation.

Scope
The policy applies to all ITS supported information systems (System/s) and facilities where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to:

(a) Provide the capability of shutting off power to all information Systems in emergency situations
(b) Place emergency shutoff switches or devices in easily accessible locations to facilitate access for authorized personnel
(c) Protect emergency power shutoff capability from unauthorized activation

Policy Mapping

ITS ISPM

PE-15

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-02		5.9.PE-10				

(PE-11) Emergency Power

Purpose
The purpose of the policy is to ensure organizations provide uninterruptible power supplies or alternate power sources to maintain critical system operations during primary power source failures.

Scope
The policy applies to all ITS supported information systems (System/s) and facilities where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to provide an uninterruptible power supply to facilitate an orderly shutdown of the information System or transition of the information System to an alternate power source in the event of a primary power source loss.

Policy Mapping

ITS ISPM

AT-03, CP-02, CP-07

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-02		5.9.PE-11				PR.DS-P4, PR.PT-P4

(PE-12) Emergency Lighting

Purpose
The purpose of the policy is to ensure organizations provide and maintain automatic emergency lighting systems that activate during power outages, covering evacuation routes and critical areas within facilities.

Scope
The policy applies to all ITS supported information systems (System/s) and facilities where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to employ and maintain automatic emergency lighting for the System that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Policy Mapping

ITS ISPM

CP-02, CP-07

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-02		5.9.PE-12				

(PE-13) Fire Protection

Purpose

The purpose of the policy is to ensure organizations implement fire detection and suppression systems to safeguard personnel, facilities, and systems from fire-related hazards.

Scope

The policy applies to all ITS supported information systems (System/s) and facilities where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS to:

(a) Employ and maintain fire detection and suppression Systems that are supported by an independent energy source

(b) *Detection Systems – Automatic Activation and Notification*: Employ fire detection Systems that activate automatically and notify organizational personnel with physical and environmental protection responsibilities and police, fire, or emergency medical personnel in the event of a fire

Policy Mapping

ITS ISPM							
AT-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-02		5.9.PE-13				

(PE-14) Environmental Controls

Purpose

The purpose of the policy is to ensure organizations implement measures to monitor and regulate environmental factors, such as temperature and humidity, to protect systems and facilities from environmental hazards.

Scope

The policy applies to all ITS supported information systems (System/s) and facilities where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS to:

(a) Maintain adequate HVAC levels within the facility where the System resides at recommended System manufacturer levels

(b) Monitor environmental control levels continuously

Policy Mapping

ITS ISPM							
AT-03, CP-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-02		5.9.PE-14				

(PE-15) Water Damage Protection

Purpose

The purpose of the policy is to ensure organizations safeguard systems and facilities from water-related damage by implementing measures such as master shutoff valves, isolation mechanisms, and automated detection systems.

Scope
The policy applies to all ITS supported information systems (System/s) and facilities where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to protect the System from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Policy Mapping

ITS ISPM							
AT-03, PE-10							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-02		5.9.PE-15				

(PE-16) Delivery and Removal

Purpose
The purpose of the policy is to ensure organizations control and document the delivery and removal of system components to prevent unauthorized access, tampering, or loss during transit.

Scope
The policy applies to all ITS supported information systems (System/s) and facilities where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires ITS to:

(a) Authorize and control System components that Handle State Data entering and exiting the facility
(b) Maintain records of the System components

Policy Mapping

ITS ISPM							
CM-03, CM-08, MA-02, MA-03, MP-05, PE-20, SR-02, SR-03, SR-04, SR-06							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.11.PE-16	5.9.PE-16				PR.DS-P3

(PE-17) Alternate Work Site

Purpose
The purpose of the policy is to ensure organizations define, implement, and assess security controls at alternate work sites, enabling secure operations and communication during contingency scenarios.

Scope
The policy applies to ITS Management and all alternate work sites.

Policy
This policy requires ITS Management to:

(a) Determine and document ITS permitted alternate work sites allowed for use by employees
(b) Employ the following controls at alternative work sites:
    1. Limit access to the area during State Data processing times to only those personnel authorized by ITS to Handle State Data

2. Lock the area, room, or storage container when unattended
3. Position systems and documents containing State Data in such a way as to prevent unauthorized individuals from access and view
4. Follow the encryption requirements found in SC-13 and SC-28 for electronic storage (i.e., data-at-rest) of State Data

(c) Assess the effectiveness of security and privacy controls at alternate work sites

(d) Provide a means for employees to communicate with information security and privacy personnel in case of security or privacy incidents

Policy Mapping

ITS ISPM							
AC-17, AC-18, CP-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010		4.11.PE-17	5.9.PE-17				

(PE-18) Location of System Components – NR

Policy Objective: No Requirement

(PE-19) Information Leakage – NR

Policy Objective: No Requirement

(PE-20) Asset Monitoring and Tracking – NR

Policy Objective: No Requirement.

(PE-21) Electromagnetic Pulse Protection – NR

Policy Objective: No Requirement.

(PE-22) Component Marking – NR

Policy Objective: No Requirement.

(PE-23) Facility Location – NR

Policy Objective: No Requirement.

(PL) Planning Family

(PL-01) Planning Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish and maintain policies and procedures to guide security and privacy planning.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and agencies with a low, moderate, or high baseline, and all planning policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the planning policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level planning policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the planning policies and the associated planning family policies

(b) Review and update the current planning:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P2010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.12.PL-1	5.17.PL-1	2.10.PL-1	12.1, 12.2		PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6

(PL-02) System Security and Privacy Plans

Purpose
The purpose of the policy is to ensure that organizations develop and document security and privacy plans to comply with system requirements and goals.

Scope
The policy applies to Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Enterprise Architect (EA), and all State personnel identified, and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy assigns responsibility to the CISO, CTO, and EA to:

(a) Develop security and privacy plans for the System that:
1. Are consistent with ITS' enterprise architecture
2. Explicitly define the constituent System components
3. Describe the operational context of the System in terms of mission and business processes
4. Identify the individuals that fulfill System roles and responsibilities
5. Identify the information types processed, stored, and transmitted by the System
6. Provide the security categorization of the System, including supporting rationale
7. Describe any specific threats to the System that are of concern to the organization
8. Provide the results of a privacy risk assessment for Systems processing personally identifiable information
9. Describe the operational environment for the System and any dependencies on or connections to other Systems or System components
10. Provide an overview of the security and privacy requirements for the System
11. Identify any relevant control baselines or overlays, if applicable
12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions
13. Include risk determinations for security and privacy architecture and design decisions
14. Include security- and privacy-related activities affecting the System that require planning and coordination with authorized agency personnel
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation

(b) Distribute copies of the plans and communicate subsequent changes to the plans to authorized agency personnel

(c) Review the plans at a minimum annually (or as a result of a significant change)

(d) Update the plans to address changes to the System and environment of operation or problems identified during plan implementation or control assessments

(e) Protect the plans from unauthorized disclosure and modification

(f) *IRS-Defined*: Include or reference a plan for media sanitization and disposition that addresses all System media and backups in the agency's System security and privacy plans

Policy Mapping

ITS ISPM							
AC-02, AC-06, AC-14, AC-17, AC-20, CA-02, CA-03, CA-07, CM-09, CM-13, CP-02, CP-04, IR-04, IR-08, MA-04, MA-05, MP-04, MP-05, PL-07, PL-08, PL-10, PL-11, PM-01, PM-07, PM-08, PM-09, PM-10, PM-11, RA-03, RA-08, RA-09, SA-05, SA-17, SA-22, SI-12, SR-02, SR-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1070, P2010, P4130	ID.AM-03, ID.AM-08, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	4.12.PL-2	5.17.PL-2	2.10.PL-2			PB, PR.PO-P5

(PL-03) System Security Plan Update – WD

Withdrawn: Incorporated into PL-02

(PL-04) Rules of Behavior

Purpose

The purpose of the policy is to ensure organizations define and communicate acceptable use policies to promote responsible system use.

Scope

The policy applies to Human Resources (HR), the Chief Information Security Officer (CISO), Chief Operating Officer (COO), and all State personnel that have authorized access to the state network.

Policy

ITS policy assigns the CISO with cooperation with the COO and HR the responsibility to:

(a) Establish and provide individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy

(b) Receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system

(c) Review and update the rules of behavior at a minimum annually

(d) Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are revised or updated

(e) *Social Media and External Site/Application Usage Restrictions*: Include in the rules of behavior, restrictions on:

1. Use of social media, social networking sites, and external sites/applications
2. Posting organizational information on public websites
3. Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications

(f) *IRS-Defined*: Unless superseded by centrally issued cross-agency policy, establish usage restrictions and implementation guidance for using Internet-supported technologies (e.g., Instant messaging) based on the potential for these technologies to cause damage or disruption to the information system or the agency's accomplishment of its mission. Document the use of internet-supporting technologies

Refer to standard (S.PL-01) Rules of Behavior for defined requirements

Policy Mapping

ITS ISPM							
AC-02, AC-06, AC-08, AC-09, AC-17, AC-18, AC-19, AC-20, AT-02, AT-03, CM-11, IA-02, IA-04, IA-05, MP-07, PS-06, PS-08, SA-05, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P5040		4.12.PL-4	5.17.PL-4		12.3, 12.3.1, 12.3.2, 12.3.5-6, 12.3.10, 12.4	164.310(b)	PB

(PL-05) Privacy Impact Assessment – WD

Withdrawn: Incorporated into NIST SP 800-53 Appendix J, AR-2

(PL-06) Security Related Activity Planning – WD

Withdrawn: Incorporated into PL-02

(PL-07) Security Concept of Operations

Purpose

The purpose of the policy is to ensure organizations define an operational framework to meet mission objectives and maintain compliance.

Scope

The policy applies to the Chief Operation Officer (COO) and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires the COO to:

(a) Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy

(b) Review and update the CONOPS annually

Policy Mapping

ITS ISPM							
PL-02, SA-02, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2030							

(PL-08) Security and Privacy Architecture

Purpose

The purpose of the policy is to ensure organizations develop and maintain enterprise architecture to align systems with security and privacy objectives.

Scope

The policy applies to the Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Enterprise Architect (EA), and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy designates the CTO and EA in conjunction with the CISO responsible for:

(a) Developing security and privacy architectures for the System that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of State Data
2. Describe the requirements and approach to be taken for processing Personally Identifiable Information (PII) to minimize privacy risk to individuals
3. Describe how the architectures are integrated into and support the enterprise architecture
4. Describe any assumptions about, and dependencies on, external System and services

(b) Reviewing and updating the security architectures at a minimum annually to reflect changes in the enterprise architecture

(c) Reflecting planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, agency procedures, and procurements and acquisitions

(d) *Defense in Depth*: Designing the security and privacy architectures for the System using a defense-in-depth approach that:

1. Allocates System communication and other relevant controls to information Systems processing, storing, and transmitting State Data
2. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner

Policy Mapping

ITS ISPM							
CM-02, CM-06, PL-02, PL-07, PL-09, PM-05, PM-07, RA-09, SA-03, SA-05, SA-08, SA-17, SC-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1070, P2010	ID.AM-03	4.12.PL-8	5.17.PL-8		1.1.1 - 1.1.7		PB, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3, PR.PT-P4

(PL-09) Central Management

Purpose

The purpose of the policy is to ensure organizations implement centralized management to consistently apply controls across all systems.

Scope
The policy applies to the Chief Information Security Officer (CISO) and Policy Officer and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the ITS Information Security Policy Manual to be centrally managed by the Policy Officer in conjunction with the CISO.

Policy Mapping

ITS ISPM							
PL-02, PL-11, RA-02, RA-03, SA-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
			5.17.PL-9				

(PL-10) Baseline Selection

Purpose
The purpose of the policy is to ensure organizations identify and tailor appropriate security and privacy controls based on system impact levels to achieve compliance and operational objectives.

Scope
The policy applies to the Chief Operating Officer (COO) and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the COO to select a control baseline for all Systems where State Data is Handled.

Policy Mapping

ITS ISPM							
PL-08, PM-09							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
			5.17.PL-10				

(PL-11) Baseline Tailoring

Purpose
The purpose of the policy is to ensure organizations customize selected control baselines by applying defined tailoring actions to align security and privacy controls with their specific mission, business functions, and operational environments.

Scope
The policy applies to Chief Operating Officer (COO) and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy allows the COO to tailor the selected baseline to specialize or customize the controls that represent the specific needs and concerns of the agency.

Policy Mapping

ITS ISPM							
PL-10, RA-02, RA-03, RA-09, SA-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
			5.17.PL-11				

(PM) Program Management Family

(PM-01) Information Security Program Plan

Purpose
The purpose of the policy is to ensure organizations develop and maintain an information security program plan that outlines roles, responsibilities, and coordination among entities.

Scope
The policy applies to the Information Security Program Plan and the Chief Information Security Officer (CISO) and agencies with a low, moderate, or high baseline.

Policy
ITS policy designates the Chief Information Security Officer (CISO) office to:

(a) Develop and disseminate an ITS-wide information security program that:
1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements
2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance
3. Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical)
4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations

(b) Review the ITS-wide data Security Program Plan every three (3) years and following significant changes

(c) Protect the data Security Program Plan from unauthorized disclosure and modification

Policy Mapping

ITS ISPM							
PL-02, PM-18, PM-30, RA-09, SI-12, SR-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140, G501	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.13.PM-1	3.2.1		12.1	164.308(a)(1)(i) 164.316(a)-(b)	GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6

(PM-02) Chief Information Security Officer

Purpose
The purpose of the policy is to ensure organizations appoint a senior official to oversee and lead the information security program effectively.

Scope
The policy applies to ITS Executive Leadership.

Policy
This policy requires Executive Leadership to appoint a CISO. The CISO's authority and responsibilities are:

(a) Establishing, documenting, and distributing security policies and procedures

(b) Monitoring and analyzing security alerts and information

(c) Distributing and escalating security alerts to appropriate personnel
(d) Establishing, documenting, and distributing security incident response plan and escalation procedures to ensure timely and effective handling of all situations
(e) Managing and monitoring ITS' Cybersecurity Awareness Training Program
(f) Establishing a risk management program

Policy Mapping

ITS ISPM							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.RR-01, GV.RR-02	4.13.PM-2	3.2.1		12.5, 12.5.1 - 12.5.5	164.308(a)(2)	GV.PO-P3

(PM-03) Information Security and Privacy Systems

Purpose
The purpose of the policy is to ensure organizations allocate adequate resources to implement and sustain information security and privacy programs.

Scope
The policy applies to the Chief Technology Officer (CTO), Chief Financial Officer (CFO), Chief Information Security Officer (CISO) and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires establishing champions for information security and privacy efforts by:
(a) Including the resources needed to implement the information security and privacy programs in capital planning and investment requests and documenting all exceptions to this requirement
(b) Preparing documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, and standards
(c) Making available for expenditure, the planned information security and privacy resources

Policy Mapping

ITS ISPM							
PM-04, SA-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.RM-03, GV.RR-03, PR.IR-04	4.13.PM-3					PB, GV.PO-P2, GV.PO-P3, GV.PO-P6

(PM-04) Plan of Action and Milestones Process

Purpose
The purpose of the policy is to ensure organizations establish a process for developing and maintaining plans of action and milestones to address identified risks.

Scope
The policy applies to all management, operational, and technical security controls that are deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the control implementation).

Policy
This policy requires ITS to:

(a) Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:
   1. Are developed and maintained
   2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to ITS operations and assets, individuals, other organizations
   3. Are reported in accordance with established reporting requirements

(b) Review plans of action and milestones for consistency with ITS' risk management strategy and agency-wide priorities for risk response actions

Policy Mapping

ITS ISPM							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OV-03, ID.IM-02, ID.IM-03	4.13.PM-4	5.11.3				PB, ID.RA-P5, GV.MT-P4

(PM-05) System Inventory

Purpose
The purpose of the policy is to ensure organizations maintain an up-to-date inventory of information systems to support security and privacy management.

Scope
The policy applies to the Chief Technology Officer (CTO), Business Operations (BusOps), Service Desk, and all ITS supported information systems (System/s).

Policy
ITS policy requires BusOps and Service Desk in conjunction with the CTO to:

(a) Develop and update continually an inventory of ITS Systems

(b) *Inventory of Personally Identifiable Information*: Establish, maintain, and update continually an inventory of all ITS Systems, applications, and projects that process Personally Identifiable Information (PII)

Policy Mapping

ITS ISPM							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4520	ID.AM-01, ID.AM-02	4.13.PM-5			12.3.3, 12.3.4		PB, ID.IM-P1, ID.IM-P6, ID.RA-P1, GV.MT-P1

(PM-06) Measures of Performance

Purpose
The purpose of the policy is to ensure organizations develop and monitor performance measures to evaluate the effectiveness of security and privacy programs.

Scope
The policy applies to the Chief Information Security Officer (CISO).

Policy
ITS policy requires the CISO to develop, monitor, and report on the results of information security and privacy measures of performance.

Policy Mapping

ITS ISPM							
CA-07, PM-09							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OV-03					164.308(a)(8)	PB, PR.PO-P5

(PM-07) Enterprise Architecture

Purpose
The purpose of the policy is to ensure organizations integrate security and privacy considerations into enterprise architecture planning and implementation.

Scope
The policy applies to the Chief Technology Officer (CTO), Enterprise Architect (EA), and all information technology used by the State of Idaho.

Policy
ITS policy requires the CTO and EA to:

(a) Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to ITS operations and assets, individuals, other organizations

(b) *IRS-Defined*: Review and update the security enterprise architecture data based on the enterprise architecture timeframes

Policy Mapping

ITS ISPM							
AU-06, PL-02, PL-08, PM-11, RA-02, SA-03, SA-08, SA-17							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1070	ID.AM-03	4.13.PM-7					PB, GV.PO-P6, CT.DP-P1, CT.DP-P3

(PM-08) Critical Infrastructure Plan

Purpose
The purpose of the policy is to ensure organizations address security and privacy in critical infrastructure and key resources protection plans.

Scope
The policy applies to the Chief Operating Officer (COO), Chief Information Security Officer (CISO), Chief Technology Officer (CTO), and Chief Compliance Officer (CCO), and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the COO in conjunction with CISO, CTO, and CCO to address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Policy Mapping

ITS ISPM							
CP-02, CP-04, PE-18, PL-02, PM-09, PM-11, PM-18, RA-03, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy

	GV.OC-04, RC.RP-04				12.3	164.308(a)(8)	PB

(PM-09) Risk Management Strategy

Purpose
The purpose of the policy is to ensure organizations develop and implement a comprehensive risk management strategy for security and privacy.

Scope
The policy applies to the Chief Information Security Officer (CISO) and the ITS Risk Officer.

Policy
This policy requires the Risk Officer in conjunction with the CISO to:

(a) Develop a comprehensive strategy to manage:
   1. Security risk to ITS operations and assets, individuals, other organizations, and the State of Idaho associated with the operation and use of ITS systems
   2. Privacy risk to individuals resulting from the authorized processing of Personally Identifiable Information (PII)

(b) Implement the risk management strategy consistently across ITS

(c) Review and update the risk management strategy every three (3) years or as required, to address agency changes

Policy Mapping

ITS ISPM							
AC-01, AU-01, AT-01, CA-01, CA-02, CA-05, CA-06, CA-07, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PL-02, PM-02, PM-08, PM-18, PM-28, PM-30, PS-01, PT-01, PT-02, PT-03, RA-01, RA-03, RA-09, SA-01, SA-04, SC-01, SC-38, SI-01, SI-12, SR-01, SR-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-02, GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.OV-01, GV.OV-02, GV.SC-03, GV.SC-09, ID.RA-04, ID.RA-06, PR.IR-04, DE.AE-04, RC.RP-04	4.13.PM-9			12.2	164.308(a)(1)(ii)(B)	PB, ID.RA-P5, ID.DE-P2, GV.PO-P6, GV.RM-P1, GV.RM-P2

(PM-10) Authorization Process

Purpose
The purpose of the policy is to ensure organizations establish a formal process for authorizing information systems and services, assessing risks, and granting approval based on compliance with security and privacy requirements.

Scope
The policy applies to the Chief Information Security Officer (CISO) and Chief Operating Officer (COO).

Policy
ITS policy requires the CISO and COO to:

(a) Manage the security and privacy state of agency systems and the environments in which those systems operate through authorization processes

(b) Designate individuals to fulfill specific roles and responsibilities within the agency risk management process
(c) Integrate the authorization processes into an agency-wide risk management program

Policy Mapping

ITS ISPM							
CA-06, CA-07, PL-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.13.PM-10					PB, GV.PO-P6

(PM-11) Mission and Business Process Definition

Purpose
The purpose of the policy is to ensure organizations define their mission and business processes with consideration for security and privacy requirements, enabling the identification of protection needs and the integration of risk management strategies.

Scope
The policy applies to the Chief Information Security Officer (CISO) and Chief Operating Officer (COO).

Policy
ITS policy requires the CISO and COO to:
(a) Define ITS mission and business processes with consideration for information security and privacy and the resulting risk to ITS operations, ITS assets, individuals, and other agencies
(b) Determine information protection and personally identifiable information (PII) processing needs arising from the defined mission and business processes
(c) Review and revise the mission and business processes annually

Policy Mapping

ITS ISPM							
CP-02, PL-02, PM-07, PM-08, RA-02, RA-03, RA-09, SA-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-01, GV.OC-04, GV.OC-05, ID.RA-04, DE.AE-04, RC.RP-04						PB, ID.BE-P2, GV.PO-P6

(PM-12) Insider Threat Program

Purpose
The purpose of the policy is to ensure organizations establish a comprehensive program to detect, prevent, and respond to malicious insider activities by integrating technical and non-technical information, fostering cross-disciplinary collaboration, and adhering to applicable laws and privacy considerations.

Scope
The policy applies to the Threat Hunter Team (THT).

Policy
ITS policy designates the THT to implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Policy Mapping

ITS ISPM

AC-06, AT-02, AU-06, AU-07, AU-10, AU-12, AU-13, CA-07, IA-04, IR-04, MP-07, PE-02, PM-16, PS-03, PS-04, PS-05, PS-07, PS-08, SC-7, SC-38, SI-04, PM-14

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-03	4.13.PM-12					

(PM-13) Security and Privacy Workforce

Purpose
The purpose of the policy is to ensure organizations establish a workforce development program that equips personnel with the necessary skills, training, and awareness to effectively address security and privacy responsibilities.

Scope
The policy applies to the Chief Information Security Officer (CISO).

Policy
ITS policy requires the CISO to establish a security and privacy workforce development and improvement program.

Policy Mapping

ITS ISPM

AT-02, AT-03, S.AT-01

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.RR-02, GV.RR-04						PB, GV.PO-P3, GV.AT-P1, GV.AT-P2, GV.AT-P3

(PM-14) Testing, Training, and Monitoring

Purpose
The purpose of the policy is to ensure organizations implement a structured approach to evaluate security and privacy controls, provide relevant training to personnel, and continuously monitor systems to maintain compliance and mitigate risks.

Scope
The policy applies to the Chief Information Security Officer (CISO) and their designated representatives.

Policy
ITS policy requires the CISO to:

(a) Implement a process for ensuring that agency plans for conducting security and privacy testing, training, and monitoring activities associated with agency systems:
   1. Are developed and maintained
   2. Continue to be executed

(b) Review testing, training, and monitoring plans for consistency with the agency risk management strategy and agency-wide priorities for risk response actions

Policy Mapping

ITS ISPM

AT-02, AT-03, CA-07, CP-04, IR-03, PM-12, SI-04

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.13.PM-14					PB, GV.AT-P1, GV.MT-P3, PR.PO-P8

(PM-15) Security and Privacy Groups and Associations

Purpose
The purpose of the policy is to ensure organizations i establish and maintain contact with relevant security and privacy groups to facilitate ongoing education, stay updated on best practices, and share critical information about threats, vulnerabilities, and incidents.

Scope
The policy applies to the Chief Information Security Officer (CISO) and their designated representatives.

Policy
ITS policy assigns responsibility to the CISO to establish and institutionalize contact with selected groups and/or associations within the security and privacy communities to:

(a) Facilitate ongoing security and privacy education and training for organizational personnel
(b) Maintain currency with recommended security and privacy practices, techniques, and technologies
(c) Share current security and privacy information, including threats, vulnerabilities, and incidents

Policy Mapping

ITS ISPM							
SA-11, SI-05							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-02, DE.AE-06				5.1.2, 6.1 and 6.2	164.308(a)(5)(ii), (ii)(A)	GV.MT-P5, CM.AW-P2

(PM-16) Threat Awareness Program

Purpose
The purpose of the policy is to ensure organizations establish a process for managing insider threats to security and privacy.

Scope
The policy applies to the Chief Information Security Officer (CISO) and their designated representatives.

Policy
ITS policy assigns responsibility to the CISO and their designated representatives to implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

Policy Mapping

ITS ISPM							
IR-04, PM-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-02, ID.RA-03, ID.RA-05, DE.AE-03, DE.AE-06, DE.AE-07				12.6		

(PM-17) Protecting CUI on External Systems – NR

Policy Objective: No Requirement.

(PM-18) Privacy Program Plan

Purpose

The purpose of the policy is to ensure organizations develop and disseminate a comprehensive privacy program plan that outlines the structure, resources, roles, responsibilities, and strategic objectives of the privacy program, while addressing compliance with applicable privacy laws, regulations, and policies.

Scope
The policy applies to the Privacy Manager.

Policy
ITS policy assigns responsibility to the Privacy Manager:

(a) Develop and disseminate an ITS-wide privacy program plan that provides an overview of the agency's privacy program:
   1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program
   2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements
   3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities
   4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program
   5. Reflects coordination among organizational entities responsible for the different aspects of privacy
   6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations

(b) Update the plan every three (3) years and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments

Policy Mapping

ITS ISPM							
PM-08, PM-09, PM-19							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-02, GV.RM-06, GV.RM-07, GV.OV-01, GV.SC-03, ID.RA-06, DE.AE-04	4.13.PM-18					PB, GV.PO-P3, GV.PO-P4, GV.PO-P6

(PM-19) Privacy Program Leadership Role

Purpose
The purpose of the policy is to ensure organizations appoint a senior official with the authority, accountability, and resources to coordinate, develop, and implement privacy requirements while managing privacy risks across the organization.

Scope
The policy applies to ITS Executive Leadership.

Policy
This policy requires Executive Leadership to appoint a Privacy Manager with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the agency wide privacy program.

Policy Mapping

ITS ISPM							
PM-18, PM-20, PM-23, PM-24							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.RR-01, GV.RR-02, GV.OV-02, GV.SC-09	4.13.PM-19					PB, GV.PO-P3, GV.PO-P4, GV.PO-P6

(PM-20) Dissemination of Privacy Program Information

Purpose
The purpose of the policy is to ensure organizations provide accessible and transparent information about their privacy program, enabling public awareness, feedback, and engagement while maintaining compliance with privacy laws and regulations.

Scope
The policy applies to the Privacy Manager and Communications.

Policy
This policy requires the Privacy Manager, with consultation from Communications, to maintain a central resource webpage on the ITS' principal public website that serves as a central source of information about the ITS' privacy program and that:

(a) Ensures that the public has access to information about organizational privacy activities and can communicate with the Privacy Manager

(b) Ensures that organizational privacy practices and reports are publicly available

(c) Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices

(d) *Privacy Policies on Websites, Applications, and Digital Services*: Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that:

1. Are written in plain language and organized in a way that is easy to understand and navigate
2. Provide information needed by the public to make an informed decision about whether and how to interact with ITS
3. Are updated whenever ITS makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes

Policy Mapping

ITS ISPM							
AC-03, PM-19, PT-05, PT-06, PT-07, RA-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
							PB, GV.MT-P7, CM.PO-P1, CM.AW-P1, CM.AW-P2

(PM-21) Accounting of Disclosures

Purpose
The purpose of the policy is to ensure organizations maintain accurate records of disclosures of personally identifiable information, enabling transparency, compliance with privacy laws, and the ability to provide individuals with access to their disclosure history upon request.

Scope
The policy applies to the Chief Information Security Officer (CISO), Privacy Manager, legal, and Personally Identifiable Information (PII).

Policy

This policy requires the Privacy Manager, with consultation from the CISO and legal to:

(a) Develop and maintain an accurate accounting of disclosures of PII, including:
   1. Date, nature, and purpose of each disclosure
   2. Name and address, or other contact information of the individual or agency to which the disclosure was made

(b) Retain the accounting of disclosures for the length of the time the PII is maintained or five (5) years after the disclosure is made, whichever is longer

(c) Make the accounting of disclosures available to the individual to whom the PII relates upon request

Policy Mapping

ITS ISPM							
AC-03, AU-02, PT-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.13.PM-21					PB, CM.AW-P4, CM.AW-P6

(PM-22) Personally Identifiable Information Quality Management – NR

Policy Objective: No Requirement.

(PM-23) Data Governance Body

Purpose

The purpose of the policy is to ensure organizations establish a dedicated group responsible for developing, implementing, and overseeing policies, procedures, and standards that balance data utility with security and privacy requirements across the information lifecycle.

Scope

The policy applies to the ITS GRC team, Privacy Manager, and any other person assigned.

Policy

ITS policy requires:

(a) ITS to establish a Data Governance Body consisting of the GRC team and Privacy Manager

(b) The Data Governance Body responsibilities to be:
   1. Establishing policies, procedures, and standards that facilitate data governance
   2. Developing and implementing guidelines that support data:
      i. Modeling
      ii. Quality
      iii. Integrity
      iv. De-identification
   3. Review and approve applications to release data outside of ITS
   4. Archiving the applications and the released data
   5. Perform post-release monitoring to ensure that the assumptions made as part of the data release continue to be valid

Policy Mapping

ITS ISPM							
AT-02, AT-03, PM-19, PM-22, PM-24, PT-07, SI-04, SI-19							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.RR-01, GV.RR-02, ID.AM-08						GV.PO-P2, GV.PO-P6, CT.PO-P2

(PM-24) Data Integrity Board – NR

Policy Objective: No Requirement.

(PM-25) Minimization of PII Used in Testing, Training, and Research – NR

Policy Objective: No Requirement.

(PM-26) Complaint Management

Purpose

The purpose of the policy is to ensure organizations establish accessible mechanisms for receiving, tracking, and addressing complaints, concerns, or questions about their security and privacy practices, fostering transparency, accountability, and continuous improvement.

Scope

The policy applies to the Privacy Manager, Executive Leadership, and Communications.

Policy

This policy requires ITS to implement a process for receiving and responding to complaints, concerns, or questions from individuals about agency security and privacy practices that includes:

(a) Mechanisms that are easy to use and readily accessible by the public
(b) All information necessary for successfully filing complaints
(c) Tracking mechanisms to ensure all complaints received are reviewed and addressed within 10 business days of receipt
(d) Acknowledgement of receipt of complaints, concerns, or questions from individuals within 5 business days
(e) Response to complaints, concerns, or questions from individuals within 10 business days of receipt

Policy Mapping

ITS ISPM							
IR-07, IR-09, PM-22, SI-18							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
							PB, GV.MT-P7, CM.AW-P2

(PM-27) Privacy Reporting

Purpose

The purpose of the policy is to ensure organizations establish mechanisms for generating and sharing reports on privacy practices, risks, and compliance, fostering transparency, accountability, and informed decision-making. Reporting can also help organizations to determine progress in meeting privacy compliance requirements and privacy controls, track progress, discover vulnerabilities, identify gaps in policy and implementation, and identify areas of success.

Scope

The policy applies to the Privacy Manager and their designated officials.

Policy

This policy requires the Privacy Management to:

(a) Develop the State of Idaho Privacy Reporting and disseminate to:

1. The Idaho Technology Authority (ITA) to demonstrate accountability with statutory, regulatory, and policy privacy mandates
2. The ITS Administrator, Chief Information Security Officer (CISO) and other personnel with responsibility for monitoring privacy program compliance

(b) Review and update privacy reports biennially

Policy Mapping

ITS ISPM							
IR-09, PM-19							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
							PB, GV.MT-P4, CM.PO-P1

(PM-28) Risk Framing – NR

Policy Objective: No Requirement

(PM-29) Risk Management Program Leadership Roles

Purpose

The purpose of the policy is to ensure organizations appoint a senior accountable official for risk management and establish a risk executive function to oversee and align risk management activities across the organization, ensuring consistency with strategic, operational, and budgetary planning processes.

Scope

The policy applies to ITS Executive Leadership.

Policy

This policy requires Executive Leadership to:

(a) Appoint a Risk Officer to align ITS information security and privacy management processes with strategic, operational, and budgetary planning processes

(b) Establish a Risk Executive (function) to view and analyze risk from an agency wide perspective and ensure management of risk is consistent across the agency

Policy Mapping

ITS ISPM							
PM-02, PM-19							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.RR-01, GV.RR-02	4.13.PM-29					GV.PO-P3, GV.PO-P4

(PM-30) Supply Chain Risk Management Strategy

Purpose

The purpose of the policy is to ensure organizations develop, implement, and maintain a comprehensive strategy to identify, assess, and mitigate risks associated with the supply chain, addressing security and privacy concerns throughout the lifecycle of systems, components, and services.

Scope

The policy applies to Risk Officer, Chief Technology Officer (CTO), Privacy Manager, and all State personnel identified, and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS to:

(a) Develop an agency-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services

(b) Implement the supply chain risk management strategy consistently across ITS

(c) Review and update the supply chain risk management strategy annually or as required, to address organizational changes

(d) *Suppliers of Critical or Mission-essential Items*: Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services

Policy Mapping

ITS ISPM							
CM-10, PM-09, SR-01, SR-02, SR-03, SR-04, SR-05, SR-06, SR-07, SR-08, SR-09, SR-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-02, GV.OC-04, GV.OC-05, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.OV-01, GV.OV-02, GV.SC-01, GV.SC-03, GV.SC-09, ID.RA-06, DE.AE-04						ID.DE-P1

(PM-31) Continuous Monitoring Strategy – NR

Policy Objective: No Requirement

(PM-32) Purposing – NR

Policy Objective: No Requirement

(PS) Personnel Security Family

(PS-01) Personnel Security Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations develop, document, and disseminate personnel security policies and procedures to establish clear roles, responsibilities, and compliance measures.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and all security and privacy personnel and security policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the personnel security policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level personnel security policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the personnel security policies and the associated personnel security family policies

(b) Review and update the current personnel security:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.RR-04, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.14.PS-1	5.12				GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P9

(PS-02) Position Risk Designation

Purpose
The purpose of the policy is to ensure organizations assign risk designations to positions and establish screening criteria to mitigate personnel-related risks.

Scope
The policy applies to the Risk Officer, ITS Management, and Human Resources (HR).

Policy
ITS policy assigns responsibility to the Risk Officer, ITS Management, and HR for assessing the duties and responsibilities of a position to determine the degree of potential damage to the efficiency or integrity of the

service due to misconduct of an incumbent of a position and establishes the risk level of that position. The Risk Officer and HR must:

(a) Assign position risk designation to all ITS positions
(b) Establish screening criteria for individuals filling those positions
(c) Review and update position risk designations:
    1. Every three (3) years
    2. When recruitment actions are taken
    3. When position descriptions are rewritten

Policy Mapping

ITS ISPM							
AC-05, AT-03, PE-02, PE-03, PL-02, PS-03, PS-06, SA-05, SA-21, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.14.PS-2					PR.PO-P9

(PS-03) Personnel Screening

Purpose

The purpose of the policy is to ensure organizations screen individuals prior to granting access to systems and rescreen them under defined conditions to maintain security.

Scope

The policy applies to ITS Management and Human Resources (HR).

Policy

ITS policy assigns responsibility to ITS Management and HR for screening potential personnel prior to hiring in an effort to minimize the risk of compromise from internal sources. HR must:

(a) Screen individuals prior to authorizing access to the systems: Refer to section Refer to section (S.PS-01) Personnel Background Screening for minimum requirements
(b) Rescreen individuals in accordance with agency defined conditions requiring rescreening but no less than once every five (5) years

Policy Mapping

ITS ISPM							
AC-02, IA-04, MA-05, PE-02, PM-12, PS-02, PS-06, PS-07, SA-21							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.14.PS-3	5.12.1	2.8.PS-3	2.8.PS-03		PR.PO-P9, PR.AC-P6

(PS-04) Personnel Termination

Purpose

The purpose of the policy is to ensure organizations disable access, revoke credentials, and retrieve security-related property upon personnel termination to prevent unauthorized access.

Scope

The policy applies to ITS Management, Human Resources (HR), Service Desk, and all staff who access supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires upon termination of personnel ITS Management is required to:

(a) Disable System access accounts within twenty-four (24) hours of the termination action

(b) Terminate/revoke any authenticators/credentials associated with the individual
(c) Conduct an exit interview that includes appropriate information security topics and applicable, legally binding post-employment requirements for the protection of agency information
(d) Retrieve all ITS property
(e) Retain access to agency information and Systems formerly controlled by the terminated individual

Policy Mapping

ITS ISPM							
AC-02, IA-04, PE-02, PM-12, PS-06, PS-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.14-PS-4	5.12.2	2.8.PS-4	8.1.3, 9.3		PR.PO-P9

(PS-05) Personnel Transfer

Purpose
The purpose of the policy is to ensure organizations review and modify access authorizations when personnel are reassigned or transferred to maintain operational security.

Scope
The policy applies to ITS Management and Service Desk.

Policy
ITS policy requires upon transfer of personnel, ITS Management to do the following:
(a) Review and confirm ongoing operational need for current logical and physical access authorizations to systems/facilities when individuals are reassigned or transferred to other positions within the agency
(b) Initiate ITS-defined transfer or reassignment actions within five (5) days following the formal transfer action
(c) Modify access authorizations as needed to correspond with any changes in operational need due to reassignment or transfer
(d) Notify designated agency personnel within five (5) business days, as required

Policy Mapping

ITS ISPM							
AC-02, IA-04, PE-02, PM-12, PS-04, PS-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.14.PS-5	5.12.3				PR.PO-P9

(PS-06) Access Agreements

Purpose
The purpose of the policy is to ensure organizations develop, document, and verify access agreements to establish accountability for system access.

Scope
The policy applies to the Chief Operating Officer (COO) and all State personnel accessing supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
This policy requires the COO to:
(a) Develop and document access agreements for ITS Systems
(b) Review and update the access agreements, at least annually

(c) Verify that personnel requiring access to State Data and Systems:
1. Sign appropriate access agreements prior to being granted access
2. Re-sign access agreements to maintain access to ITS Systems when access agreements have been updated or at least annually

(d) *Classified Information Requiring Special Protection*:
1. Have a valid access authorization that is demonstrated by assigned official government duties
2. Satisfy associated personnel security criteria (PS-03) Personnel Screening
3. Have read, understood, and signed a nondisclosure agreement

(e) *Post-employment Requirements*:
1. Notify individuals of applicable, legally binding post-employment requirements for protection of agency information
2. Require individuals to sign an acknowledgement of these requirements, if applicable, as part of granting initial access to covered information

(f) *SSA-Defined*: SSA requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain SSA data

Policy Mapping

ITS ISPM							
AC-17, PE-02, PL-04, PS-02, PS-03, PS-06, PS-07, PS-08, SA-21, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.14.PS-6		2.8.PS-6			PB, PR.PO-P9, PR.DS-P5

(PS-07) External Personnel Security

Purpose
The purpose of the policy is to ensure organizations define and enforce personnel security requirements for external providers to align with organizational policies.

Scope
The policy applies to ITS' management, the Chief Information Security Officer (CISO), and all third-party personnel.

Policy
This policy requires ITS to:

(a) Establish personnel security requirements, including security roles and responsibilities for external providers

(b) Require external providers to comply with the ITS Information Security Policy Manual

(c) Documents personnel security requirements

(d) Require external providers to notify ITS of any personnel transfers or terminations of external personnel who possess ITS credentials and/or badges, or who have information system privileges within three (3) business days

(e) CISO will monitor provider compliance with personnel security requirements

(f) Grant access to external personnel only if they have:
1. Valid business needs
2. Valid access authorization
3. Read, understand, and signed a Non-Disclosure Agreement (NDA)
4. Read, understand, and signed an acknowledgment that they understand and will abide by ITS' policies, procedures, standards, and guidelines

Policy Mapping

ITS ISPM

AT-02, AT-03, MA-05, PE-03, PS-02, PS-03, PS-04, PS-05, PS-06, SA-05, SA-09, SA-21							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.RR-04, DE.CM-06	4.14.PS-7		2.8.PS-7			ID.DE-P5, GV.PO-P3, GV.AT-P4, PR.PO-P9

(PS-08) Personnel Sanctions

Purpose
The purpose of the policy is to ensure organizations employ a formal sanctions process for individuals who fail to comply with established information security and privacy policies, ensuring accountability and adherence to organizational standards.

Scope
The policy applies to ITS Management and Human Resources (HR).

Policy
This policy requires ITS Management and HR to:

(a) Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures

(b) Notify designated agency personnel within seventy-two (72) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction

Policy Mapping

ITS ISPM							
XX-1, PL-04, PM-12, PS-06, PT-01							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.14.PS-8	5.12.4				PR.PO-P9

(PS-09) Position Descriptions

Purpose
The purpose of the policy is to ensure organizations define and document position descriptions that include security and privacy responsibilities to align personnel roles with organizational objectives and compliance requirements.

Scope
The policy applies to Human Resources (HR), ITS Management, and the Chief Information Security Officer (CISO).

Policy
This policy requires ITS to incorporate security and privacy roles and responsibilities into agency position descriptions. Specification of these roles in individual agency position descriptions facilitates clarity in understanding the security and privacy responsibilities associated with the roles and the role-based security and privacy training requirements for the roles.

Policy Mapping

ITS ISPM							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.RR-04	4.14.PS-9					GV.PO-P3, PR.PO-P9

(PT) Personally Identifiable Information (PII) Processing and Transparency Family

(PT-01) PII Processing and Transparency Policies and Procedures

Purpose

The purpose of the policy is to ensure organizations develop, document, and disseminate policies and procedures for PII processing and transparency to address compliance and management commitments.

Scope

The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and all security and privacy PII processing and transparency policies and procedures.

Policy

ITS policy designates the CISO to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An agency level PII processing and transparency policies that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the PII processing and transparency policies and the associated security and privacy PII processing and transparency family policies

(b) Review and update the current security and privacy PII processing and transparency:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.15.PT-1	4.1				PB, ID.IM-P5, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CT.PO-P1, CT.PO-P3, CM.PO-P1, CM.PO-P2

(PT-02) Authority to Process PII

Purpose

The purpose of the policy is to ensure organizations determine and document the authority that permits the processing of PII and restrict processing to authorized purposes.

Scope

The policy applies to the Privacy Manager, Agency Legal, and all personnel who access supported information systems (System/s) where data classified as Personal Identification Information (PII) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires ITS to:

(a) Determine and document the authority that permits the processing of PII. Document authority in:
1. Privacy policies and notices
2. System of records notices
3. Privacy impact assessments
4. PRIVACT statements
5. Computer matching agreements and notices
6. Contracts
7. Information sharing agreements
8. Memorandum of Understanding
9. Internal Revenue Code § 6103
10. Or other documentation

(b) Restrict the handling of PII to only that which is authorized

Policy Mapping

ITS ISPM							
AC-02, AC-03, CM-13, IR-09, PM-09, PM-24, PT-01, PT-03, PT-05, PT-06, RA-03, RA-08, SI-12, SI-18							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-03	4.15.PT-2					PB, ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1

(PT-03) PII Processing Purposes

Purpose

The purpose of the policy is to ensure organizations identify, document, and restrict PII processing to purposes compatible with organizational privacy notices and policies.

Scope

The policy applies to the Privacy Manager and all personnel who access supported information systems (System/s) where data classified as Personal Identification Information (PII) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires the Privacy Manager to:

(a) Identify and document ITS defined purposes for processing PII
(b) Describe the purpose(s) in the public privacy notices and policies of ITS
(c) Restrict the processing of PII to only that which is compatible with the identified purpose(s)
(d) Monitor changes in processing PII and implement ITS defined mechanisms to ensure that any changes are made in accordance with the defined requirements

Policy Mapping

ITS ISPM							
AC-02, AC-03, AT-03, CM-13, IR-09, PM-09, PM-25, PT-02, PT-05, PT-06, PT-07, RA-08, SC-43, SI-12, SI-18							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1020	GV.OC-03		4.2.1, 4.2.2, 4.2.3				PB, ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1

(PT-04) Consent – NR

Policy Objective: No Requirement

(PT-05) Privacy Notice

Purpose

The purpose of the policy is to ensure organizations provide clear and accessible notices to individuals about the processing of their PII, including the authority and purposes for processing.

Scope

The policy applies to the ITS, Privacy Manager and all ITS supported information systems where Personally Identifiable Information (PII) is collected.

Policy

This policy requires ITS to provide notice to individuals about the processing of PII that:

(a) Is available to individuals upon first interacting with an organization, and subsequently at the time an individual is being asked to supply information that will become part of a system of record
(b) Is clear and easy-to-understand, expressing information about PII processing in plain language
(c) Identifies the authority that authorizes the processing of PII
(d) Identifies the purposes for which PII is to be processed
(e) Includes details on personal information and choice, access and correction of personal information, and contact information for comments and questions
(f) *Just-in-time Notice*: Present notice of personally identifiable information processing to individuals at a time and location where the individual provides PII or in conjunction with a data action, or to highlight specific changes that occurred since last presenting notice
(g) *Privacy Act Statements*: Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals

Policy Mapping

ITS ISPM							
PM-20, PM-22, PT-02, PT-03, PT-04, PT-07, RA-03, SC-42, SI-18							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-03						PB, CM.PO-P1, CM.AW-P1, CM.AW-P3

(PT-06) System of Records Notice – NR

Policy Objective: No Requirement

(PT-07) Specific Categories of PII

Purpose

The purpose of the policy is to ensure organizations identify and document specific categories of PII processed and implement measures to protect sensitive information.

Scope

The policy applies to the Privacy Manager, supported information systems (System/s) where data classified as Personal Identification Information (PII) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires the Privacy Manager to:

(a) Categorize PII by the requirements of laws, executive orders, directives, regulations, policies, standards, or guidelines

(b) Apply ITS-defined processing conditions for specific categories of PII defined by (PT-07)(a)

(c) *Social Security Numbers*: When a System Handles Social Security Numbers (SSN):

1. Eliminate unnecessary collection, maintenance, and use of SSNs, and explore alternatives to their use as a personal identifier
2. Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN
3. Inform any individual who is asked to disclose their SSN whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it

(d) *First Amendment Information*: Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity

Policy Mapping

ITS ISPM							
IR-09, PT-02, PT-03, RA-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-3		4.1, 4.3				PB

(PT-08) Computer Matching Requirements – NR

Policy Objective: No Requirement

(RA) Risk Assessment Family

(RA-01) Risk Assessment Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations develop, document, and maintain a risk assessment policy and procedures to manage risks effectively.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and all security and privacy risk assessment policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the risk assessment policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level risk assessment policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the security and privacy risk assessment policies and the associated security and privacy risk assessment family policies

(b) Review and update the current security and privacy risk assessment:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P2040, P4140, G215	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.16.RA-1	5.19.RA-1	2.11.RA-01	12.2		PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.PO-P6, GV.MT-P2, GV.MT-P6, PR.PO-P10

(RA-02) Security Classification

Purpose
The purpose of the policy is to ensure organizations classify information based on its sensitivity and potential impact to protect confidentiality, integrity, and availability effectively.

Scope
The policy applies to the Chief Information Security Officer (CISO), Privacy Manager, all personnel, and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires all State Data to be classified and Handled accordingly. State Data may only be disclosed to appropriate individuals and only to the extent allowed by the classification. A willful, unauthorized

disclosure of data will be prosecuted under all applicable statutes. If data is commingled, then the more restrictive classification must apply.

ITS must:

(a) Classify the System and data it Handles
(b) Document the security classification results, including supporting rationale, in the security plan for the System
(c) Verify that the ITS CISO reviews and approves the security classification decision

State personnel, in conjunction with the CISO, must classify all data as one of the following:

Classification Level 1 – "Unrestricted or Public" includes, but is not limited to, any information relating to the conduct or administration of the public's business prepared, owned, used, or retained by any state agency, independent public body corporate and politic or local agency regardless of physical form or characteristics. The agency's worst-case scenario for a breach of confidentiality, integrity, and availability is considered **low risk** (FIPS-199).

Classification Level 2 – "Limited or Private" includes sensitive information that may or may not be protected from public disclosure but if made easily and readily available may jeopardize the privacy or security of agency employees or individuals. The agency's worst-case scenario for a breach of confidentiality, integrity, or accessibility is considered **low risk** (FIPS-199).

Classification Level 3 – "Restricted or Confidential" includes PII, FTI, CJI, SSA, PCI, PHI, and sensitive information intended for agency use that may be exempted from public use and disclosure. Unauthorized disclosure may jeopardize the privacy or security of agency employees, organizations, or individuals. Direct access is limited to internal parties, authorized in the performance of their duties. External agencies requesting this information for authorized agency business must be under contractual obligation of confidentially or confidentiality with the disclosing agency (for example, confidentiality/non-disclosure agreement) prior to receiving the information. The agency's worst-case scenario for a breach of confidentiality, integrity, or accessibility is considered **medium risk** (FIPS-199).

Classification Level 4 – "Critical" includes extremely sensitive information. Information disclosure could potentially cause major damage or injury up to and including death to the named individual, or agency employees. The agency's worst-case scenario for a breach of confidentiality, integrity, or accessibility is considered **high risk** (FIPS-199).

Reference (S.MP-01) Classifications for more information.

Policy Mapping

ITS ISPM							
CM-08, MP-04, PL-02, PL-10, PL-11, PM-07, RA-03, RA-05, RA-07, RA-08, SA-08, SC-07, SC-38, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4120, P4130	ID.AM-05, ID.RA-04, ID.RA-05		5.19.RA-2		9.6.1		ID.RA-P4

(RA-03) Risk Assessment

Purpose

The purpose of the policy is to establish organizations conduct risk assessments to identify, analyze, and manage threats, vulnerabilities, and impacts to their information systems and operations effectively.

Scope

The policy applies to the Risk Officer and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the Risk Officer to conduct risk assessments at all three (3) levels in the risk management hierarchy (i.e., agency level, mission/business process level, and information System level), at any stage in the system development life cycle, and prior to System implementation. Risk assessments can also be conducted at various steps in the Risk Management Framework, including preparation, categorization, control selection, control implementation, control assessment, authorization, and control monitoring. The Risk Officer must:

(a) Conduct a risk assessment, including:
   1. Identifying threats to and vulnerabilities in the System
   2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the System, the State Data it Handles, and any related information
   3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of PII
   4. Document risks in a risk register with mitigation efforts

(b) Integrate risk assessment results and risk management decisions from ITS and mission or business process perspectives with System-level risk assessments

(c) Document risk assessment results in System security plans and risk assessment plans

(d) Review the risk assessment results at least annually

(e) Disseminate risk assessment results to the CISO and COO

(f) Update the risk assessment at least every three (3) years or when there are significant changes to the System, its environment of operation, or other conditions that may impact the security or privacy state of the System

(g) *Supply Chain Risk Assessment*:
   1. Assess supply chain risks associated with State Data
   2. Update the supply chain risk assessment every three (3) years, when there are significant changes to the relevant supply chain, or when changes to the System, environments of operation, or other conditions may necessitate a change in the supply chain

The risk assessment should take into account NIST SP 800-37 rev 1 - Guide for Applying the Risk Management Framework to Federal Information Systems.

Policy Mapping

ITS ISPM							
CA-03, CA-06, CM-04, CM-13, CP-06, CP-07, IA-08, MA-05, PE-03, PE-08, PE-18, PL-02, PL-10, PL-11, PM-08, PM-09, PM-28, PT-07, RA-02, RA-05, RA-07, SA-08, SA-09, SC-38, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2040, P2045 G215	GV.RM-06, GV.RM-07, GV.SC-03, GV.SC-09, GV.SC-10, ID.AM-05, ID.RA-01, ID.RA-03, ID.RA-04, ID.RA-05, ID.IM-01, ID.IM-02, ID.IM-03, DE.AE-07, RS.AN-08	4.16.RA-3	5.19.RA-3		6.1, 12.2	164.308(a)(1)(ii)(A) and (B)	PB, ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, PR.PO-P10

(RA-04) Risk Assessment Update – WD

Policy Objective: Withdrawn: Incorporated into RA-03

(RA-05) Vulnerability Monitoring and Scanning

Purpose

The purpose of the policy is to ensure ITS monitors for vulnerabilities.

Scope

The policy applies to Security Operations (SecOps) at the direction of the Chief Information Security Officer (CISO), and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy assigns responsibility to SecOps to:

(a) Monitor and scan for vulnerabilities in the System and hosted applications at a minimum of monthly for all Systems and when new vulnerabilities potentially affecting the Systems are identified and reported

(b) Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
1. Enumerating platforms, software flaws, and improper configurations
2. Formatting checklists and test procedures
3. Measuring vulnerability impact

(c) Analyze vulnerability scan reports and results from security control assessments

(d) Remediate legitimate vulnerabilities within the number of days listed:
1. Critical - fifteen (15) days
2. High – thirty (30) days
3. Medium – sixty (60) days
4. Low – ninety (90) days

(e) Share information obtained from the vulnerability scanning process and security control assessments with designated ITS officials to help eliminate similar vulnerabilities in other Systems (i.e., systemic weaknesses or deficiencies)

(f) Employ vulnerability scanning tools that include the capability to readily update the System vulnerabilities to be scanned

(g) *Update Vulnerabilities to Be Scanned*: Update the System vulnerabilities scanned at least every thirty (30) days; prior to a new scan, and when new vulnerabilities are identified and reported

(h) *Breadth and Depth of Coverage*: Define the breadth and depth of vulnerability scanning coverage

(i) *Discoverable Information*: Determine information about the System that is discoverable and take appropriate corrective actions

(j) *Privileged Access*: Implement privileged access authorization to selected System components in certain situations as required (such as when the nature of the vulnerability scanning may be more intrusive, or the System component subject to scanning may contain highly sensitive information)

(k) *Automated Trend Analyses*: Compare the results of multiple vulnerability scans using a (SIEM)

(l) *Review Historic Audit Logs*: Review historical audit logs to determine if identified vulnerabilities were exploited on ITS assets

(m) *Privileged Access*: Implement privileged access authorization to all System components for selected vulnerability scanning activities

(n) *IRS-Defined*: Implement a vulnerability management process for IT software Systems (including wireless networks) to complement their patch management process

(o) *PCI-Defined*: For assets within scope for PCI DSS, ITS is required to perform:
1. External network vulnerability scans via an approved scanning vendor (ASV), at least once every ninety (90) days or after any significant change in the network and include rescans until passing results are obtained, or all “High” vulnerabilities as defined in the PCI DSS are resolved
2. Internal network vulnerability scans at least once every ninety (90) days or after any significant change in the network and include rescans until passing results are obtained, or all “High” vulnerabilities as defined in the PCI DSS are resolved

Policy Mapping

ITS ISPM							
CA-02, CA-07, CA-08, CM-02, CM-04, CM-06, CM-08, RA-02, RA-03, SA-11, SA-15, SC-38, SI-2, SI-03, SI-04, SI-07, SR-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2040, P2045, P4520	GV.SC-10, ID.RA-01, ID.RA-08, ID.IM-01, ID.IM-02, ID.IM-03	4.16.RA-5	5.19.RA-5	2.11.RA-05	11.2, 11.2.1 - 11.2.3, 11.3		PR.PO-P10

(RA-06) Technical Surveillance Countermeasures Survey – NR

Policy Objective: No Requirement

(RA-07) Risk Response

Purpose

The purpose of the policy is to ensure organizations develop and implement strategies to address identified risks, including mitigation, acceptance, transfer, or avoidance, to safeguard their operations and assets effectively.

Scope

The policy applies to the Risk Officer, and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires the Risk Officer to respond to findings from security and privacy assessments, monitoring, and audits in accordance with agency risk tolerance.

Policy Mapping

ITS ISPM							
CA-05, IR-09, PM-04, PM-28, RA-02, RA-03, SR-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-05, GV.RM-01, GV.RM-03, GV.OV-01, GV.OV-02, GV.OV-03, GV.SC-03, GV.SC-09, GV.SC-10, ID.RA-05, ID.RA-06, ID.IM-01, ID.IM-02, ID.IM-03, RS.AN-08	4.16.RA-7	5.19.RA-7				PB, ID.RA-P5

(RA-08) Privacy Impact Assessments

Purpose

The purpose of the policy is to ensure organizations conduct Privacy Impact Assessments to evaluate the risks and impacts of collecting, using, and storing personal information, ensuring compliance with privacy regulations and safeguarding individual rights.

Scope

The policy applies to the Privacy Manager and ITS supported information systems (System/s) where personally identifiable information (PII) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires the Privacy Manager to conduct privacy impact assessments for Systems, programs, or other activities before:

(a) Developing or procuring information technology that processes (PII)
(b) Initiating a new collection of PII that:
    1. Will be processed using information technology
    2. Includes PII permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten (10) or more individuals, other than agencies, instrumentalities, or employees of the federal government

Policy Mapping

ITS ISPM							
CM-04, CM-09, CM-13, PT-02, PT-03, PT-05, RA-01, RA-02, RA-03, RA-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-04	4.16.RA-8					PB, ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.RA-P5, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, CM.PO-P1

(RA-09) Criticality Analysis

Purpose

The purpose of the policy is to ensure organizations perform criticality analysis to identify and prioritize essential system components, functions, and services, ensuring their protection aligns with mission objectives and operational needs.

Scope

The policy applies to the Chief Information Security Officer (CISO), Chief Operation Officer (COO) and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires the COO in conjunction with the CISO to identify critical System components and functions by performing a criticality analysis for information System components that Handle State Data at the planning, design, development, testing, implementation, and maintenance stages of the system development life cycle.

Policy Mapping

ITS ISPM							
CP-02, PL-02, PL-08, PL-11, RA-02, SA-08, SA-15, SR-05							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-04, GV.SC-04, GV.SC-07, ID.AM-05, ID.RA-04		5.19.RA-9				ID.BE-P3

(RA-10) Threat Hunting

Purpose

The purpose of the policy is to ensure organizations establish and maintain a cyber threat hunting capability to proactively detect, track, and disrupt threats that evade existing security controls, safeguarding their systems and operations effectively.

Scope

The policy applies to the Threat Hunter Team (THT) and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

This policy requires the THT to:

(a) Establish and maintain a cyber threat hunting capability to:
   1. Search for indicators of compromise in Systems
   2. Detect, track, and disrupt threats that evade existing controls

(b) Employ the threat hunting capability at ITS-defined frequency

Policy Mapping

ITS ISPM							
CA-02, CA-07, CA-08, RA-03, RA-05, RA-06, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	DE.AE-06, DE.AE-07						

(SA) System and Service Acquisition Family

(SA-01) System and Service Acquisition Policies and Procedures

Purpose

The purpose of the policy is to ensure organizations establish and maintain policies and procedures for effective system and service acquisition.

Scope

The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and all system and service acquisition policies and procedures.

Policy

ITS policy designates the CISO to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level system and service acquisition policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the system and service acquisition policies and the associated system and service acquisition family policies

(b) Review and update the current system and service acquisition:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PS-08, SA-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.17.SA-1					PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6

(SA-02) Allocation of Systems

Purpose

The purpose of the policy is to ensure organizations allocate sufficient resources to meet security and privacy requirements during system and service acquisition.

Scope

The policy applies to the Chief Information Security Officer (CISO), Chief Technology Officer (CTO), and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires all Systems to have sufficient funding to ensure the confidentiality and integrity of data and Systems commensurate with their defined risk level. System allocation for information security includes funding for the initial System or information System service acquisition and funding for the sustainment of the System/service. This is done by the CTO in conjunction with the CISO:

(a) CTO and CISO determine the high-level information security and privacy requirements for the System or System service in mission and business process planning
(b) CTO determine, document, and allocate the resources required to protect the System or System service as part of the ITS capital budget planning and investment control process
(c) CTO establish a discrete line item for information security and privacy in ITS programming and budgeting documentation

Policy Mapping

ITS ISPM							
PL-07, PM-03, PM-11, SA-09, SR-03, SR-05							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2010		4.17-SA-2	5.1.1 (2-6, 8)				PB, GV.PO-P2

(SA-03) System Development Lifecycle

Purpose

The purpose of the policy is to ensure organizations integrate security and privacy considerations throughout the system development life cycle (SDLC).

Scope

The policy applies to the Chief Technology Officer (CTO), Enterprise Architect (EA), Business Operations (BusOps), Application Development (AppDev), and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the CTO, EA, and BusOps for all significant development and/or acquisitions to:

(a) Acquire, develop, and manage Systems using a SDLC that incorporates information security and privacy considerations
(b) Define and document information security and privacy roles and responsibilities throughout the SDLC
(c) Identify personnel having information security and privacy roles and responsibilities
(d) Integrate ITS information security and privacy risk management process into SDLC activities
(e) *Use of Live or Operational Data*:
    1. Approve, document, and control the use of live data in preproduction environments for the System, System component, or System services
    2. Protect preproduction environments for the System, System components, System service at the same impact or classification level as any live data in use within the preproduction environment
(f) *Technology Refresh*: Plan for and implement a technology refresh schedule for the System throughout the SDLC

Policy Mapping

ITS ISPM							
AT-03, PL-08, PM-07, SA-04, SA-05, SA-08, SA-11, SA-15, SA-17, SA-22, SR-03, SR-04, SR-05, SR-09							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-08, PR.PS-06	4.17.SA-3			6.3		PB, GV.PO-P2, CT.PO-P4

(SA-04) Acquisition Process

Purpose

The purpose of the policy is to ensure organizations include security and privacy requirements in acquisition contracts for systems, components, and services.

Scope

The policy applies to the Chief Technology Officer (CTO), Enterprise Architect (EA), Business Operations (BusOps), and ITS supported information systems (System/s) or services being procured.

Policy

ITS policy requires the CTO, EA and BusOps to include the following requirements, descriptions, and criteria, explicitly or by reference, using ITS-defined contract language in the acquisition contract for the System, System component, or System service:

(a) Security and privacy functional requirements
(b) Strength of mechanism requirements
(c) Security and privacy assurance requirements
(d) Policies needed to satisfy
(e) Security and privacy documentation requirements
(f) Requirements for protecting security and privacy documentation
(g) Description of the system development environment and environment in which the System is intended to operate
(h) Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management
(i) Acceptance criteria
(j) The CTO must:

1. *Functional Properties of Controls*: Require the developer of the System, System component, or System service to provide a description of the functional properties of the policies to be implemented
2. *Design and Implementation Information for Controls*: Require the developer of the System, System component, or System service to provide design and implementation information for the policies that includes:
    i. Security-relevant external System interfaces
    ii. High-level design
    iii. Low-level design
    iv. Source code or hardware schematics
    v. ITS-defined design and implementation information for the security policies to be employed at sufficient level of detail to permit analysis and testing of policies
3. *Continuous Monitoring Plan for Controls*: Require the developer of the System, System component, or System service to produce a plan for continuous monitoring of policy effectiveness that is consistent with the continuous monitoring program of the agency
4. *Functions, Ports, Protocols and Services in Use*: Require the developer of the System, System component, or System service to identify the functions, ports, protocols, and services intended for agency use
5. *Data Ownership*:
    i. Include agency data ownership requirements in the acquisition contract
    ii. Require all data to be removed from the contractor's System and returned to ITS within seven (7) calendar days prior to contract termination
6. *IRS-Defined*: Information Systems that receive, process, store, access, protect and/or transmit State Data must be located, operated, and accessed within the United States. When a contract developer is used, agencies must document, through contract requirements, that all Systems (i.e., beyond commercial products used as components) are located within the United States and

are developed physically within the United States by United States citizens or those with lawful resident status

7. *IRS-Defined*: In acquiring information technology, agencies must use common security configurations, when applicable, by:
   i. Requiring vendors to configure IT with common security configurations (when available and applicable, e.g., Center for Internet Security benchmarks) prior to delivery
   ii. Configuring acquired IT to meet agency-tailored, secure parameters (e.g., configurations that meet Publication 1075 and applicable SCSEM requirements) after delivery but prior to deployment. Agencies do not need to require that vendors securely configure IT for delivery
8. Employ only information technology products on the FIPS 201-approved products list for PIV-I capability implemented within Systems

Policy Mapping

ITS ISPM							
CM-06, CM-08, PS-07, SA-03, SA-05, SA-08, SA-11, SA-15, SA-16, SA-17, SA-21, SR-03, SR-05							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10, ID.AM-08, ID.RA-09, ID.IM-03, DE.CM-06	4.17.SA-4	5.1.1 (2-6, 8), 5.7.1.1				PB, ID.DE-P3, CT.PO-P4

(SA-05) System Documentation

Purpose
The purpose of the policy is to ensure organizations obtain or develop documentation that supports secure system configuration, operation, and maintenance.

Scope
The policy applies to the Chief Technology Officer (CTO), Enterprise Architect (EA), and supported information systems (System/s) and/or services being procured.

Policy
ITS policy requires the CTO and EA on all Systems and/or services being procured to:

(a) Obtain or develop administrator documentation for the System, System component, or System service that describes:
   1. Secure configuration, installation, and operation of the System, component, or service
   2. Effective use and maintenance of security and privacy functions and mechanisms
   3. Known vulnerabilities regarding configuration and use of administrative or privileged functions

(b) Obtain or develop user documentation for the System, System, System component, or System service that describes:
   1. User-accessible security and privacy functions and mechanisms and how to effectively use those security functions and mechanisms
   2. Methods for user interaction, which enable individuals to use the System, component, or service in a more secure manner and protect individual privacy
   3. User responsibilities in maintaining the security of the System, component, or service and privacy of individuals

(c) Document attempts to obtain System, component, or service documentation when such documentation is either unavailable or nonexistent and take ITS-defined actions (e.g., recreates documentation that is essential to the effective implementation or operation of security policies) in response

(d) Distribute documentation to designated agency officials

Policy Mapping

ITS ISPM							
CM-04, CM-06, CM-07, CM-08, PL-02, PL-04, PL-08, PS-02, SA-03, SA-04, SA-08, SA-09, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-02, ID.RA-09	4.17-SA-5	5.7.2				

(SA-06) Software Usage Restrictions – WD

Policy Objective: Withdrawn: Incorporated into CM-10 and SI-7

(SA-07) User Installed Software – WD

Policy Objective: Withdrawn: Incorporated into CM-11 and SI-7

(SA-08) Security and Privacy Engineering Principals

Purpose

The purpose of the policy is to ensure organizations apply security and privacy engineering principles in system design and development.

Scope

The policy applies to the Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Enterprise Architect (EA), and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the CTO and EA, in conjunction with the CISO to:

(a) Apply the following Systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the System and System components: ITS-defined systems security and privacy engineering principles

(b) *Minimization*: Implement the privacy principle of minimization using ITS-defined processes

Policy Mapping

ITS ISPM							
PL-08, PM-07, RA-02, RA-03, RA-09, SA-03, SA-04, SA-15, SA-17, SA-20, SC-02, SC-03, SC-32, SC-39, SR-02, SR-03, SR-04, SR-05							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
G530, G509A	ID.AM-08, ID.IM-01 ID.IM-02, ID.IM-03, PR.DS-10, PR.PS-06, PR.IR-03	4.17.SA-8			2.2		CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5

(SA-09) External Information Systems Services

Purpose

The purpose of the policy is to ensure organizations manage risks associated with external system services through agreements and monitoring.

Scope

The policy applies to the Chief Technology Officer (CTO), Chief Information Security Officer (CISO), Risk Officer, and external information systems where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled)

Policy

This policy requires ITS to: The CISO in conjunction with the CTO is required to:

(a) Require the providers of external services to comply with ITS security and privacy requirements and employ the following controls: the security and privacy requirements contained within this manual and applicable state and federal laws, Executive Orders, directives, policies, regulations, standards, and established service-level agreements

(b) Define and document ITS oversight and user roles and responsibilities with regard to external system services

(c) Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: continuous monitoring activities (e.g., perform internal inspections, complete self-assessments using SCSEM, perform automated configuration compliance scans, etc.)

1. *Risk Assessments and Organizational Approvals*: Conduct an organizational assessment of risk prior to the acquisition of outsourcing of information security services
2. Verify that the acquisition or outsourcing of dedicated information security services is approved by a designated agency official

(d) *Identification of Functions, Ports, Protocols and Services*: Require providers of external information system services that Handle State Data to identify the functions, ports, protocols, and other services required for the use of such services

(e) *Establish and Maintain Trust Relationship with Providers*: Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: ITS ISPM requirements for information systems that Handle State Data

(f) *Processing, Storage and Service Location*: Restrict the location of handling State Data to the United States and territories

(g) *Organization-Controlled Cryptographic Keys*: Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system

(h) *Processing and Storage Location – U.S. Jurisdiction*: Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States

(i) Maintain written and executed agreements with business partners to ensure:

1. Appropriate management, operational and technical control safeguards are in place to ensure the confidentiality, integrity, and availability of State Data the business associate creates, receives, maintains, or transmits
2. Service providers acknowledge in writing that they are responsible for the security of State Data (e.g., cardholder data) that the service provider possesses, stores, or transmits on behalf of ITS, or to the extent that they could impact the security of State Data environment

(j) *IRS-Defined*: The contract for the acquisition must contain Exhibit 7 language, as appropriate (see IRS 1075 Revision November 2021 - Exhibit 7 Safeguarding Contract Language)

(k) *SSA Data requirements*:

1. Provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents
2. Prior to signing the Agreement, and thereafter at SSA's request, obtain from its contractors and agents, a current list of employees and agents with access to SSA data and provide such lists to SSA

(l) *PCI-Defined*: Maintain information about which PCI DSS requirements are managed by each service provider and which are managed by ITS, where applicable

Policy Mapping

ITS ISPM							
AC-20, CA-03, CP-02, IR-04, IR-07, PL-10, PL-11, PS-07, SA-02, SA-04, SR-03, SR-05							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P2040, P4130, G215	GV.OC-05, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10, ID.AM-02,	4.17.SA-9	5.1.1.7, 5.1.1.8, 5.1.2, 5.1.2.1	2.15.SA-9	2.4, 2.6, 12.8, 12.8.1 - 12.8.4, 12.9	164.308(a)(2)(a), 164.308(a)(4)(a), 164.314(a), 164.308(b)(a), 164.314(a)(1)(i)-(ii), 164.314(a)(1)(ii)(A)-	PB, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4

	ID.AM-04, DE.CM-06					(B), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(ii)(a)-(b)	

(SA-10) Developer Configuration Management

Purpose

The purpose of the policy is to ensure organizations require developers to implement configuration management practices for secure system development.

Scope

The policy applies to Application Developers (AppDev), System Administrator (SysAdmin), Chief Information Security Officer (CISO), and all ITS supported information systems (System/s) under development, implementation or operation that may receive, receive, store, process, or transmit (Handle) data classified as Level 1 and higher (State Data).

Policy

ITS policy requires AppDev and SysAdmin to:

(a) Perform configuration management during System, component, or service development, implementation, and operation
(b) Document, manage, and control the integrity of changes to the System, component, or service
(c) Implement only ITS-approved changes to the System, component, or service
(d) Document approved changes to the System, component, or service and the potential security impacts of such changes
(e) Track security flaws and flaw resolution within the System, component, or service and report findings to CISO
(f) *Software and Firmware Integrity Verification*: Require the developer of the System, System component, or System service to enable integrity verification of software and firmware components
(g) *Hardware Integrity Verification*: Require the developer of the System, System component, or System service to enable integrity verification of hardware components
(h) *Security and Privacy Representatives*: Require agency designated security and privacy representatives to be included in the configuration change management and control process

Policy Mapping

ITS ISPM							
CM-02, CM-03, CM-04, CM-07, CM-09, SA-04, SA-05, SA-08, SA-15, SI-02, SR-03, SR-04, SR-05, SR-06							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-09, PR.PS-02, PR.PS-03, PR.PS-06	4.17.SA-10	5.10.4.1		6.4		CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8

(SA-11) Developer Security Testing and Evaluation

Purpose

The purpose of the policy is to ensure organizations require developers to conduct testing and evaluation to verify security and privacy requirements.

Scope

The policy applies to Application Developers (AppDev), System Administrator (SysAdmin), and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the developer of the System, System component, or System service, at all post-design stages of the system development life cycle (SDLC) to:

(a) Develop and implement a plan for ongoing security and privacy assessments
(b) Perform System testing/evaluation at all post-design phases of the SDLC at the depth of one or more of the following:
    1. Security-related functional properties
    2. Security-related externally visible interfaces
    3. High/Low-level design
    4. Implementation representation (i.e., source code and hardware schematics)
(c) Produce evidence of the execution of the assessment plan and the results of the testing and evaluation
(d) Implement a verifiable flaw remediation process
(e) Correct flaws identified during testing and evaluation
(f) *Static Code Analysis*: Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis
(g) *Manual Code Reviews*: Require the developer of the system, system component, or system service to perform a manual code review of FTI-related applications using the following processes, procedures, and/or techniques: agency-defined manual review process
(h) *Penetration Testing*: Require the developer of the system, system component, or system service to perform penetration testing:
    1. At the following level of rigor: at a minimum Whitebox testing
    2. Under the following constraints: Where State Data is Handled
(i) *Attack Surface Reviews*: Require the developer of the system, system component, or system service to perform attack surface reviews Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers

Policy Mapping

ITS ISPM							
CA-02, CA-07, CM-04, SA-03, SA-04, SA-05, SA-08, SA-15, SA-17, SI-02, SR-05, SR-06, SR-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-01, ID.RA-09, ID.IM-01, ID.IM-02, ID.IM-03, PR.PS-06	4.17.SA-11			6.3, 6.3.1, 6.3.2, 6.4, 6.4.4, 6.6		PB, ID.DE-P5, CT.PO-P4

(SA-12) Supply Chain Protection – WD

Policy Objective: Withdrawn: Moved to Supply Chain Risk Management Family

(SA-13) Trustworthiness – WD

Policy Objective: Withdrawn: Incorporated into SA-08

(SA-14) Criticality Analysis – WD

Policy Objective: Withdrawn: Incorporated into RA-09

(SA-15) Development Process, Standards, and Tools

Purpose

The purpose of the policy is to ensure organizations use secure development processes, standards, and tools to mitigate risks.

Scope

The policy applies to all Application Developers (AppDev), the Chief Security Information Officer (CISO), Chief Technology Officer (CTO), Enterprise Architect (EA), and ITS Management.

Policy

ITS policy requires the developer of the system, system component, or system service to:

(a) Follow a documented development process that:
1. Explicitly addresses security and privacy requirements
2. Identifies the standards and tools used in the development process
3. Documents the specific tool options and tool configurations used in the development process
4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development

(b) Review the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy security and privacy requirements

(c) *Criticality Analysis*: Require the developer of the system, system component, or system service to perform a criticality analysis:
1. At the following decision points in the system development life cycle: the agency-defined
2. breadth/depth
3. At the following level of rigor: post-design phases of the SDLC

(d) At least annually, developers must be trained in current, secure coding techniques, including:
1. How to avoid common coding vulnerabilities
2. Understanding how State Data is Handled in memory

(e) The following "live" production data is prohibited from use in testing or development:
1. Personally Identifiable Information (PII)
2. Primary Account Numbers (PANs)

Policy Mapping

ITS ISPM							
MA-06, SA-03, SA-04, SA-08, SA-10, SA-11, SR-03, SR-04, SR-05, SR-06, SR-09							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
G591B	ID.RA-01, ID.RA-09, PR.PS-06	4.17.SA-15			6.3, 6.5, 6.5.1-6.5.10, 6.4 and 6.4.3		ID.DE-P2, CT.PO-P4

(SA-16) Developer Provided Training – NR

Policy Objective: No Requirement

(SA-17) Developer Security and Privacy Architecture and Design - NR

Policy Objective: No Requirement

(SA-18) Tamper Resistance and Detection – WD

Policy Objective: Withdrawn: Moved to SR-9

(SA-19) Component Authenticity – WD

Policy Objective: Withdrawn: Moved to SR-11

(SA-20) Customized Development of Critical Components – NR

Policy Objective: No Requirement

(SA-21) Developers Screening – NR

Policy Objective: No Requirement

(SA-22) Unsupported System Components

Purpose
The purpose of the policy is to ensure organizations replace system components when support is no longer available from the developer, vendor, or manufacturer.

Scope
The policy applies to the Chief Technology Officer (CTO), Enterprise Architect (EA), and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy prohibits unsupported Systems and System components from operating on any network, without the CTO and EA first:

(a) Replace System components when support for the components is no longer available from the developer, vendor, or manufacturer

(b) Provide the following options for alternative sources for continued support for unsupported components: Extended security support agreement that include security software patches and firmware updates from an external source for each unsupported component Implementing compensating controls, if applicable

Policy Mapping

ITS ISPM							
PL-02, SA-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-08	4.17.SA-22	5.14.SA-22				

(SA-23) Specialization – NR

Policy Objective: No Requirement

(SC) System and Communication Protection Family

(SC-01) System and Communication Protection Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish and maintain policies and procedures for system and communications protection.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and all system and communication protection policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the system and communications protection policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level system and communication protection policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the system and communication protection policies and the associated system and communication protection family policies

(b) Review and update the current system and communication protection:
   1. Policies annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data
   2. Procedures annually and following any security incidents involving unauthorized access to State Data or systems used to handle State Data

Policy Mapping

ITS ISPM							
PM-09, PS-08, SA-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.18.SC-1	5.10.SC-1				GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6

(SC-02) Separation of System and User Functionality

Purpose
The purpose of the policy is to ensure organizations isolate security functions from non-security functions to protect system integrity.

Scope
The policy applies to all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires all applications, services, or Systems to:

(a) Separate user functionality, including user interface services, from Systems management functionality

(b) *Interfaces for Non-privileged Users*: Prevent the presentation of System management functionality at interfaces to non-privileged users

Policy Mapping

ITS ISPM							
AC-06, SA-04, SA-08, SC-03, SC-7, SC-22, SC-32, SC-39							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.18.SC-2	5.10.SC-2		2.2, 2.2.1, 7.1.1,		CT.DP-P3

(SC-03) Security Function Isolation

Purpose
The purpose of the policy is to ensure organizations isolate security functions from non-security functions to protect system integrity.

Scope
The policy applies to the Infrastructure Team, System Administrator (SysAdmin), Hosting Team, Security Operations (SecOps), Network Operations (NetOps), and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
Infrastructure Team, SysAdmin, Hosting Team, SecOps, and NetOps are required to isolate security functions from non-security functions.

Policy Mapping

ITS ISPM							
AC-03, AC-06, AC-25, CM-02, CM-04, SA-04, SA-05, SA-08, SA-15, SA-17, SC-02, SC-7, SC-32, SC-39, SI-16							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4570, G535	PR.PS-03				2.2, 2.2.1, 7.1.1,		

(SC-04) Information in Shared System Resources

Purpose
The purpose of the policy is to ensure organizations prevent unauthorized information transfer through shared system resources.

Scope
The policy applies to the Chief Operating Officer (COO), Chief Information Security Officer (CISO), and ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the COO in consultation with the CISO to prevent unauthorized and unintended information transfer via shared System resources.

Policy Mapping

ITS ISPM							
AC-03, AC-04, SA-08, SC-06							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01	4.18.SC-4	5.10.SC-4		2.6		

(SC-05) Denial-of-Service (DoS) Protection

Purpose
The purpose of the policy is to ensure organizations protect against and limit the effects of denial-of-service events.

Scope
The policy applies to Security Operations (SecOps), Network Operations (NetOps), and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires SecOps and NetOps to:

(a) Protect against or limit the effects of the following types of denial-of-service events: distributed denial of service, DNS Denial of Service, etc.

(b) Employ the following controls to achieve the denial-of-service objective: boundary protection devices and intrusion detection or prevention devices

Policy Mapping

ITS ISPM							
CP-02, IR-04, SC-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-01, DE.CM-01		5.10.SC-5				PR.DS-P4, PR.PT-P3

(SC-06) System Availability

Purpose
The purpose of the policy is to ensure organizations allocate resources to maintain system availability during adverse conditions.

Scope
The policy applies to the Service Desk, Unified Endpoint Management (UEM), and all ITS supported information systems (System/s).

Policy
ITS policy requires the Service Desk and UEM to protect the availability of ITS resources by allocating Systems:

(a) By roles, responsibilities, and baseline configuration

(b) To personnel following (S.SC-01) System Allocation

Policy Mapping

ITS ISPM							
AC-05, CM-08, PS-05, SC-04, SC-05, S.SC-01							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.IR-03						PR.PT-P4

(SC-07) Boundary Protection

Purpose
The purpose of the policy is to ensure organizations monitor and control communications at system boundaries to prevent unauthorized access.

Scope

The policy applies to Network Operations (NetOps), Security Operations (SecOps), and all ITS supported information systems (System/s) and connection to an external network and key internal boundaries.

Policy

ITS policy requires NetOps and SecOps to manage the interfaces for boundary protection of Systems are employed, monitored, audited, and controlled at connection points to external networks using security devices (e.g., firewalls, routers, encrypted tunnels) in accordance with ITS enterprise architecture. NetOps and SecOps must:

(a) Monitor and control communications at the external managed interfaces to the System and at key internal managed interfaces within the Systems

(b) Implement subnets for publicly accessible System components that are physically or logically separated from internal ITS networks

(c) Connect to external networks or Systems only through managed interfaces consisting of boundary protection devices arranged in accordance with ITS security and privacy architecture

(d) *Access Points*: Limit the number of external network connections to the System

(e) *External Telecommunications Service*s:

1. Implement a managed interface for each external telecommunication service
2. Establish a traffic flow policy for each managed interface
3. Protect the confidentiality and integrity of the information being transmitted across each interface
4. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need
5. Review exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the System, while removing exceptions that are no longer supported by an explicit mission or business need
6. Prevent unauthorized exchange of control plane traffic with external networks
7. Publish information to enable remote networks to detect unauthorized controls plane traffic from internal networks
8. Filter unauthorized control plane traffic from external networks

(f) *Deny by Default – Allow by Exception*: Deny network communications traffic by default and allow network communications traffic by exception at boundary devices for Systems used to handle State Data

(g) *Split Tunneling for Remote Devices*: Prevent split tunneling for remote devices connecting to ITS Systems unless the split tunnel is securely provisioned using:

1. Individual users must not have the ability to configure split tunneling
2. Auditing must be performed semi-annually on each workstation with split tunneling enabled. Auditing must include:
   i. Only those users authorized for split tunneling have it enabled in their user profile or policy object
   ii. There is a continued need for split tunneling for the user
   iii. Only the correct and authorized split tunneling configurations are present on the workstation
3. Host checking is enabled and configured on the VPN server:
   i. Ensure the OS is supported
   ii. Ensure that anti-malware is installed and up to date
   iii. The most current hotfixes are applied
   iv. ITS-defined additional parameters

(h) *Route Traffic to Authenticated Proxy Servers*: Route all internal communications traffic that may be proxied, except traffic specifically exempted by SecOps, to all untrusted networks through authenticated proxy servers at managed interfaces

(i) *Restrict Threatening Outgoing Communications Traffic*:

1. Detect and deny outgoing communications traffic posing a threat to external systems
2. Audit the identity of internal users associated with denied communications

(j) *Prevent exfiltration*:
1. Prevent the exfiltration of information
2. Conduct exfiltration tests at least semi-annually

(k) *Restrict Incoming Communications Traffic*: Only allow incoming communications from ITS-defined authorized sources to be routed to ITS-defined authorized destinations

(l) *Host-Based Protection*: Implement firewalls and intrusion detection Systems at access points and end user equipment as appropriate

(m) *Networked Privileged Accesses*: Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing

(n) *Automated Enforcement of Protocol Format*: Enforce adherence to protocol formats

(o) *Fail Secure*: Prevent Systems from entering unsecure states in the event of an operations failure of a boundary protection area

(p) *For Systems that process PII*:
1. Apply the following processing rules to data elements of PII: all applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
2. Monitor for permitted processing at the external interfaces to the System and at key internal boundaries within the System
3. Document each processing exception
4. Review and remove exceptions that are no longer supported

(q) *IRS-Defined*: ITS must implement and manage boundary protection (typically using firewalls) at trust boundaries. Each trust boundary must be monitored and communications across each boundary must be controlled

(r) *IRS-Defined*: ITS must block known malicious sites (inbound or outbound), as identified to ITS from US-CERT, MS-ISAC, or other sources, at each internet access point (unless explicit instructions are provided to agencies not to block specific sites). Blocking is to be accomplished within two (2) business days following release of such sites

(s) *SSA-Defined*: Provide SSA with a logical network layout as part of the system authorization process

Policy Mapping

ITS ISPM							
AC-04, AC-17, AC-18, AC-19, AC-20, AU-13, CA-03, CM-02, CM-04, CM-07, CM-10, CP-08, CP-10, IR-04, MA-04, PE-03, PL-08, PM-12, SA-08, SA-17, SC-05, SC-26, SC-32, SC-35, SC-43							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P3010, P3020, P4570	PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01, DE.CM-01	4.18.SC-7	5.10.SC-7	2.13.SC-7	1.1, 1.1.4, 1.2.1, 1.2.3 and 1.3, 1.4,		PB, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3

(SC-08) Transmission Confidentiality and Integrity

Purpose
The purpose of the policy is to ensure organizations protect the confidentiality and integrity of transmitted information.

Scope
The policy applies to Application Development (AppDev), Hosting Team, Security Operations (SecOps), as well as both internal and external networks and all types of supported information systems (System/s) components from which data can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

Policy
ITS policy requires AppDev, Hosting Team, and SecOps to prevent unauthorized disclosure of information during transmission, ensuring Systems transmitting information:

(a) Protect the confidentiality and integrity of transmitted information

(b) *Cryptographic Protection*: Implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission

(c) *(IRS-Defined)*: Agencies shall ensure appropriate transmission protections are in place commensurate with the highest sensitivity of information to be discussed over video and voice telecommunication and teleconferences

Policy Mapping

ITS ISPM							
AC-17, AC-18, AU-10, IA-03, IA-08, IA-09, MA-04, PE-04, SA-04, SA-08, SC-07, SC-16, SC-20, SC-23, SC-28							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4130	PR.DS-02	4.18.SC-8	5.10.SC-8	2.13.SC-8	4.1, 4.1.1, 8.2.1,	164.312(e)(2)(i)	PR.DS-P2

(SC-09) Transmission Confidentiality – WD

Policy Objective: Withdrawn: Incorporated into SC-8.

(SC-10) Network Disconnect

Purpose
The purpose of the policy is to ensure organizations terminate network connections after defined periods of inactivity.

Scope
The policy applies to Infrastructure Team, Network Operations (NetOps), Security Operations (SecOps), and supported information systems (System/s) where data classified as Level 2 or higher is received, processed, stored, accessed, protected, and/or transmitted.

Policy
ITS policy requires Infrastructure Team, NetOps, and SecOps to configure Systems to terminate sessions and require users to re-authenticate to re-activate a terminal or session if a session has been idle for more than thirty (30) minutes.

Policy Mapping

ITS ISPM							
AC-17, SC-23							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.18.SC-10	5.10.SC-10		8.1.8, 12.3.8		PR.AC-P5, PR.PT-P3

(SC-11) Trusted Path – Define

Purpose
The purpose of the policy is to ensure organizations provide a trusted communication path for secure user interactions with security functions.

Scope
The policy applies WHO , and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires ITS to:

(a) Provide a [Assignment: *physically, logically*] isolated trusted communications path for communications between the user and the trusted components of the system
(b) Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: [Assignment: *organization-defined security functions*]
(c) *Irrefutable Communications Path*:
1. Provide a trusted communications path that is irrefutably distinguishable from other communications paths
2. Initiate the trusted communications path for communications between the [Assignment: *organization-defined security functions*] of the system and the user

Policy Mapping

ITS ISPM							
AC-16, AC-25, SC-12, SC-23							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-02, PR.DS-10						PR.DS-P2, PR.PT-P3

(SC-12) Cryptographic Key Establishment and Management

Purpose
The purpose of the policy is to ensure organizations establish and manage cryptographic keys securely.

Scope
The policy applies to Infrastructure Team and cryptographic keys.

Policy
ITS policy requires the Infrastructure Team to establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: NIST SP 800-57, Recommendation for Key Management, for key generation, distribution, storage, access, and destruction.

Policy Mapping

ITS ISPM							
AC-17, AU-09, AU-10, CM-03, IA-03, IA-07, SA-04, SA-08, SA-09, SC-8, SC-11, SC-12, SC-13, SC-17, SC-20, SC-37, SC-40, SI-03, SI-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-01, PR.DS-02	4.18.SC-12	5.10.SC-12		3.5, 3.5.1-3.5.4, 3.6, 3.6.1 - 3.6.8		

(SC-13) Cryptographic Protection

Purpose
The purpose of the policy is to ensure organizations implement cryptographic methods to protect information.

Scope
The policy applies to Infrastructure Team and all ITS supported information systems (System/s) where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled) that utilizes cryptographic keys.

Policy
ITS policy requires Infrastructure Team to ensure Systems handling State Data:
(a) Determine the use of encryption for State Data in-transit when outside a physically secure location

(b) Implement the following types of cryptography required for each specified cryptographic use. Use of SHA-1 for digital signatures is prohibited:
1. Latest FIPS-140 validated encryption mechanism
2. NIST (SP) 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
3. Encryption in transit (payload encryption)

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-07, AC-17, AC-18, AC-19, AU-09, AU-10, CM-11, CP-09, IA-03, IA-05, IA-07, MA-04, MP-02, MP-04, MP-05, SA-04, SA-08, SA-09, SC-08, SC-12, SC-20, SC-23, SC-28, SC-40, SI-03, SI-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-01, PR.DS-02, PR.DS-10	4.18.SC-13	5.10.SC-13	2.13.SC-13		164.312(e)(2)(ii)	

(SC-14) Public Access Protections – WD

Policy Objective: Withdrawn: Incorporated into AC-02, AC-03, AC-05, SI-03, SI-04, SI-05, SI-07, SI-10

(SC-15) Collaborative Computing Devices and Applications

Purpose
The purpose of the policy is to ensure organizations protect collaborative computing devices from unauthorized use.

Scope
The policy applies to the VoIP Team, Unified Endpoint Management (UEM) and all collaborative computing devices such as networked whiteboards, cameras, and microphones.

Policy
ITS policy requires the VoIP Team and UEM to configure systems to:

(a) Prohibit remote activation of collaborative computing devices and applications with the following exceptions: users are notified by signage of the presence of such devices

(b) Provide an explicit indication of use to users physically present at the devices

(c) *Explicitly Indicate Current Participants*: Provide an explicit indication of current participants in meetings that involve State Data

Policy Mapping

ITS ISPM							
AC-21, SC-42							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.18.SC-15	5.10.SC-15				PR.AC-P3

(SC-16) Transmission of Security and Privacy Attributes – NR

Policy Objective: No Requirement

(SC-17) Public Key Infrastructure Certificates

Purpose
The purpose of the policy is to ensure organizations manage public key infrastructure certificates to support secure communications.

Scope
The policy applies to the Infrastructure Team and all public key infrastructure certificates (PKI).

Policy
ITS policy requires the Infrastructure Team to:

(a) Issue public key certificates under an ITS-defined certificate authority or obtain public key certificates from an approved service provider

(b) Include only approved trust anchors in trust stores or certificate stores managed by ITS

Policy Mapping

ITS ISPM							
AU-10, IA-05, SC-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.18.SC-17	5.10.SC-17				

(SC-18) Mobile Code

Purpose
The purpose of the policy is to ensure organizations manage and control the use of mobile code to prevent security risks.

Scope
The policy applies to Application Developers (AppDev) and the mobile code on supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires AppDev to:

(a) Define acceptable and unacceptable mobile code and mobile code technologies

(b) Authorize, monitor, and control the use of mobile code within the system

(c) *Identify Unacceptable Code and Take Corrective Actions:* Identify unacceptable mobile code and take corrective actions

(d) *Acquisition, Development and Use:* Verify that the acquisition, development, and use of mobile code to be deployed in the system meets ITS Information Security Policy Manual requirements

Policy Mapping

ITS ISPM							
AU-02, AU-12, CM-02, CM-06, SI-03							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	4.18.SC-18	5.10.SC-18					

(SC-19) Voice Over Internet Protocol (VoIP) – WD

Withdrawn: Technology-specific; addressed as any other technology or protocol

(SC-20) Secure Name/Address Resolution Service (Authoritative Source)

Purpose
The purpose of the policy is to ensure organizations implement secure name/address resolution services to prevent spoofing.

Scope
The policy applies to the Infrastructure Team and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the Infrastructure Team to:

(a) Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the System returns in response to external name/address resolution queries

(b) Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace

(c) *Data Origin and Integrity :*Provide data origin and integrity protection artifacts for internal name/address resolution queries

Policy Mapping

ITS ISPM							
AU-10, SC-8, SC-12, SC-13, SC-21, SC-22							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.18.SC-20	5.10.SC-20				PR.AC-P5, PR.PT-P3

(SC-21) Secure Name/Address Resolution Service (Recursive or Caching Resolver)

Purpose
The purpose of the policy is to ensure organizations secure recursive or caching resolvers to protect name/address resolution.

Scope
The policy applies to the Infrastructure Team and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the Infrastructure Team to request and perform data origin authentication and data integrity verification on the name/address resolution responses the System receives from authoritative sources.

Policy Mapping

ITS ISPM							
SC-20, SC-22							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.18.SC-21	5.10.SC-21				PR.PT-P3

(SC-22) Architecture and Provisioning for Name/Address Resolution Service

Purpose
The purpose of the policy is to ensure organizations design and provision secure name/address resolution architectures.

Scope
The policy applies to the Infrastructure Team and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the Infrastructure Team to ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Policy Mapping

ITS ISPM							
SC-02, SC-20, SC-21, SC-24							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.18.SC-22	5.10.SC-22				PR.PT-P3

(SC-23) Session Authenticity

Purpose
The purpose of the policy is to ensure organizations protect the authenticity of communications sessions.

Scope
The policy applies to communication protections at the session level versus the packet level (e.g., sessions in service-oriented architectures providing Web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

Policy
This policy requires ITS to:

(a) Protect the authenticity of communications sessions
(b) *Invalidate Session Identifiers at Logout*: Invalidate session identifiers upon user logout or other session termination
(c) *Unique System-generated Session Identifiers*: Generate a unique session identifier for each session and recognize only session identifiers that are system-generated
(d) *Allowed Certificate Authorities*: Only allow the use of ITS defined certificate authorities for verification of the establishment of protected sessions

Policy Mapping

ITS ISPM							
AU-10, SC-08, SC-10, SC-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.18.SC-23	5.10.SC-23				PR.PT-P3

(SC-24) Fail in Known State – NR

Policy Objective: No Requirement.

(SC-25) Thin Nodes – NR

Policy Objective: No Requirement.

(SC-26) Decoys – NR

Policy Objective: No Requirement.

(SC-27) Platform-Independent Applications – NR

Policy Objective: No Requirement.

(SC-28) Protection of Data at Rest

Purpose
The purpose of the policy is to ensure organizations protect the confidentiality and integrity of information stored within systems.

Scope
The policy applies to Database Administrators (DBA), the Infrastructure Team, and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires DBA and the Infrastructure Team to:

(a) Protect the confidentiality and integrity of the following information at rest:
   1. State Data
   2. IT System related information (e.g., configurations, rule sets)

(b) *Cryptographic Protection*: Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of State Data at rest on end user computing Systems (i.e., desktop computers, laptop computers, mobile devices, portable and removable storage devices) in non-volatile storage

(c) If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating System access control mechanisms (for example, by not using local user account databases)

(d) Render data unreadable anywhere it is stored

(e) Not assign user accounts to decryption keys

Policy Mapping

ITS ISPM							
AC-03, AC-04, AC-06, AC-19, CA-07, CM-03, CM-05, CM-06, CP-09, MP-04, MP-05, PE-03, SC-08, SC-12, SC-13, SC-34, SI-03, SI-07, SI-16							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4550, S2140, G540	PR.DS-01	4.18.SC-28	5.10.SC-28	2.13.SC-28	3.1		PR.DS-P1

(SC-29) Heterogeneity – NR

Policy Objective: No Requirement

(SC-30) Concealment and Misdirection – NR

Policy Objective: No Requirement

(SC-31) Covert Channel Analysis – NR

Policy Objective: No Requirement

(SC-32) Information System Partitioning

Purpose
The purpose of the policy is to ensure organizations partition information systems to reduce risks and enhance security.

Scope
The policy applies to System Administrators (SysAdmin), Network Operations (NetOps), the Infrastructure Team, and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires SysAdmin, NetOps, and the Infrastructure Team to partition Systems into components residing in separate physical domains (or environments) as deemed necessary:

(a) Network access and information flow among partitioned System components must be restricted or prohibited by managed interfaces
(b) An assessment of risk must guide the partitioning of System components into separate physical domains (or environments)
(c) The security categorization must guide the selection of appropriate candidates for domain partitioning
(d) Partition privileged functions into separate physical domains

Policy Mapping

ITS ISPM							
AC-04, AC-06, SA-08, SC-02, SC-03, SC-07, SC-36							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-01, PR.DS-10		5.10.3.1		3.4.1		

(SC-33) Transmission Preparation Integrity – WD

Policy Objective: Withdrawn: Incorporated into SC-08

(SC-34) Non-Modifiable Executable Programs – NR

Policy Objective: No Requirement

(SC-35) External Malicious Code Identification

Purpose
The purpose of the policy is to ensure organizations proactively identify network-based malicious code or malicious websites using system components designed for this purpose.

Scope
The policy applies to the Chief Information Security Officer (CISO).

Policy
ITS policy requires the CISO to include system components that proactively seek to identify network-based malicious code or malicious websites.

Policy Mapping

ITS ISPM							
AC-04, AC-06, SA-08, SC-02, SC-03, SC-07, SC-36							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy

	DE.CM-09	4.18.SC-35			5.10.4.2		

(SC-36) Distributed Processing and Storage – NR

Policy Objective: No Requirement

(SC-37) Out-of-Band Channels – NR

Policy Objective: No Requirement

(SC-38) Operations Security – NR

Policy Objective: No Requirement

(SC-39) Process Isolation

Purpose
The purpose of the policy is to ensure organizations isolate processes to prevent unauthorized access and interference.

Scope
The policy applies to the Infrastructure Team and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the Infrastructure Team to maintain a separate execution domain for each executing process.

Policy Mapping

ITS ISPM							
AC-03, AC-04, AC-06, AC-25, SA-08, SC-02, SC-03, SI-16							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-01, PR.DS-10, PR.PS-03, PR.IR-03	4.18.SC-39	5.10.SC-39				

(SC-40) Wireless Link Protections

Purpose
The purpose of the policy is to ensure organizations restrict wireless access to authorized users and devices.

Scope
The policy applies to Network Operations (NetOps).

Policy
ITS policy requires NetOps to protect external and internal wireless links from signal parameter attacks.

Policy Mapping

ITS ISPM
AC-18, PE-21, SC-05, SC-12, SC-13, SI-04

ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-02, PR.DS-10		5.13.1.4		11.1-11.1.2		

(SC-41) Port and I/O Device Access – NR

Policy Objective: No Requirement

(SC-42) Sensor Capability and Data – NR

Policy Objective: No Requirement

(SC-43) Usage Restrictions – NR

Policy Objective: No Requirement

(SC-44) Detonation Chambers – NR

Policy Objective: No Requirement

(SC-45) System Time Synchronization

Purpose
The purpose of the policy is to ensure ITS synchronizes time between systems.

Scope
The policy applies to the Infrastructure Team and the logs being collected for ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
ITS policy requires the Infrastructure Team to:

(a) Synchronize System clocks within and between Systems and System components
(b) *Synchronization with Authoritative Time Source*:
1. Compare the internal System clocks daily with the official NIST or USNO Internet Time Service:
   i. Time.nist.gov 192.43.244.18 [primary]
   ii. Time-nw.nist.gov 131.107.13.100 [alternate]
2. Synchronize the internal System clocks to the authoritative time source when the time difference is greater than ITS-defined time period

Policy Mapping

ITS ISPM							
AC-03, AU-08, IA-02, IA-08							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.18.SC-45					

(SC-46) Cross Domain Policy Enforcement – NR

Policy Objective: No Requirement

(SC-47) Alternate Communications Paths – NR

Policy Objective: No Requirement

(SC-48) Sensor Relocation – NR

Policy Objective: No Requirement

(SC-49) Hardware-Enforced Separation and Policy Enforcement – NR

Policy Objective: No Requirement

(SC-50) Software-Enforced Separation and Policy Enforcement – NR

Policy Objective: No Requirement

(SC-51) Hardware-Based Protection – NR

Policy Objective: No Requirement

(SI) System and Information Integrity Family

(SI-01) System and Information Integrity Policies and Procedures

Purpose
The purpose of the policy is to ensure organizations establish and maintain policies and procedures to manage system and information integrity effectively.

Scope
The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and all system and information integrity policies and procedures.

Policy
ITS policy designates the CISO to manage the development, documentation, and dissemination of the system and information integrity policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level system and information integrity policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the system and information integrity policies and the associated system and information integrity family policies

(b) Review and update the current system and information integrity:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PS-08, SA-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.19.SI-1	5.15.SI.1				PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6

(SI-02) Flaw Remediation (Software Patching)

Purpose
The purpose of the policy is to ensure organizations monitor systems to detect unauthorized changes and potential threats.

Scope
The policy applies to the Infrastructure Team and Unified Endpoint Management (UEM) and security-relevant software updates to all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the Infrastructure Team and UEM to ensure all System components and software are protected from known vulnerabilities by:

(a) Identifying, reporting, and correcting System flaws
(b) Testing software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation
(c) Installing security-relevant software and firmware updates based on severity and associated risk to the confidentiality of data:
    1. Critical within ten (10) days of release from the vendor
    2. High within thirty (30) days of release from the vendor
    3. Medium within sixty (60) days of release from the vendor
    4. Low within ninety (90) days of release from the vendor
(d) Incorporating flaw remediation into ITS configuration management process
(e) *Automated Flaw Remediation Status*: Determining if System components have applicable security relevant software and firmware updates installed using automated mechanisms at a minimum monthly, daily for network workstations and malicious code protection
(f) *Time to Remediate Flaws and Benchmarks for Corrective Actions*:
    1. Measure the time between flaw identification and flaw remediation
    2. Establish the following benchmarks for taking corrective actions: Agency defined based on criticality
(g) *Automated Patch Management Tools*: Employing automated patch management tools to facilitate flaw remediation to all Systems where State Data is Handled that includes but not limited to mainframes, workstations, applications, and network components
(h) *Automatic Software and Firmware Updates*: Installing security relevant software and firmware updates automatically all Systems
(i) *Removal of Previous Versions of Software and Firmware*: Removing previous versions of security relevant software and firmware components after updated versions have been installed
(j) *IRS-Defined*: Ensuring that, upon daily power up and connection to the ITS' network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than once every twenty (24) hours (excluding weekends, holidays, etc.)
(k) Centrally manage the flaw remediation process that includes, but is not limited to the following:
    1. Measuring the time between flaw identification and flaw remediation
    2. Establishing the following benchmarks for taking corrective actions: Agency defined based on criticality
    3. Documentation of impact
    4. Documented change approval by authorized parties
    5. Functionality testing to verify that the change does not adversely impact the security of the System
    6. Back-out procedures
    7. Upon completion of significant change, all relevant compliance requirements must be implemented on all new or changed Systems and networks, and documentation updated as applicable

Policy Mapping

ITS ISPM							
CA-05, CM-03, CM-04, CM-05, CM-06, CM-08, MA-02, RA-05, SA-08, SA-10, SA-11, SI-03, SI-05, SI-07, SI-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4520	ID.IM-01, ID.IM-02, ID.IM-03, PR.PS-02	4.19.SI-2	5.15.SI-2	2.14.SI-2	6.2, 6.4.6		PR.PO-P10

(SI-03) Malicious Code Protection

Purpose
The purpose of the policy is to ensure organizations implement malicious code protection mechanisms to safeguard systems.

Scope
The policy applies to Security Operations (SecOps) and the malicious code protection including antivirus software, antimalware, and intrusion detection system for supported information systems (System/s) entry/exit points that may receive, process, store, access, protect, and/or transmit (Handle) data classified as Level 2 and higher (State Data).

Policy
ITS policy requires SecOps to deploy anti-malware software on all Systems commonly affected by malicious software. SecOps is responsible for:

(a) Implementing signature based and/or non-signature based malicious code protection mechanisms at System entry and exit points to detect and eradicate malicious code
(b) Automatically updating malicious code protection mechanisms as new releases are available in accordance with ITS configuration management policies and procedures
(c) Configuring malicious code protection mechanisms to:
    1. Perform periodic scans of the System and implement weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with agency security policy
    2. Either block or quarantine take and send alert to System administrator in response to malicious code detection
(d) Addressing the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the System
(e) Scanning all removable media for malicious code upon introduction of the media into any System on the network and before users may access the media
(f) Not less than daily, check for updates to malicious code scanning tools, including anti-virus (AV) and anti-spyware software and intrusion detection tools and when updates are available, implement on all devices on which such tools reside
(g) Selecting and implementing the approved application for centrally managing host-based, malicious code protection mechanisms
(h) Developing and implementing the process for periodic evaluations to identify and evaluate evolving malware threats for Systems considered to be not commonly affected by malicious software
(i) Ensuring that anti-virus mechanisms are actively running and cannot be disabled or altered by users unless specifically authorized by management on a case-by-case basis for a limited time
(j) Ensuring anti-malware software is configured to automatically update malicious code protection mechanisms

Policy Mapping

ITS ISPM							
AC-04, AC-19, CM-03, CM-08, IR-04, MA-03, MA-04, PL-09, RA-05, SC-7, SC-23, SC-26, SC-28, SC-44, SI-02, SI-04, SI-07, SI-08, SI-15							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-01, PR.DS-02, PR.DS-10	4.19.SI-3	5.15.SI-3	2.14.SI-3	5.1.1, 5.1.2, 5.2, 5.3		

(SI-04) System Monitoring

Purpose
The purpose of the policy is to ensure organizations use information system monitoring tools to identify and respond to security incidents.

Scope

The policy applies to Security Operations (SecOps), Threat Hunting Team (THT), the Chief Information Security Officer (CISO), Computer Security Incident Response Team (CSIRT), and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires all Systems to be continuously monitored for malicious activity. SecOps must:

(a) Monitor all Systems to detect:
   1. Attacks and indicators of potential attacks
      i. Intrusion detection and prevention
      ii. Malicious code protection
      iii. Vulnerability scanning
      iv. Audit record monitoring
      v. Network monitoring
      vi. Firewall monitoring
   2. Unauthorized local, network, and remote connections

(b) Identify unauthorized use of Systems through a variety of techniques and methods

(c) Invoke internal monitoring capabilities or deploy monitoring devices:
   1. Strategically within the Systems to collect essential information
   2. At ad hoc locations within the System to track specific types of transactions of interest to ITS

(d) Analyze detected events and anomalies

(e) Adjust the level of System monitoring activity when there is an indication of increased risk to ITS operations and assets, individuals, other organizations, or the nation

(f) Obtain legal opinion regarding System monitoring activities

(g) Provide System monitoring information to the CISO at a minimum every two (2) weeks or sooner if deemed necessary

(h) *System-wide Intrusion Detection System*: Connect and configure individual intrusion detection tools into a system-wide intrusion detection system

(i) *Automated Tools and Mechanisms for Real-Time Analysis*: Employ automated tools and mechanisms to support near real-time analysis of events

(j) *Inbound and Outbound Communications Traffic*:
   1. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic:
   2. Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions

(k) *System-Generated Alerts*: Alert the appropriate agency personnel when the following system generated indications of compromise or potential compromise occur: suspicious activity reported from firewalls, intrusion detection systems, malware detection systems, and other agency-defined security tools that report indications of compromise or potential compromise

(l) *Visibility of Encrypted Communications*: Make provisions so that agency-defined encrypted communications traffic is visible to agency-defined system monitoring tools and mechanisms

(m) *Analyze Communications Traffic Anomalies*: Analyze outbound communications traffic at the external boundary of the System and selected interior points within the network (e.g., sub-networks, subsystems) to discover anomalies

(n) *Automated Organization-Generated Alerts*: Alert the CSIRT using automated mechanisms when the following indications of inappropriate or unusual activities with security or privacy implications occur: agency-defined activities that trigger events

(o) *Analyze Traffic and Covert Exfiltration*: Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information at agency defined interior points within the system

(p) *Indicators of Compromise*: Discover, collect, and distribute to organization-defined personnel or roles, indicators of compromise provided by government and non-government sources

(q) *IRS-Defined*: All Internet Access Points/portals shall capture and retain, for at least one year, inbound and outbound traffic header information, with the exclusion of approved Internet "anonymous" connections, as may be approved by the agency CISO

Policy Mapping

ITS ISPM							
AC-02, AC-03, AC-04, AC-08, AC-17, AU-02, AU-06, AU-07, AU-09, AU-12, AU-13, AU-14, CA-07, CM-03, CM-06, CM-08, CM-11, IA-10, IR-04, MA-03, MA-04, PL-09, PM-12, RA-05, RA-10, SC-5, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SC-43, SI-03, SI-06, SI-07, SR-09, SR-10							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-01, ID.IM-01, ID.IM-02, ID.IM-03, PR.DS-01, PR.DS-02, PR.DS-10, DE.CM-01, DE.CM-06, DE.CM-09, DE.AE-02, DE.AE-03	4.19.SI-4	5.15.SI-4	2.14.SI-4	10.2, 10.2.1 - 10.2.7, 10.6.1		PR.PO-P6, PR.DS-P5

(SI-05) Security Alerts, Advisories, and Directives

Purpose
The purpose of the policy ensures organizations manage security alerts and advisories to mitigate risks.

Scope
The policy applies to the Chief Information Security Officer (CISO) and the Computer Security Incident Response Team (CSIRT).

Policy
ITS policy requires the CISO to:

(a) Receive system security alerts, advisories, and directives from designated external agencies on an ongoing basis

(b) Generate internal security alerts, advisories, and directives as deemed necessary

(c) Disseminate security alerts, advisories, and directives to designated agency officials

(d) Implement security directives in accordance with established time frames or notify the issuing agency of the degree of noncompliance

Policy Mapping

ITS ISPM							
PM-15, RA-05, SI-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010	ID.RA-01, ID.RA-02, ID.RA-03	4.19.SI-5	5.15.SI-5				

(SI-06) Security and Privacy Function Verification – NR

Policy Objective: No Requirement.

(SI-07) Software, Firmware, and Data Integrity

Purpose
The purpose of the policy is to ensure organizations enforce software, firmware, and information integrity measures to prevent unauthorized modifications.

Scope

The policy applies to the Infrastructure Team, Security Operations (SecOps), and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the Infrastructure Team and SecOps on Systems where State Data is Handled to:

(a) Employ integrity verification tools to detect unauthorized changes to the following firmware, and information:
   1. System kernels
   2. Drivers
   3. Firmware (e.g., BIOS, UEFI)
   4. Software (e.g., OS, application, middleware)
   5. Security attributes

(b) Take the following actions when unauthorized changes to the software, firmware, and information are detected: immediately disconnect the device from the network and notify the CISO

(c) *Integrity Checks*: Perform an integrity check of software, firmware, and information:
   1. At startup
   2. At the identification of a new threat to which the System is susceptible
   3. The installation of new hardware, software, or firmware
   4. At a minimum annually

(d) *Integration of Detection and Response*: Incorporate the detection of the following unauthorized changes into ITS' incident response capability:
   1. Unauthorized changes to baseline configuration setting
   2. Unauthorized elevation of System privileges

(e) *Protection of Boot Firmware*: Implement the following mechanisms to protect the integrity of boot firmware in System where State Data Handled: verifying the checksum of downloaded firmware

Policy Mapping

ITS ISPM							
AC-04, CM-03, CM-07, CM-08, MA-03, MA-04, RA-05, SA-08, SA-09, SA-10, SC-8, SC-12, SC-13, SC-28, SC-37, SI-03, SR-03, SR-04, SR-05, SR-06, SR-09, SR-10, SR-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
P4590, S6010	ID.RA-09, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-02, DE.CM-09	4.19.SI.7	5.15.SI-7		A3.5.1		PR.DS-P6

(SI-08) Spam Protection

Purpose

The purpose of the policy is to ensure organizations implement mechanisms to detect, prevent, and respond to spam to maintain system integrity and protect against unauthorized access or disruptions.

Scope

The policy applies to Security Operations (SecOps) and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires SecOps to:

(a) Employ spam protection mechanisms at System entry/exit points to detect and act on unsolicited messages

(b) Update spam protection mechanisms when new releases are available in accordance with ITS configuration management policy and procedures

(c) *Automatic Updates*: Automatically update spam protection mechanisms at minimum quarterly

Policy Mapping

ITS ISPM							
PL-09, SC-05, SC-07, SC-38, SI-03, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.19.SI.8	5.15.SI-8		11.4		

(SI-09) Information Input Restrictions – WD

Withdrawn: Incorporated into AC-02, AC-03, AC-05, AC-06

(SI-10) Data Input Validation

Purpose

The purpose of the policy is to ensure organizations validate data inputs to detect and prevent unauthorized or malicious entries, ensuring system integrity and reliability.

Scope

The policy applies to Application Development (AppDev), Threat Hunter Team (THT), and ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires custom-developed applications and web pages, AppDev, and THT to enforce rules for checking the valid syntax and semantics of System inputs are in place to verify that inputs match specified definitions for format and content.

Policy Mapping

ITS ISPM							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-10	4.19.SI-10	5.15.SI-10				CT.DM-P6, PR.DS-P6

(SI-11) Error Handling

Purpose

The purpose of the policy is to ensure organizations implement error-handling mechanisms that provide corrective information without exposing sensitive details, maintaining system integrity and security.

Scope

The policy applies to the Chief Information Security Officer (CISO), Security Operations (SecOps), Application Development (AppDev), and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires SecOps and AppDev to configure all Systems to:

(a) Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited

(b) Reveal error messages only to designated agency officials

Policy Mapping

ITS ISPM							
AU-02, AU-03, SC-31, SI-02, SI-15							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
		4.19.SI-11	5.15.SI-11				

(SI-12) Information Management and Retention

Purpose

The purpose of the policy is to ensure organizations manage and retain information in accordance with applicable laws, regulations, and operational requirements to maintain integrity, accessibility, and compliance.

Scope

The policy applies to the Chief Information Security Officer (CISO), all State personnel and supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the CISO to:

(a) Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements

(b) *Information Disposal*: Use the following techniques to dispose of, destroy, or erase information following the retention period: as defined in MP-06

Reference (S.MP-01) Classifications and (S.SI-1) Retention Schedule for more information.

Policy Mapping

ITS ISPM							
All XX-1, AC-16, AU-05, AU-11, CA-02, CA-03, CA-05, CA-06, CA-07, CA-09, CM-05, CM-09, CP-02, IR-08, MP-02, MP-03, MP-04, MP-06, PL-02, PL-04, PM-04, PM-08, PM-09, PM-22, PS-02, PS-06, PT-02, PT-03, RA-02, RA-03, SA-05, SA-08, SR-02							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.AM-07, ID.AM-08	4.19.SI-12	5.15.SI-12	2.14.SI-12	3.1, 10.7		PB, CT.PO-P2, CT.PO-P4, CT.DM-P4, CT.DM-P5, CT.DP-P2

(SI-13) Predictable Failure Prevention – NR

Policy Objective: No Requirement.

(SI-14) Non-Persistence – NR

Policy Objective: No Requirement.

(SI-15) Information Output Filtering – NR

Policy Objective: No Requirement.

(SI-16) Memory Protection

Purpose

The purpose of the policy is to ensure organizations implement memory protection mechanisms to prevent unauthorized code execution and safeguard system integrity.

Scope

The policy applies to the Infrastructure Team, Security Operations (SecOps), and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the Infrastructure Team and SecOps to implement the following controls to protect the system memory from unauthorized code execution:

(a) Hardware-based or software-based data execution prevention
(b) Data execution prevention and address space layout randomization

Policy Mapping

ITS ISPM							
AC-25, SC-03, SI-07							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	PR.DS-10	4.19.SI-16	5.15.SI-16				

(SI-17) Fail-Safe Procedures – NR

Policy Objective: No Requirement

(SI-18) PII Quality Operations – NR

Policy Objective: No Requirement

(SI-19) De-Identification – NR

Policy Objective: No Requirement

(SI-20) Tainting – NR

Policy Objective: No Requirement

(SI-21) Information Refresh – NR

Policy Objective: No Requirement

(SI-22) Information Diversity – NR

Policy Objective: No Requirement

(SI-23) Information Fragmentation – NR

Policy Objective: No Requirement

(SR) Supply Chain Risk Management Family

(SR-01) Supply Chain Risk Management Policies and Procedures

Purpose

The purpose of the policy is to ensure organizations establish, document, and maintain comprehensive supply chain risk management policies and procedures to systematically identify, assess, and mitigate risks, ensuring the security, resilience, and integrity of supply chain operations.

Scope

The policy applies to the Chief Information Security Officer (CISO), Governance Risk and Compliance (GRC) Team, and all security and privacy supply chain risk management policies and procedures.

Policy

ITS policy designates the CISO to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures. The CISO along with GRC must:

(a) Develop, document, and disseminate to State personnel:
   1. An State level supply chain risk management policy that:
      i. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance
      ii. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines
   2. Procedures to facilitate the implementation of the security and privacy supply chain risk management policies and the associated security and privacy supply chain risk management family policies

(b) Review and update the current security and privacy supply chain risk management:
   1. Policies annually, following changes to ITS' system operating environment and when security incidents occur
   2. Procedures annually, following changes to ITS' system operating environment and when security incidents occur

Policy Mapping

ITS ISPM							
PM-09, PM-30, PS-08, SI-12							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.20.SR-1					ID.BE-P1, ID.DE-P1, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6

(SR-02) Supply Chain Risk Management Plan

Purpose

The purpose of the policy is to ensure organizations develop and implement a structured Supply Chain Risk Management Plan (SCRM) that proactively identifies, assesses, and mitigates risks associated with supply chain dependencies, ensuring operational resilience, security, and compliance with regulatory requirements.

Scope

The policy applies to the Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Enterprise Architect (EA), and Business Operations (BusOps) and all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy requires the CISO, CTO, EA, and BusOps to:

(a) Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and maintenance, and disposal of Systems that Handle State Data

(b) Review and update the supply chain risk management plan every three (3) years or as required, to address threat, organizational or environmental changes

(c) Protect the supply chain risk management plan from unauthorized disclosure and modification

(d) *Establish a SCRM Team*: Establish a supply chain risk management team consisting of CISO, CTO, and BusOps to lead and support the following SCRM activities:

1. Provide expertise in acquisition processes
2. Legal practices
3. Vulnerabilities
4. Threats
5. Attack vectors
6. As well as an understanding of the technical aspects and dependencies of Systems

Policy Mapping

ITS ISPM							
CA-02, CP-04, IR-04, MA-02, MA-06, PE-16, PL-02, PM-09, PM-30, RA-03, RA-07, SA-08, SI-04							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.RM-01, GV.RM-03, GV.RM-04, GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-08, GV.SC-09, GV.SC-10, ID.AM-04, ID.IM-04	4.20.SR-2					ID.DE-P1, ID.DE-P2, ID.DE-P3

(SR-03) Supply Chain Controls and Processes

Purpose

The purpose of the policy is to ensure organizations establish and implement robust supply chain controls and processes to proactively manage risks, enforce security measures, and maintain operational integrity across all stages of supply chain operations.

Scope

The policy applies to the Chief Technology Officer (CTO), Enterprise Architect (EA), Business Operations (BusOps), and the Chief Information Security Officer (CISO).

Policy

ITS policy requires the CTO, EA and BusOps to:

(a) Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of systems that handle State Data in coordination with the CISO:

1. Supply chain elements include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components
2. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components

(b) Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: ITS defined Supply Chain Risk Management policies

(c) Document the selected and implemented supply chain processes and controls in security and privacy plans; supply chain risk management plan; ITS System Security Plan

(d) *Limitation of Harm*: Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain:

1. Avoid purchasing custom or non-standardized configurations
2. Employ approved vendor lists with standing reputations in industry
3. Follow pre-agreed maintenance schedules and update and patch delivery mechanisms
4. Maintain a contingency plan in case of a supply chain event
5. Use procurement carve-outs that provide exclusions to commitments or obligations
6. Use diverse delivery routes
7. Minimize the time between purchase decisions and delivery

(e) *Sub-Tier Flow Down*: Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors

Policy Mapping

ITS ISPM							
CA-02, MA-02, MA-06, PE-03, PE-16, PL-08, PM-30, SA-02, SA-03, SA-04, SA-05, SA-08, SA-09, SA-10, SA-15, SC-07, SC-29, SC-30, SC-38, SI-07, SR-06, SR-09, SR-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-02, GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-05, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10, RS.MA-01, RS.CO-02, RS.CO-03	4.20-SR-3					ID.BE-P1, ID.DE-P1, ID.DE-P2, ID.DE-P3

(SR-04) Provenance – NR

Policy Objective: No Requirement

(SR-05) Acquisition Strategies, Tools, and Methods – NR

Policy Objective: No Requirement

(SR-06) Supplier Assessments and Reviews

Purpose

The purpose of the policy is to ensure organizations conduct systematic supplier assessments and reviews to evaluate security practices, enforce compliance with risk management standards, and mitigate supply chain vulnerabilities through continuous monitoring and validation.

Scope

The policy applies to the Chief Technology Officer (CTO), Enterprise Architect (EA), and Business Operations (BusOps).

Policy

ITS policy requires CTO, EA, and BusOps to assess and review the supply-chain related risks associated with suppliers or contractors and the system, system component, or system service they provide at a minimum annually.

Policy Mapping

ITS ISPM							
CA-08, SI-04, SR-03, SR-05							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.OC-02, GV.OV-01, GV.OV-02, GV.OV-03, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-09, GV.SC-10, ID.RA-09, ID.RA-10	4.20-SR-6					ID.DE-P2

(SR-07) Supply Chain Operations Security – NR

Policy Objective: No Requirement

(SR-08) Notification Agreements – NR

Policy Objective: No Requirement

(SR-09) Tamper Resistance and Detection

Purpose

The purpose of the policy is to ensure organizations implement tamper resistance and detection measures to safeguard supply chain components from unauthorized modifications, counterfeiting, or security breaches, maintaining the integrity and reliability of acquired resources.

Scope

The policy applies to (SecOps), Threat Hunter Team (THT), the Chief Technology Officer (CTO), Business Operations (BusOps), and supported information systems (System/s), system components, or system services where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy makes SecOps, THT, CTO, and BusOps responsible for employing anti-tamper technologies and techniques throughout the multiple phases of the SDLC including design, development, integration, operations, and maintenance. To protect Systems that Handle State Data from tampering and substitution by:

(a) Implement a tamper protection program for the system, system component, or system service
(b) *Multiple Stages of System Development Life Cycle*: Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle

Policy Mapping

ITS ISPM							
PE-03, PM-30, SA-03, SA-15, SI-04, SI-07, SR-03, SR-04, SR-05, SR-10, SR-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
					9.2.1.1, 9.5.1.3		

(SR-10) Inspection of Systems or Components

Purpose

The purpose of the policy is to ensure organizations establish and implement rigorous inspection processes for systems and components to verify integrity, detect anomalies, and mitigate supply chain risks associated with tampering, counterfeiting, or security vulnerabilities.

Scope

The policy applies to Security Operations (SecOps), Threat Hunter Team (THT), the Chief Technology Officer (CTO), Business Operations (BusOps), and supported information systems (System/s), system components, or system services where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy makes SecOps, THT, CTO, and BusOps responsible for inspecting hardware/software components that Handle State Data upon delivery to detect tampering.

Policy Mapping

ITS ISPM							
AT-03, PM-30, SI-04, SI-07, SR-03, SR-04, SR-05, SR-09, SR-11							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	GV.SC-05, ID.RA-09	4.20.SR-10					

(SR-11) Component Authenticity

Purpose

The purpose of the policy is to ensure organizations implement verification mechanisms to assess component authenticity, mitigating risks associated with counterfeit, altered, or unauthorized supply chain elements to maintain operational security and reliability.

Scope

The policy applies to Security Operations (SecOps), Threat Hunter Team (THT), the Chief Technology Officer (CTO), Business Operations (BusOps), and supported information systems (System/s), system components, or system services where data classified as Level 1 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy

ITS policy makes SecOps, THT, CTO, and BusOps responsible for:

(a) Developing and implementing anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the System

(b) Reporting counterfeit System components to source of counterfeit components; agency defined personnel or roles

(c) *Anti-Counterfeit Training*: Training agency defined personnel or roles to detect counterfeit System components (Including hardware, software, and firmware)

(d) *Configuration Control for Component Service and Repair*: Maintaining configuration control over the following System components awaiting service or repair and serviced or repaired components awaiting return to service: hardware used to receive, access, process, store, transmit, or protect State Data

Policy Mapping

ITS ISPM							
AT-03, CM-03, MA-02, MA-04, PE-03, RA-05, SA-04, SA-10, SI-07, SR-09, SR-10							
ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy
	ID.RA-09	4.20.SR-11					

(SR-12) Component Disposal – NR

Policy Objective: No Requirement

ITS Information Security Policies

(P.ITS) ITS Policies

(P.ITS-01) AI Usage Policy

Purpose
The purpose of the policy is to establish a governance framework for artificial intelligence (AI) within State of Idaho agencies and departments. It defines risk classification methodologies, oversight responsibilities, and implementation requirements to enable innovation and ensure appropriate safeguards for privacy, security, and fairness.

Scope
The policy applies to the use of all AI tools by all Idaho State personnel, contractors, and affiliates (personnel) conducting state business.

Policy
The policy defines the structures that enable Idaho to govern AI implementation reliably across varying system complexities, agency and department sizes, and use cases. The model balances comprehensive oversight with operational flexibility, allowing agencies and departments to fulfill their missions according to established governance principles. ITS must:

(a) Establish the following:
   1. AI Executive Committee
   2. Ethics Advisory Committee
   3. Technical Review Board
   4. AI Innovation Team

(b) Define the roles and responsibilities for:
   1. The AI Executive Committee
   2. The Ethics Advisory Committee
   3. The Technical Review Board
   4. The AI Innovation Team
   5. Information Owners
   6. Agencies and Departments
   7. AI Coordinators
   8. State Personnel

(c) Risk Classification Model:
   1. Define a risk classification model incorporating risk factors and risk tiers
   2. Classify all AI implementations according to a multi-factor risk classification model that aligns with existing ITS policy Security Classification (RA-02)

(d) AI System Governance:
   1. Designate specific approval authorities that align with the risk classification tiers
   2. Align AI System Governance with the NIST AI RMF
   3. Document requirements based off risk classifications
   4. Follow a structured AI implementation process throughout its lifecycle

(e) Define Generative AI (GenAI) requirements

(f) Define AI privacy and security requirements

(g) Define documentation requirements for all AI systems

(h) Define AI procurement requirements

(i) Define transparency and fairness requirements

(j) Define AI system monitoring and maintenance requirements

(k) Include AI in the incident response plans

(l) Define training and awareness requirements
(m) Adopt a shared responsibility model for AI governance: see Appendix A
(n) Standard Alignment: AI tools must comply with the (S.ITS-01) AI Usage Standard

Policy Mapping

ITS ISPM							
AC-19, CA-06, CM-10, MP-02, MP-03, MP-04, MP-05, MP-06, MP-07,							
ITA	CSF	CSC	FTI	CJI	SSA	PCI	PHI

(P.ITS-02) Delegated Access Policy

Purpose
The purpose of the policy is to ensure there is proper authorization before delegated access is granted.

Scope
The policy applies to all ITS supported information systems (System/s) where data classified as Level 2 and higher (State Data) is received, processed, stored, accessed, protected, and/or transmitted (Handled).

Policy
It is the policy of ITS that all delegated access to active directory or Microsoft 365 must be requested or approved and submitted by the requesting agencies Human Resources (HR) or Deputy Attorney General (DAG).

Policy Mapping

ITS ISPM							
ITA	CSF	CSC	FTI	CJI	SSA	PCI	PHI

(P.ITS-03) Solution Vetting Policy for Network Access

Purpose
The purpose of the policy is to ensure all solutions (including but not limited to SAAS, On-Premise, Third-Party, In-House, Open-Source, or Proprietary software) introduced to the State network are thoroughly vetted to maintain security, reliability, and compliance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Scope
This policy applies to all of ITS and all government or private entity that receiving or renders support from or to ITS for End-User Device, Servers, Web Hosting, Web Servers, Cloud Solutions, or any other solution or equipment where ITS is responsible for deployment, support, or configuration or where the device or service could connect to the State's network or access the State's data.

Policy
This policy requires:
(a) The creation of a Solution Vetting Board (SVB) with members defined in (S.ITS-02)
(b) All requested solutions to be thoroughly vetted by the process defined in standard (S.ITS-02)
(c) Approved solutions to follow the solution lifecycle defined in standard (S.ITS-02)
(d) ITS to reduce solution redundancy

Policy Mapping

ITS ISPM							
AC-04, CA-03, CM-02, CM-03, CM-05, CM-07, CM-08, CM-10, CM-11, CM-14, PL-02, PM-04, PM-09, PM-21, PT-07, RA-03, RA-05, SA-10, SA-15, SA-22, SI-02, SI-03, SI-07, SI-12, SR-03, SR-06, SR-11, P.ITS-01							
ITA	CSF	CSC	FTI	CJI	SSA	PCI	PHI
P2040, P4550, P4570, S2140	ID.AM-2, ID.AM-8, ID.RA-9, PR.PS-2, PR.PS-5, PR.PS-6	4.4, 4.5, 12.4, 16.14, 3.1, 3.4, 15.2, 15.4,	4.4.CA-03, 4.5.CM-7, 4.12.PL-02, 4.13.PM-04, 4.13.PM-09, 4.13.PM-21, 4.16.RA-03, 4.19.SI-12, 4.20.SR-6	5.7.CM-7, 5.17.PL-02, 5.1.1, 5.1.1.1 - 5.1.1.8, 4.1, 4.3, 5.19.RA-03, 5.15.SI-12	1.6, AC-04, AC-06, 2.12, 2.13	6.1, 12.2, 3.1, 10.7	308(a)(1)(ii)(A) and (B)

ITS Information Security Standards

(S.AC) Access Control Standards

(S.AC-01) System Use Notification

Exhibit 1 Standard banner for Microsoft Windows based workstation and server logon

WARNING

You are accessing a State of Idaho information system that may contain restricted information, which is accessible to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system is prohibited and subject to criminal and civil penalties. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

Exhibit 2 Banner for systems that receive, process, store, access, protect, and/or transmit FTI

WARNING

This system may contain U.S. Government information, which is restricted to authorized users ONLY. Unauthorized access, use, misuse, or modification of this computer system or of the data contained herein or in transit to/from this system constitutes a violation of Title 18, United States Code, Section 1030, and may subject the individual to criminal and civil penalties pursuant to Title 26, United States Code, Sections 7213, 7213A (the Taxpayer Browsing Protection Act), and 7431. This system and equipment are subject to monitoring to ensure proper performance of applicable security features or procedures. Such monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by a user. If monitoring reveals possible evidence of criminal activity, such evidence may be provided to Law Enforcement Personnel.

ANYONE USING THIS SYSTEM EXPRESSLY CONSENTS TO SUCH MONITORING.

Exhibit 3 Banner for systems that have limited space

WARNING *BY ACCESSING AND USING THIS GOVERNMENT COMPUTER SYSTEM, YOU ARE CONSENTING TO SYSTEM MONITORING FOR LAW ENFORCEMENT AND OTHER PURPOSES. UNAUTHORIZED USE OF, OR ACCESS TO, THIS COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.*

Related Policies	AC-08

(S.AC-02) Mobile Device Requirements

Mobile devices owned and supported by ITS **and** personally owned devices must meet the following:

(a) Loss/Theft: Immediately notify ITS management if a mobile device is lost or stolen and the user must alert management to the circumstance of the loss and the data contained on the mobile device

(b) Conduct: Users must conduct themselves in accordance with ITS' (S.PL-01) Rules of Behavior

(c) Passwords/PIN: The device must comply with the requirements in (S.IA-01) Authentication Requirements

(d) Lockout/purge: The mobile device must be configured on:

1. ITS and personally owned devices to lock after three (3) unsuccessful attempts to enter a password or PIN

2. ITS owned devices to purge ALL data automatically if ten (10) unsuccessful attempts are made to gain access
3. Personally owned devices to purge State Data automatically if ten (10) unsuccessful attempts are made to gain access, while making every attempt to maintain personal data

(e) Encryption: Must employ full-device or container encryption to protect the confidentiality and integrity of information on ITS-owned or managed mobile devices. For FTI, mobile devices must use a cryptographic module that is FIPS 140-2 compliant to protect confidentiality and integrity of local data

(f) Data Backups: If the user backs up the data from the mobile device to another device that is not encrypted (e.g., backing up a tablet using an unencrypted computer), then the backup data must be encrypted

(g) Software Protections: Applications that create, store, access, send or receive data must meet ITS security standards and custom developed applications used on mobile devices must undergo a security design review

(h) Anti-malware: Anti-malware software must be installed on mobile devices that can run such software:
1. Android: Android devices are required to have anti-malware software installed
2. Windows: Windows devices are required to have anti-malware software installed
3. Apple: The Apple iOS is not currently capable of running anti-malware software, since no such software exists, based on the design of the iOS

(i) Updates: Mobile device and installed applications must be kept updated with the latest vendor software releases:
1. Operating Systems: The most recent operating system available for the mobile data device must be used
2. Applications: Available security updates for any applications must be applied in a regular and timely manner unless instructed otherwise by ITS IT personnel

(j) Rooting: Users must not circumvent the security of mobile devices by removing limitations designed to protect the device (e.g., "jailbreaking") and users must not tamper with the mobile device by using unauthorized software, hardware, or other methods

(k) Wireless: Users are required to utilize good judgment when connecting the mobile device to other devices and networks:
1. Bluetooth: Passwords or PINs must be used to secure Bluetooth connections with devices and block unknown devices
2. Wi-Fi: Users may only use secure (e.g., WPA2) Wi-Fi networks known to be trustworthy
3. Cellular: ITS is not responsible for overages or data plans for cellular usage

(l) Additional requirements on protecting FTI accessed by mobile systems are provided in Section 3.3.4 Mobile Devices, Section 2.C.7 Offshore Operations, and on the Office of Safeguards website

Related Policies	AC-07, AC-19, AC-20

(S.AC-03) ITS User Accounts

(S.AC-03a) Standard User

(a) Access to Necessary Applications: Permissions to use essential software and tools required to fulfill daily tasks

(b) Limited File Access: Access to personal files and directories, along with necessary shared resources relevant to their role

(c) No Administrative Rights: Restrictions on system-level configurations, installations, or modifications that could impact the overall system stability

(d) Restricted Network Permissions: Access to necessary network resources while restricting access to sensitive network settings or configurations

(e) Limited Print and Device Access: Permissions to use designated printers and authorized devices essential for their work without broader system access

(f) Accounts must be reviewed annually
(g) Must be disabled when the account:
    1. Has expired
    2. Is no longer associated with a user
    3. Is in violation of ITS policy
    4. Has been inactive for ninety (90) days
(h) Must be deleted ninety (90) days after the account has been disabled
(i) Follow (S.IA-01) Authentication Requirements

(S.AC-03b) Local Admin Accounts

(a) Prohibited from web browsing and other internet connections outside of the local protected boundary
(b) Must not have access to email
(c) Follow (S.IA-01) Authentication Requirements

(S.AC-03c) Privileged User Accounts

(a) Must re-authenticate when switching from standard user
(b) Must only be used to perform administration and maintenance
(c) System Configuration: Permissions limited to essential system configurations required for maintenance, updates, and critical troubleshooting tasks
(d) User and Access Management: Authority to manage user accounts, permissions, and access controls while ensuring strict adherence to role-based access controls (RBAC)
(e) Software and Patch Management: Rights to install and update authorized software and patches necessary for system functionality, security, and compliance
(f) Network Configuration: Access to configure and manage network settings, ensuring connectivity, security protocols, and limited access to sensitive network configurations
(g) Security Monitoring and Incident Response: Permissions to access security logs, monitoring tools, and incident response protocols to identify and address security threats promptly
(h) Backup and Recovery: Authority to manage system backups and recovery procedures ensuring data integrity and system restoration capabilities in case of failures
(i) Prohibited from web browsing and other internet connections outside of the local protected boundary
(j) Access to email is prohibited while using privileged accounts
(k) Must be disabled when the account:
    1. Has expired
    2. Is no longer appropriate
    3. Is in violation of ITS policy
    4. Has been inactive for sixty (60) days
(l) Must be deleted ninety (90) days after the account has been disabled
(m) Follow (S.IA-01) Authentication Requirements
(n) Additional role-based training is required
(o) Accounts must be reviewed semi-annually

(S.AC-03d) Domain Admin Accounts

(a) Must re-authenticate when switching from standard user
(b) Must only be used to preform administration and maintenance
(c) Domain Configuration: Limited permissions for essential domain-level configurations necessary for network functionality, such as user account management, group policies, and domain trusts
(d) Server Management: Access rights restricted to critical server configurations, including domain controllers, ensuring stability, security, and compliance
(e) User and Access Management: Authority to manage user accounts, roles, and access controls within the domain, adhering strictly to the principle of least privilege to ensure appropriate access levels

(f) Security Monitoring and Response: Permissions to access and manage security logs, monitoring tools, and incident response procedures at the domain level to promptly address and mitigate security threats
(g) Group Policy Management: Rights to create, modify, and manage group policies ensuring standardized security settings and configurations across the domain
(h) Backup and Recovery: Permissions for managing domain-wide backup and recovery processes to ensure data integrity and the ability to restore the network in case of failures or security incidents
(i) Network Infrastructure Management: Limited access to critical network infrastructure configurations, allowing necessary changes for connectivity and security while minimizing the risk of network-wide disruptions
(j) Prohibited from web browsing and other internet connections outside of the local protected boundary
(k) Access to email is prohibited while using privileged accounts
(l) Must be disabled when the account:
    1. Has expired
    2. Is no longer appropriate
    3. Is in violation of ITS policy
    4. Has been inactive for sixty (60) days
(m) Must be deleted ninety (90) days after the account has been disabled
(n) Follow (S.IA-01) Authentication Requirements
(o) Additional role-based training is required
(p) Accounts must be reviewed semi-annually

(S.AC-03e) Emergency Accounts 'Break Glass'

(a) Only one (1) 'Break Glass' account is permitted per technology
(b) Must re-authenticate when switching from standard user
(c) Must ONLY be used when a device (firewall, switch, etc.) is not available or functioning
(d) Must ONLY be used to fix issues to administration
(e) Revert to privileged account once emergency issue has been resolved
(f) Limited Access: Access to only essential system components and functionalities required for emergency or recovery purposes, such as critical system files, recovery tools, and network access necessary for restoration
(g) System Recovery Tools: Permissions to utilize specific recovery tools or utilities essential for restoring system functionality in case of critical failures or security incidents
(h) Emergency User Management: Limited rights to manage user accounts or permissions temporarily for immediate resolution of access issues or security breaches
(i) Logging and Monitoring: Access to system logs and monitoring tools to identify the cause of emergencies and to ensure appropriate actions can be taken
(j) Specific Administrative Tasks: Restricted access to perform only the critical administrative tasks necessary for system recovery, such as restoring backups or resetting configurations to a known secure state
(k) Additional role-based training is required
(l) Prohibited from web browsing and other internet connections outside of the local protected boundary
(m) Access to email is prohibited
(n) Automatically disable access after two (2) business days
(o) Follow (S.IA-01) Authentication Requirements

(S.AC-03f) Service Accounts

(a) Specific Resource Access: Grant permissions limited to the specific resources (files, databases, networks) required for the service to operate. Avoid granting broad access to unrelated resources
(b) Restrictive Authentication: Use unique, strong credentials for the service account and avoid using privileged or administrative credentials unless necessary for the service's functionality

(c) Least-Privilege Principle: Assign the minimum necessary permissions to perform the service's functions, avoiding unnecessary access to data classified as Level 2 or higher or system configurations
(d) Regular Review and Maintenance: Periodically review and update permissions as the service's requirements change, ensuring that access remains limited to what's essential for its operation
(e) Security Monitoring: Monitor service account activity and access regularly to detect any unusual behavior or potential security breaches
(f) Accounts must be reviewed annually
(g) Follow (S.IA-01) Authentication Requirements

(S.AC-03g) Temporary Accounts

(a) Limited Access Scope: Grant access only to resources, applications, and data required for the specific duration or task for which the account is created
(b) Time-bound Access: Set an expiration date or a defined time frame for the account's validity to ensure it's only active for the duration needed. Automatically disable accounts after two (2) business days
(c) Task-Specific Permissions: Assign permissions based on the temporary user's role or responsibilities for the particular project or task, avoiding unnecessary access beyond their defined scope
(d) No Administrative Rights: Avoid granting administrative privileges unless essential for the temporary role, restricting system-level configurations or critical access
(e) Regular Review and Revocation: Monitor the account's usage and revoke access promptly once the temporary need expires or the task is completed
(f) Follow (S.IA-01) Authentication Requirements

(S.AC-03h) Shared Accounts

(a) Must be approved by the CISO
(b) Identify Access Needs: Determine the specific tasks and responsibilities each user requires within the shared account
(c) Grant Minimal Access: Provide access only to the resources, data, or functionalities necessary for users to fulfill their roles effectively
(d) Restrict Unnecessary Privileges: Avoid granting excessive permissions that surpass the scope of their job responsibilities
(e) Regular Review and Updates: Annually assess and adjust permissions to ensure they align with current needs, removing and unnecessary access
(f) Implement Access Controls: Utilize access controls, to assign permissions based on predefined roles rather than individual user requirements
(g) Follow (S.IA-01) Authentication Requirements

Related Policies	AC-02

(S.AT) Awareness and Training Standards

(S.AT-01) Role-Based Training Content

- All individuals with unescorted access to a physically secure location
- General User: A user, but not a process, who is authorized to use an ITS system
- Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform
- State personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of State Data and the implementation of technology in a manner compliant with the ISPM

(a)

(b) All individuals with unescorted access to a physically secure location:

1. Access, use, and dissemination of State Data penalties
2. Reporting security events
3. Incident response training
4. System use notification
5. Physical access authorizations
6. Physical access control
7. Monitoring physical access
8. Visitor control
9. Personnel sanctions

(c) General User: A user, but not a process, who is authorized to use an ITS system. In addition to S.AT-01(a) above, include the following topics:

1. Proper access, use, and dissemination of ITS non-restricted files information
2. Personally Identifiable Information (PII)
3. Information handling
4. Media storage
5. Media access
6. Audit monitoring, analysis, and reporting
7. Access enforcement
8. Least privilege
9. System access control
10. Access control criteria
11. Session lock
12. Personally owned information systems
13. Passwords
14. Access control for display medium
15. Encryption
16. Malicious code protection
17. Spam and spyware protection
18. Cellular devices
19. Mobile device management
20. Wireless device risk mitigations
21. Wireless device malicious code protection
22. Literacy training and awareness/social engineering and mining
23. Identification and Authentication (Organizational Users)
24. Media protection
25. When unescorted logical or physical access to any system results in the ability, right, or privilege to view, modify, or make use of unencrypted State Data with initial and annual training in the employment and operation of PII processing and transparency controls

26. Most recent changes to the ISPM

(d) Privileged User: A user that is authorized (and, therefore, trusted) to perform security relevant functions that general users are not authorized to perform. In addition to S.AT-01(a) and (b) above, include the following topics:
   1. Access control
   2. System and communications protection and information integrity
   3. Patch management
   4. Data backup and storage – centralized or decentralized approach

(e) State personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of State Data and the implementation of technology in a manner compliant with the ISPM. In addition to S.AT-01(a), (b), and (c) above, include the following topics:
   1. Additional state/local/tribal/territorial or federal agency roles and responsibilities
   2. Summary of audit findings from previous state audits of local agencies
   3. Findings from the last mandated audit
   4. CJIS defined:
      i. Local Agency Security Officer Role
      ii. Authorized recipients Security Officer Role

(f) *(SSA Defined)* SSA training and awareness programs must include:
   1. The sensitivity of SSA data
   2. The rules of behavior concerning use and security in systems and/or applications processing SSA data
   3. The Privacy Act and other Federal and State laws governing collection, maintenance, use, and dissemination of information about individuals
   4. The possible criminal and civil sanctions and penalties for misuse of SSA data
   5. The responsibilities of employees, contractors, and agents pertaining to the proper use and protection of SSA data
   6. Restrictions on viewing and/or copying SSA data
   7. The proper disposal of SSA data
   8. The security breach and data loss incident reporting procedures
   9. The basic understanding of procedures to protect the network from viruses, worms, Trojan horses, and other malicious code
   10. Social engineering (phishing, vishing, and pharming) and network fraud prevention

Related Policies	AT-03, AT-04, PM-12

(S.AU) Audit and Accountability Standards

(S.AU-01) Event Logging

The following are events that ITS requires to be logged:

(a) All individual accesses to State Data
(b) Use of identification and authentication mechanisms:
    1. Log onto system
    2. Log off system
    3. Change of password
(c) Attempts to use:
    1. Access permission on a user account, file, directory, or other system resource
    2. Create permission on a user account, file, directory, or other system resource
    3. Write permission on a user account, file, directory, or other system resource
    4. Delete permission on a user account, file, directory, or other system resource
    5. Change permission on a user account, file, directory, or other system resource
(d) Failed logons or failed invalid logical access attempts
(e) Attempts for users to:
    1. Access the audit log file
    2. Modify the audit log file
    3. Destroy the audit log file
(f) All SysAdmin commands, while logged in as SysAdmin
(g) Switching accounts or running privileged actions from another account, (e.g., Linux/Unix SU or Windows RUNAS)
(h) Subset of SysAdmin commands, while logged on in the:
    1. Security administrator role
    2. User role
(i) Clearing of the audit log file
(j) Startup and shutdown of audit functions
(k) Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su)
(l) Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system
(m) Changes made to an application or database by a batch file
(n) Application-critical record changes
(o) Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility)
(p) All system and data interactions
(q) Access to data must be audited at the operating system, software, and database levels. Software and platforms have differing audit capabilities. Each individual platform audit capabilities and requirements are maintained on the platform-specific Office of Safeguards SCSEM, which is available on the IRS Office of Safeguards website
(r) Account creation, modification, enabling, disabling, and removal actions
(s) Execution of privileged functions
(t) Activities associated with configuration-controlled changes
(u) Nonlocal maintenance and diagnostic sessions
(v) System and privacy attribute changes

Related Policies	AU-02, AU-03, AU-07, AU-11, AU-12

(S.AU-02) Critical Security Control Systems

(a) Firewalls
(b) IDS/IPS
(c) FIM
(d) Anti-malware
(e) Physical access controls
(f) Logical access controls
(g) Audit logging mechanisms
(h) Segmentation controls (if used)
(i) Security Information and Event Management (SIEM)

Related Policies	AU-06, RA-09

(S.IA) Identification and Authentication Standards

(S.IA-01) Authentication Requirements

Passwords must never be shared with, used by, or disclosed to others and meet the parameters within ITS policy.

(a) IT Operations will never ask personnel for their password/PIN
(b) Passwords must not be inserted into email messages or other forms of electronic communications
(c) Passwords must not be embedded in automated programs, utilities, applications, documents, or other methods whereby they may be stored on the supported information system

(S.IA-01a) Password-Based Authentication

For **ALL** password-based authentication:

- Password Length: Minimum of fourteen (14) characters
- Password History/Reuse:
  - For all systems: Twenty-four (24) generations
  - For systems unable to implement history/reuse restriction by generations but are able to restrict history/reuse for a specified time period, passwords must not be reusable for a period of six (6) months
- Password must not be transmitted in the cleartext outside the secure location
- Must be immediately changed when a temporary password has been issued
- Not be displayed when entered
- At least one (1) character change when new passwords are selected for use
- Password lifetime restrictions:
  - One (1) day minimum and ninety (90) days maximum
  - Service account passwords must expire within 366 days (inclusive)
- Password Complexity:
  - Passwords are not a derivative of the user ID
  - Not to be a dictionary word or proper name
  - Passwords have at least one (1) lower alpha, one (1) upper alpha, one (1) number, and one (1) special character (0-9, ! @ # $ % ^ & * ( ) [{] } etc.)
  - Passwords cannot contain two identical, consecutive characters

(S.IA-01b) Personal Identification Number (PIN) Authentication

As an authenticator for Multi-Factor Authentication (MFA):

- Minimum length of eight (8) digits. If the system does not enforce a minimum length of 8 digits, the maximum length possible must be used
- Enforce complex sequences (e.g., 73961548 – no repeating digits and no sequential digits)
- Do not store with the SmartCard
- Do not share

For voicemail:

- Minimum length of four (4) digits.
- Enforce complex sequences (e.g., 7396 – no repeating digits and no sequential digits)
- PIN must not be an identifiable number (e.g., phone extension, employee PCN)

- Do not share

(S.IA-01c) Public Key-Based Authentication

- For public key-based authentication:
  - Enforce authorized access to the corresponding private key
  - Map the authenticated identity to the account of the individual or group
- When public key infrastructure (PKI) is used:
  - Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information
  - Implement a local cache of revocation data to support path discovery and validation

(S.IA-01d) One-Time Passwords (OTP)

One-time passwords are considered a "something you have" token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e., OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP must meet the requirements described below:

- Be a minimum of six (6) randomly generated characters
- Be valid for a single session
- If not used, expires within a maximum of five (5) minutes after issuance

(S.IA-01e) Verified Push Authentication

Verified Push streamlines the process by verifying the authentication request through a push notification with a verification code, minimizing the risk of accidental or unauthorized approvals.

When agencies implement the use of Verified Pushes as an authenticator, the Verified Push must meet the requirements described below:

- Be a minimum of 2-6 digits randomly generated
- Be valid for a single session
- If not used, expires within a maximum of five (5) minutes after issuance

(S.IA-01f) Security Assertion Markup Language (SAML)

SAML works by exchanging user information, such as logins, authentication state, identifiers, and other relevant attributes between the identity (IdP) and service provider to simplify and secure the authentication process where users need to access multiple, independent web applications.

It achieves this objective by centralizing user authentication with an identity provider. Web applications can then leverage SAML via the identity provider to grant access to their users. This SAML authentication approach means users do not need to remember multiple usernames and passwords.

When agencies implement the use of SAML as an authenticator, SAML must meet the requirements described below:

- Access to the identity provider must be protected with multi-factor authentication
- Must implement multi-factor authentication on accounts used for SAML authentication to multiple systems
- Must support SAML 2.0 or greater

Password Protection

- Do not use the same password for ITS accounts as for other non-ITS access (e.g., personal ISP account, online banking, benefits, etc.). Users must not use the same password for various ITS access needs and are required to have unique passwords for each account they access
- Do not share ITS passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as Restricted ITS information
- Prohibited password practices: **Do NOT:**
  - Use default vendor passwords
  - Reveal a password over the phone to anyone for any reason
  - Reveal a password in an e-mail message
  - Reveal a password to a co-worker or supervisor
  - Talk about a password in front of others
  - Hint at the format of a password (e.g., "my family name")
  - Reveal a password on questionnaires or security forms
  - Share a password with family members
  - Write passwords down and store them anywhere in the user's office
  - Store passwords in a file on any information asset without encryption
- If you suspect your password may have been compromised:
  - Report the incident to your supervisor
  - Change your password immediately

Related Policies	IA-02, IA-05, PL-04

(S.IR) Incident Response Standards

(S.IR-01) Incident Reporting Guidelines

This is a list of reportable incidents, who to report the incident to and the timeframe you must report it. This is not a complete list. Report anything that is suspicious.

Table 2 ITS Reporting Examples

Incident ** This is not a complete list**	Who to Report to	Time to Report
Suspects their password may have been compromised	Service Desk	30 mins
Loss or inappropriate disclosure of data, or violation of security policy	CISO	2 hrs.
Any level of inappropriate level of access to data, supported information systems, or Media	Service Desk, Supervisor	2 hrs.
Any discovered access to systems or data that can be accessed by the public	Supervisor, IT Operations	30 mins
Computer has been infected with virus, ransomware, malware, etc..	CISO	Immediately
Loss or theft of Mobile system	CISO, Supervisor	Immediately
Loss or theft of badge	CISO, Supervisor	Immediately
Termination of personnel	CISO	Immediately
Any threat, actual or perceived, against ITS or personnel	Security Guard	Immediately
Loss or stolen ITS system	CISO, Supervisor	Immediately
Unauthorized disclosure of data classified as Level 2 and Higher	CISO, Supervisor	Immediately
Security incidents or problems	CISO, Supervisor	Immediately

For FTI, contact the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards immediately but no later than twenty-four (24) hours after identification of a possible issue involving FTI

(S.MP) Media Protection Standards

(S.MP-01) Classifications

(S.MP-01a) Data Classifications

Table 3 Data Classification Definitions, Impact, and Examples

Classification	Data Classification Description	
Unrestricted |Public Classification 1	Definition	Includes, but is not limited to, any information relating to public business that is prepared or owned by government agencies and is meant for public access.
	Potential Impact of Loss	**LOW DAMAGE** would occur if Public data were to become available to parties either internal or external to ITS.
		Impact would not be damaging or a risk to business operations.
	Examples	Press releases, brochures, public websites, published research, materials created for public consumption
Limited | Internal Classification 2	Definition	Includes sensitive information that might not be fully protected from public disclosure but could harm privacy or security if widely accessible.
	Potential Impact of Loss	**LOW DAMAGE** would occur if Internal Use data were to become available to unauthorized parties either internal or external to ITS.
		Impact could include damaging the agency's reputation and violating contractual requirements.
	Examples	Internal audit reports, financial transactions, emails, non-public phone numbers, building schematics, names and addresses that are not protected from disclosure
Restricted Classification 3	Definition	Includes sensitive information that is meant for internal use and is not for public disclosure. If disclosed, it could harm the privacy or security of employees, agencies, or individuals. Only authorized internal staff can access this information. External agencies need to sign confidentiality agreements before accessing it.
	Potential Impact of Loss	**SERIOUS DAMAGE** would occur if Restricted data were to become available to unauthorized parties either internal or external to ITS.
		Loss of Restricted data can lead to security breaches, financial loss, reputational damage, legal consequences, and compromised operations.
	Examples	Employee records, financial data, internal reports, personal contact details, confidential legal number
Personally Identifiable Information (PII) Classification 3	Definition	Includes any data that can be used to identify a specific individual. This includes both direct identifiers (e.g., name, Social Security number) and indirect identifiers (e.g., date of birth, address) that, when combined, can pinpoint a person.
	Potential Impact of Loss	**SERIOUS DAMAGE** would occur if PII were inappropriately accessed, used, or disclosed.
		Loss of PII can lead to identity theft, financial fraud, reputational damage, legal penalties, cyberattacks, and privacy violations.
	Examples	Full name, Social Security Number (SSN), date of birth, home address, driver's license number, passport number
Idaho Controlled Technical Information (ICTI) Classification 3	Definition	Technical data, research, engineering specifications, or software developed, maintained, or utilized within Idaho.
	Potential Impact of Loss	**SERIOUS DAMAGE** would occur if ICTI were inappropriately accessed, used, or disclosed.
		Loss of ICTI could lead to security risks, economic harm, regulatory violations, supply chain disruptions, and loss of public trust.
	Examples	Network diagrams, information systems and telecommunications systems configuration information, security plans, administrator level passwords, engineering designs, specialized software
Federal Tax Information (FTI) Classification 3	Definition	Includes any data provided to the IRS by taxpayers or collected by the IRS during tax administration.
	Potential Impact of Loss	**SERIOUS DAMAGE** would occur if PII were inappropriately accessed, used, or disclosed.
		Loss of FTI can result in identity theft, financial fraud, legal penalties, unauthorized access to taxpayer data, erosion of public trust in tax agencies, and compliance violations.
	Examples	Tax returns, 1099 forms, W-2 forms, Tax Identification Numbers (TIN), Employer Identification Number (EIN)
	Definition	Includes the information collected, maintained, and used by the SSA, which manages social security programs in the U.S., including retirement, disability, and survivor benefits.
		SERIOUS DAMAGE would occur if SSA data were inappropriately accessed, used, or disclosed.

Social Security Administration (SSA) Data Classification 3	Potential Impact of Loss	Loss of SSA data can lead to identity theft, fraudulent benefit claims, financial fraud, legal consequences, disruption of critical social security services, and compliance violations.
	Examples	Social Security Numbers (SSNs), disability or retirement benefit information, earnings records
Criminal Justice Information (CJI) Classification 3	Definition	refers to data related to criminal investigations, law enforcement activities, and legal proceedings, managed by various agencies within the criminal justice system.
	Potential Impact of Loss	**SERIOUS DAMAGE** would occur if CJI were inappropriately accessed, used, or disclosed.
		Loss of CJI can result in identity theft, compromised investigations, threats to law enforcement and public safety, legal liabilities, misuse of sensitive criminal data, and compliance violations.
	Examples	Arrest records, court records, fingerprint data, warrants or restraining orders
Personal Health Information (PHI) Classification 3	Definition	Includes any information related to an individual's health, medical history, or treatment that can be used to identify them.
	Potential Impact of Loss	**SERIOUS DAMAGE** would occur if PHI were inappropriately accessed, used, or disclosed.
		Loss of PHI can lead to identity theft, medical fraud, privacy violations, discrimination, reputational damage, legal consequences for healthcare providers, and compliance violations.
	Examples	Medical records, test results, prescription information
Payment Card Industry (PCI) Data Classification 3	Definition	Includes sensitive information related to credit, debit, and other payment cards used for transactions.
	Potential Impact of Loss	**SERIOUS DAMAGE** would occur if PII were inappropriately accessed, used, or disclosed.
		Loss of PCI data can result in financial fraud, unauthorized transactions, identity theft, regulatory fines, reputational damage, legal liabilities for businesses handling payment information, and compliance violations.
	Examples	Credit card numbers (PAN), security codes (CVV)
Critical Classification 4	Definition	Includes highly sensitive information. If disclosed, it could cause serious harm, including injury or death, to individuals or agency employees.
	Potential Impact of Loss	**SEVERE OR CATASTRPHIC DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to ITS.
		Disclosure that could result in loss of life, disability or serious injury or regulated information with significant penalties for unauthorized disclosure.
	Examples	Medical records with life-threatening information, detailed security plans for high-risk operations, or personal details of individuals in witness protection programs.

(S.MP-01b) Data Risk Classification

FIPS Publication 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each agency and the overall national interest.

The *potential impact* is **Low** if –
The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on ITS operations, ITS assets, or individuals.

A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a degradation in mission capability to an extent and duration that ITS is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced
- Result in minor damage to ITS assets
- Result in minor financial loss
- Result in minor harm to individuals

The *potential impact* is **Moderate** if –
The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on ITS operations, ITS assets, or individuals.

A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a significant degradation in mission capability to an extent and duration that the ITS is able to perform its primary functions, but the effectiveness of the functions is significantly reduced
- Result in significant damage to ITS assets
- Result in significant financial loss

- Result in significant harm to individuals that does not involve loss of life or life-threatening injuries

The *potential impact* is **High** if –
The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on ITS operations, ITS assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions
- Result in major damage to ITS assets
- Result in major financial loss
- Result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries

Table 4 Data Risk Classification Examples

Data Risk Classification		
Low Risk	**Moderate Risk**	**High Risk**
- Research data (at data owner's discretion) - Information authorized to be available on or through ITS' website - Policy and procedure manuals designated by the owner as public - Job posting - ITS contact information - Information in the public domain - ITS details, marketing, or press releases	- Unpublished research data (at data owner's discretion) - Customer records - Personnel: employment applications, personnel files, date of birth, personal contact details (e.g., home address, phone number) - Non-public ITS policies and procedures - Non-public contracts - ITS internal memos and email - Unpublished planning and budgeting info - Engineering, design, and operational information regarding ITS infrastructure	- Personal Identifiable Information (PII) - Federal Tax Information (FTI) - State Tax Information - PCI data Security Standards - Social Security Administration Information (SSA) - Criminal Justice Information (CJI) - Protected Health Information (PHI) - Information that pertains to the security of State Data - Information that pertains to the security of ITS Facilities

(S.MP-01c) System Risk Classification

Systems are classified based on the data stored, processed, transferred, or communicated by the supported information system and the overall risk of unauthorized disclosure.

The following are the Supported Information System Risk Classifications:

Low Risk– Systems that contain only data that is public by law or directly available to the public via such mechanisms as the Internet. Desktops, laptops and supporting systems used by agencies are Low Risk unless they store, process, transfer or communicate Medium Risk or High-Risk data.

Low Risk systems must maintain a minimum level of protection as outlined by ITA Information Security Policies, e.g., passwords and data at rest restrictions. Low risk systems are also subject to State laws and may require legal review to ensure that only public data is released in response to a public records request.

Breaches of Low-Risk systems can potentially pose significant risk to the State. Websites with high visibility are often targets of opportunities for compromise and defacement. In addition, an unauthorized user may be able to pivot to a higher classified supported information system. However, this policy is confined to data classification requirements.

Medium Risk – Stores, processes, transfers or communicates Medium Risk data or has a direct dependency on a Medium Risk system. Any system that stores, processes, or transfers or communicates PII is classified as a Medium Risk system, at a minimum.

High Risk– Stores, processes, transfers, or communicates High Risk data or has a direct dependency on a High-Risk system.

Table 5 System Risk Classification Examples

System Risk Classification		
Low Risk	**Moderate Risk**	**High Risk**
- Servers used for research computing purposes without involving Level 2 and Higher Data - File server used to store published public data - Applications handling Low Risk Data	- Servers handling Medium Risk Data - Database of non-public ITS contracts - File server containing non-public policies and procedures - Server storing personnel and customer records - Applications handling Medium Risk Data	- Servers handling High Risk Data - Servers managing access to High-Risk systems - ITS email systems - DNS and DHCP servers - Active Directory servers - Applications handling High Risk Data - HR application that stores personnel PII - Applications collecting personal information of personnel and Customers - Applications that processes customer applications

(S.MP-01d) Classification Labeling

All data and information systems must be labeled to reflect its classification.

If a storage volume or information source contains multiple classifications, then the highest classification must appear on the label. Data labeling may be automated where possible or done manually.

Labeling Assumptions:

- Any data created or received by ITS employees in the performance of their duties is "*Limited | Internal*", by default, unless the data requires greater confidentiality or is approved for release to the general public
- Treat data that is not assigned a classification level as "*Limited | Internal*" at a minimum and use corresponding controls
- When commingling data with different sensitivity levels into a single application or database, assign the mist restrictive classification of the combined asset. For example, if an application contains "*Limited | Internal*" and "*Restricted*" data, the entire application is "*Restricted*"
- "*Confidential*", "*Restricted*", and "*Limited | Internal*" data must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification
- You may not change the format or media of data if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export "*Restricted*" data from a secure database to an unprotected Microsoft Excel spreadsheet

Table 6 Classification Labeling Examples

	Classification			
Media	**Level 1 | Unrestricted | Public**	**Level 2 | Limited | Internal**	**Level 3 | Restricted | Federal**	**Level 4 | Critical**
Electronic Media Email/Text	No label required	Applicable Statute, if known (i.e., "EXEMPT per Idaho Code § 74-106") External **and** Internal labels	Applicable Statute, if known (i.e., "EXEMPT per Idaho Code § 74-106") External **and** Internal labels	Applicable Statute (i.e., "EXEMPT per Idaho Code § 74-106") (i.e., Federal requirements per E.O. 13526") Non-shareable

Recorded Media CS/DVD/USB (Soft Copy)		Email – Beginning of Subject line Physical Enclosure - Label	Email – Beginning of subject line Physical Enclosure – Label (Reference IRS Pub 1075 for additional marking requirements for FTI)	Will remain in approved systems only Accessed only by approved users
Hard Copy	No label required	Each page if loose sheets; Front **and** Back covers **and** Title page if bound	Each page if loose sheets; Front **and** Back covers **and** Title page if bound	Hard-copy production is **not** authorized
Web Sites	No label required	**Internal Website Only** Each page labeled "LIMITED" on Top **and** Bottom of page	**Internal Website Only** Each page labeled "HIGHLY RESTRICTED" on Top **and** Bottom of page	**Not authorized for any Website** Each system page labeled "CRITICAL" on Top **and** Bottom of page Page WARNING required

Exhibit 4 Security Footer

U//FOUO – Unclassified//For Official Use Only | TLP: Amber | State of Idaho, Level III Data – Confidential
Exempt from Public Records Act disclosure per Idaho Code Title 74, Chapter 1, Section 74-105

(S.MP-01e) Data Handling Guidelines

All users must observe the requirements for transferring or communicating information based on its sensitivity, which are defined in the tables below. Data stewards, or their assigned representative, may designate additional controls to further restrict access to, or to further protect information.

Access to Low Risk and High-Risk data may be granted only after a business need has been demonstrated and approved by the data steward.

Table 7 Classifying Data Transfer or Communication Examples

	Classification			
Method of Transfer or Communication	**Level 1 | Unrestricted | Public**	**Level 2 | Limited | Private**	**Level 3 | Restricted | Confidential | Federal**	**Level 4 | Critical**
Non-Disclosure Agreement (NDA)	No NDA requirements	No NDA requirements	NDA is recommended prior to access by non-ITS employees.	NDA is required prior to access by non-ITS employees.
Internal Network Transmission (wired & wireless)	No special requirements	No special requirements	- Encryption is required - Instant messages are prohibited - FTP is prohibited	- Encryption is required - Instant messages are prohibited - FTP is prohibited
External Network Transmission (wired & wireless)	No special requirements	- Encryption is recommended - Instant message with caution - FTP is prohibited	- Encryption is required - Instant messages are prohibited - FTP is prohibited - Remote access should be used only when necessary and only with VPN and MFA	- Encryption is required - Instant messages are prohibited - FTP is prohibited - Remote access is prohibited
Copying	No restrictions	Permission of data custodian advised	Permission of data custodian required	Permission of data custodian required
Data at Rest (file servers, databases, archives, etc.)	- Logical access controls are required to limit unauthorized use - Physical access restricted to specific groups	- Encryption is recommended - Logical access controls are required to limit unauthorized use - Physical access restricted to specific groups	- Encryption is required - Logical access controls are required to limit unauthorized use - Physical access restricted to specific individuals	- Encryption is required - Logical access controls are required to limit unauthorized use - Physical access restricted to specific individuals
Mobile Devices (cell phone, tablets, etc.)	No special requirements	- Encryption is recommended - Remote wipe should be enabled, if possible	- Encryption is required - Remote wipe must be enabled, if possible	- Encryption is required - Remote wipe must be enabled, if possible

Email (with and without attachments)	No special requirements	- Encryption is recommended	- Encryption is required - Do not forward	- Encryption is required - Do not forward
Physical Mail	No special requirements	- Mail with agency interoffice mail - US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	- Mark "*Open by Addressee Only*" - Use "*Certified Mail*" and sealed, tamper-resistant envelopes for external mailings - Delivery confirmation is required - Hand delivering is recommended over interoffice mail	- Mark "*Open by Addressee Only*" - Use "*Certified Mail*" and sealed, tamper-resistant envelopes for external mailings - Delivery confirmation is required - Hand deliver internally
Printer	No special requirements	- Verify destination printer - Retrieve printed material without delay	- Verify destination printer - Use secure print - Attend printer while printing	- Verify destination printer - Use secure print - Attend printer while printing
Web Sites	No special requirements	Posting to publicly accessible Internet sites is prohibited	Posting to publicly accessible Internet sites is prohibited	Posting to publicly accessible Internet sites is prohibited
Telephone	No special requirements	Confirm participants on the call line	- Confirm participants on the call line - Ensure private location	- Confirm participants on the call line - Ensure private location
Video / Web Conference Call	No special requirements	- Roster of attendees - Confirm participants on the call line	- Pre-approve roster of attendees - Confirm participants on the call line - Ensure private location	- Pre-approve roster of attendees - Confirm participants on the call line - Ensure private location
Spoken Word	No special requirements	Reasonable precautions to prevent unintentional disclosure	Active measure to control and limit information disclosure to authorized individuals	Active measure to control and limit information disclosure to authorized individuals
Fax	No special requirements	- Verify destination number - Confirm receipt	Faxing is prohibited	Faxing is prohibited

(S.MP-01f) Media Sanitation/Destruction for Data Classifications

Before disposal or re-use, media must be sanitized in accordance with ITS policy (MP-06) Media Sanitization. These methods ensure that data is not unintentionally disclosed to unauthorized users.

The following table summarizes sanitation/destruction requirements .

Table 8 Media Sanitation/Destruction for Data Classification Requirements

	Classification			
	Level 1 | Unrestricted | Public	**Level 2 | Limited | Private**	**Level 3 | Restricted | Federal**	**Level 4 | Critical**
Electronic Media Sanitization	Not Required (Recommended)	Mandatory	Mandatory	Mandatory
Physical Media Destruction	Not Required (Recommended)	Mandatory	Mandatory	Mandatory

Related Policies	MP-03, MP-04, MP-06

(S.MP-01g) Disposal Methods for Classifications

Disposal methods must follow all federal and state laws and are crucial for ensuring sensitive information is securely removed to prevent unauthorized access. Ensuring that proper disposal methods are followed is vital for compliance with data protection regulations and safeguarding privacy.

The following table summarizes disposal methods for the four data classifications.

Table 9 Disposal Methods for Data Classification Requirements

	Classification			
	Level 1 | Unrestricted | Public	**Level 2 | Limited | Private**	**Level 3 | Restricted | Federal**	**Level 4 | Critical**
Paper, Film/Video, Microfiche	No Special Requirements	Shred or delete all documents or place in secure receptacle for future shredding	Shred or delete all documents or place in secure receptable for future shredding	- Return to owner for destruction - Owner personally verifies destruction - Shred or secure disposal
Storage Media (Hard Drives, Flash Drives, tapes, CDs/DVDs, etc.)	Physically destroy the hard drives and media or use commercial overwrite software to destroy the	Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media	- Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient) - Requires use of ITS-approved vendor for destruction	- Physically destroy the hard drives and media - Requires use of ITS-approved vendor for destruction

(S.MP-02) Federal Tax Information (FTI) Handling

Personnel must understand the criticalness of their roles and responsibilities in safeguarding data and protecting the information resources entrusted to them, and how to detect and avoid risk. State personnel must be familiar with all policies, regulations, standards, and guidance around protecting FTI.

ITS restricts contractors from accessing FTI.

Personnel authorized to handle FTI are restricted from:

(a) Accessing FTI outside the continental United States
(b) Storing, transmitting, processing and/or receiving FTI from telework locations
(c) Commingling physical and electronic FTI with non-FTI data
(d) Transmitting, processing and/or receiving FTI with remote access methods
(e) Using FTI in cloud computing environments
(f) Storing FTI in a data warehouse or off-site storage facilities
(g) Transferring FTI via email communications
(h) Transmitting FTI over fax equipment
(i) Using integrated voice response supported information systems to discuss FTI
(j) Using FTI on storage area networks
(k) Storing, transmitting, process and/or receiving FTI in a virtualized environment
(l) Transmitting FTI on VoIP supported information systems
(m) Providing FTI on web-based supported information systems
(n) Transmitting FTI over any wireless networks

(S.PE) Physical and Environmental Protection Standards

(S.PE-01) Visitors

Visitors must:

(a) Provide proof of identity before being granted access to where supported information systems reside or data is transmitted, stored, or processed
(b) Sign the visitor log with name, reason, escort, time-in, and signature
(c) Always display their visitor badge between their neck and waist
(d) Be escorted where supported information systems reside or data is transmitted, stored, or processed

Related Policies	PE-03

(S.PE-02) Restricted Area Access

To ensure data is protected ITS restricts physical access to areas (i.e., restricted areas) by:

(a) All restricted areas must have at least two barriers of protection to deter, delay, or detect illegal or unauthorized entry
(b) Data must be containerized in areas where personnel that are unauthorized have access
(c) Access to restricted areas must be monitored and records maintained of all persons entering these areas
(d) ITS must establish procedures for restricted area access including:
    1. Protection of data after normal business hours
    2. Appropriate storage containers
    3. Signs should be prominently posted
    4. Visitor access logs that comply with federal laws, Executive Orders, directives, policies, regulations, and standards
    5. Visitor sign-in and validation of visitor's identity
    6. Use of Authorized Access List
    7. Control Access to Area
    8. Control and safeguard keys and combinations
    9. Keep to a minimum physical key (or knowledge of combination) to restricted areas
    10. Protect data in transit

Related Policies	PE-02

(S.PE-03) Alternate Work Sites

Once personnel have completed and submitted a telecommuting application and HR reviews and approves the application, ITS and employee must enter a written "teleworking agreement" to assure that both parties understand and agree to all the expectations during telecommuting.

Telecommuting from home presents security risks that the employee and ITS must mitigate to ensure the confidentiality, integrity and availability of State Data and network services. For personnel that work with sensitive information such as FTI telecommuting does not meet the necessary requirements, therefore is not authorized.

All ITS information, regardless of risk level, must be protected. Adequate precautions must be taken at the telecommuter location to ensure the security of State Data, hardware, and communication links. personnel must adhere to ITS approved security policies, standards, and guidelines to ensure confidentiality, integrity, and availability of ITS resources. In the event a telecommuter has received authorization from ITS to

transport or store State Data at their alternate work site, data encryption and/or physical security measures must be implemented.

Supervisors must be aware of what information is at the telecommuter's alternate work site.

ITS:

(a) May require personnel who enter into a teleworking agreement to take additional training to ensure a complete understanding of the telecommuting agreement
(b) Must establish an incident reporting process in case of a security incident or an information breach
(c) Must determine what equipment and supplies (e.g., personal computer, printer, modem, software, phone line, WATS service, telephone), are appropriate for it to provide to the telecommuting employee for use at the telecommuting location
(d) Must encrypt all data being transported, received, processed, and stored at a minimum, must match the encryption required for the data risk level
(e) Must determine what level of physical protection is required for the information a teleworker works on. The protection, at a minimum, must match the security required for that information in the central workplace
(f) Must ensure security patching and anti-virus updates are maintained on the telecommuter's hardware (PC, PDA, etc.)
(g) Must ensure electronic access by telecommuters to all internal resources, applications, data, and services on ITS' network and at ITS locations must be made according to the established state's VPN standard (S3220)
(h) Must initiate a security check for current security patches, anti-virus/anti-spyware signatures at the start of a VPN connection
(i) Must keep an inventory of all equipment signed out the employee and the liability for loss or damage spelled out in advance
(j) Must determine what data is appropriate for access by employees while telecommuting and what is considered State Data that cannot be accessed
(k) Must provide essential state-owned equipment to the telecommuter
(l) Must provide the supplies and materials required for normal work activities related to the state-owned equipment
(m) Is responsible for maintaining, servicing, and repairing all state-owned equipment
(n) Will aid in the installation of equipment and software during normal work hours
(o) May conduct periodic inspections of alternate work locations during the year to ensure compliance with ITS policies are being met
(p) Results of each inspection must be fully documented

Teleworkers:

(a) Understand state-owned equipment may be used only for legitimate state business purposes, by authorized employees, and complies with ITS policies
(b) Are responsible for protecting the state-owned equipment from theft, damage, and unauthorized use
(c) Are responsible for transport of equipment and for returning it to the central workplace for maintenance and repair, as well as upon termination of the telecommuting period
(d) Must ensure no unauthorized software is installed on the state-owned equipment
(e) Must ensure State Data, applications, documents and other ITS resources are protected from unauthorized viewing, use or access by all third parties including family and friends
(f) Must utilize a screen-lock program on the computer used for work at the alternate work location
(g) Must protect State Data and resources, such as computers, hard drives, and removable media between the central workplace and the alternate work location
(h) Telecommuters must avoid leaving equipment or documents in a car, even if it is locked
(i) If ITS equipment and/or documents must be left in a vehicle, they must be locked in a hard trunk
(j) May not access the network using a home wireless network unless strong security features are enabled, to include 128-bit to 256-bit AES or 3DES encryption of the wireless signal. All wireless network access that is not being used must be turned off

(k) Must report security incidents or information breaches immediately to their supervisor and CISO
(l) May have access to ITS resources through remote access, additionally they must ensure their supervisor is aware of what documents and data is being accessed
(m) Must only use ITS owned computer equipment and protective software used by ITS in order to meet State IT security standards
(n) Must ensure that no unauthorized people, including family and friends, have access to ITS equipment, data, or VPN

Related Policies	PE-17

(S.PE-04) Clean Desk

Requirements for maintaining a "clean desk", whether on paper, storage media, or hardware is properly secured and protected from unauthorized view.

(a) Supported information systems must be locked when the workspace is unoccupied
(b) All State Data must be removed from the desk and locked away when the desk is unoccupied and at the end of the day
(c) Containers containing FTI data must be labeled and remain locked when not in use or unattended
(d) Keys used for access to Medium or High-Risk Data must be secured in a locked desk
(e) Printouts containing Medium or High-Risk Data should be immediately removed from the printer
(f) All data must be shredded in an approved shredder or placed in the locked confidential disposal bins
(g) Portable supported information systems must be either locked with a locking cable or locked away in a drawer
(h) Storage devices when not in use such as CD's, DVD, hard drives, USB drives, etc. containing Medium or High-Risk data must be secured in a drawer and data must be encrypted
(i) Whiteboards containing Medium or High-Risk data must be thoroughly erased when you leave the area containing the whiteboard

Related Policies	PE-01

(S.PL) Planning Standards

(S.PL-01) Rules of Behavior

This ITS standard outlines the rules of behavior of all State personnel as it relates to the security of data or supported information systems owned or operated by ITS.

All personnel must actively participate in ensuring the security of State Data and supported information systems.

Rules of Behavior for all State personnel:

(a) Compliance with all policies is a necessary condition of employment. Noncompliance or conduct unbecoming a state employee may result in disciplinary action, up to and including termination

(b) All work products including, but not limited to, programs, software, source code, and documentation generated on behalf of ITS, are the sole property of ITS without exception. ITS owns all data stored, created, transmitted, and received on behalf of ITS. In the event the data received is subject to a MOU, ITS will ensure that the MOU is enforced. All Media received from an external source must be scanned prior to accessing the data, using approved tools and methods

(c) Use of supported information systems to perform work on behalf of ITS does not indicate an expectation of Privacy. ITS may Audit, examine, inspect, or monitor, at any time without notice, any ITS supported information systems or a non-ITS system that is connected to ITS networks.

(d) Use of ITS supported information systems for personal purposes is permitted if it is not used in a way that is illegal, could compromise security or cause an unauthorized cost to be incurred by ITS. Authorization is determined by your immediate supervisor

(e) Personnel must be observant of any action or occurrence that could violate security policies including unusual behaviors, unlawful activity, unauthorized disclosure of data, or attempts to gain unauthorized access to data or supported information systems. personnel must report loss or inappropriate disclosure of data, loss or theft of supported information systems, or violation of security policy to CISO within two (2) hours of suspected loss or disclosure

(f) Personnel must safeguard their logon ID and password to ensure it is used only for the purpose for which it is intended. If personnel suspect their password may have been compromised, they should change it, and notify CISO and their immediate supervisor within thirty (30) minutes

(g) Personnel will not attempt to access data, supported information systems, or Media, that are not appropriate for their duties and responsibilities or for which they are not authorized. personnel must report any inappropriate level of access to data, supported information systems, or Media to Service Desk and their immediate supervisor within two (2) hours

(h) Personnel will not tamper with or change security configurations of supported information systems

(i) Personnel will not copy, distribute, or use in any manner ITS software that knowingly violates the licensing agreement

(j) Personnel must report suspected security incidents to their immediate supervisor and CISO immediately. Examples of security incidents include but is not limited to:

1. Suspects their password may be compromised
2. Loss or inappropriate disclosure of data
3. Violation of security policies
4. Any level of inappropriate level of access to data, supported information systems, or Media
5. Any discovered access to supported information systems or data that can be accessed by the public
6. Supported information system has been infected with a virus, ransomware, malware, etc.
7. Loss or theft of supported information systems
8. Loss or theft of badge
9. Any threat, actual or perceived, against ITS or personnel

(k) Electronic communications, such as text or email, must not contain statements or content that is libelous, offensive, harassing, illegal, derogatory, or discriminatory. Foul, inappropriate, or offensive messages such as racial, sexual, or religious slurs or jokes are prohibited. Sexually explicit messages or images, cartoons, or jokes are prohibited. Messages for political fund raising, election campaigns, profit, or non-ITS approved fund raising are prohibited

(l) Personnel will not install hardware or software that provides network services (e.g., Wi-Fi, hotspots, wireless access points, etc.). "Sniffing" or listening in on ITS owned networks, wired or wireless, is prohibited

(S.PL-01a) Internet Use

Access to the internet is considered a privilege, and personnel must use it responsibly and professionally and make no intentional use of it in an illegal, malicious, or obscene manner.

(a) Access to the Internet does not convey an expectation of privacy. ITS may audit, examine, inspect, and monitor, at any time, the use of the Internet without notice

(b) No software should be downloaded from the Internet onto ITS supported information systems without the approval of the CISO. The downloader is solely responsible for ensuring that the software is used in a manner consistent with all applicable software copyright and licensing laws. Violation of copyright protection or licensing agreements may subject the downloader to civil and criminal liability

(c) All files downloaded from the Internet must be scanned using CISO approved products prior to use

(d) No FTI or Confidential Information should be transmitted over the internet without prior approval of the CISO and must comply with all policies and procedures. Any questions regarding the appropriateness of transmitting information should be referred to CISO

(S.PL-01b) Messaging Systems

All messages created, sent, received, or stored on the official messaging supported information systems are the sole property of ITS. Use of alternative messaging supported information systems for the purpose of conducting ITS business is expressly prohibited including auto-forwarding of messages.

(a) The use of these supported information systems should be always professional. Personnel must not use messaging systems for harassment, discrimination, to distribute objectionable or illicit material, disrupt work, transmit large files, or in a manner that violates local, state, or federal laws

(b) Access to these supported information systems does not convey an expectation of privacy. ITS may audit, examine, inspect, and monitor, at any time, the use of the messaging systems without notice

(c) Meeting attendees must be limited to individuals that have been authorized to participate

(d) FTI should never be disclosed in messaging systems

(e) Confidential information should only be disclosed to authorized participants with an established business need, and the information must be used for processing a valid business request

(f) Cameras should never capture Confidential or FTI within the video stream. Prior to the start of the session, participants should remove information from desktops, walls, and any other area that is viewable by the camera that will not be used during the meeting

(g) Multiple meetings should not be held using the same web session. This could lead to an unauthorized disclosure

(h) When not in use, collaborative computing devices (i.e., cameras and microphones) are to be disabled

(i) When sessions are complete, all participants must completely logout

(j) All messages will be archived for twelve (12) months

(k) Instant messaging must only be used for communications between State personnel and only authorized state approved software may be used

(S.PL-01c) Social Media

The use of social media by personnel is subject to ITS standards and values. personnel should demonstrate respect for others and exercise good judgment when participating in social media. Except when authorized by Communications, personnel must refrain from:

(a) Making any statements regarding ITS and engage in communications that represents, or makes it appear they are representing, ITS
(b) Using ITS trademarks, logos, letterheads, copyright materials
(c) Communicating information about ITS that has not already been made public
(d) Using a personal email as the POC for a social media site representing ITS
(e) Personnel must refrain from making offensive comments that have the purpose or effect of creating an intimidating or hostile environment such as the use of ethnic slurs, personal insults, profanity, or other offensive language
(f) Personnel must not engage in communications that defame or violate the privacy or publicity rights of any party
(g) Personnel must not use personal accounts for ITS business

(S.PL-01d) Individual Privacy Expectations

To safeguard an individual's privacy in a manner consistent with State and Federal safeguards ITS must:

(a) Safeguard all data in its possession
(b) Limit the collection of data to only that which is necessary to accomplish an official ITS mission, administrative function, regulatory or statutory requirement, or to comply with Homeland Security directives concerning privacy
(c) Provide a Privacy Act Statement to the individual whose data is being collected when required by applicable law
(d) Not collect or use a social security number as a personal identifier in connection with any supported information system or database, unless the collection and/or use is authorized by law
(e) Not disseminate or publish data without the prior consent of the individual or unless provided for by law
(f) Report as soon as practicable all incidents involving the security, loss, misuse, or unauthorized disclosure of data regardless of form or format in accordance with established ITS security incident reporting procedures and requirements
(g) Ensure prompt notification to individuals affected by a breach of State Data (i.e., social security numbers or financial information associated with an individual) commensurate with risk of harm to the individuals and consistent with ITSs breach notification procedures
(h) Approve in writing all requests to access State Data from an offsite location or to transport or transmit State Data offsite
(i) Employ a risk-based approach to protect data from unauthorized disclosure and misuse
(j) Ensure the use of supported information systems will support and not diminish the protections provided in statutes related to the use, collection, and disclosure of data
(k) Ensure that no supported information system of records is used in a computer matching agreement (CMA) unless the matching activity is reflected in the supported information system's routine uses and approved by CISO
(l) Comply with applicable federal laws relating to privacy in its social media use
(m) Review, in consultation with PIO, all memoranda of understanding (MOUs), interconnection security agreements and other agreements that cover sharing data prior to finalizing the agreement
(n) Train all personnel on their responsibilities, privacy rules of conduct and the consequences for non-compliance

Personnel working on behalf of ITS must:

(a) Safeguard data and follow ITS procedures when teleworking and using mobile devices and cloud technologies
(b) Adhere to privacy rules of conduct and may be subject to all applicable penalties under the Privacy Act. Each case will be handled on an individual basis with a full review of all pertinent facts

(c) Comply with ITS regulations and policies pertaining to collecting, accessing, using, disseminating, and storing data

(d) Ensure that data contained in a supported information system of records, to which they have access in the performance of their duties, is protected so that the security and confidentiality of the information are preserved

(e) Not disclose any personal information contained in any supported information system of records or data collection, except as authorized

(f) Access and use only information for which they have official authorization

(g) Be accountable for their actions and responsibilities related to the data and supported information systems entrusted to them

(h) Protect data from disclosure to unauthorized individuals; Protect the integrity of data in their possession

(i) Protect the availability of data and ensure appropriate access levels; Be knowledgeable of data policies, requirements, and issues

(j) Promptly report breaches of data, unauthorized disclosures, and supported information system vulnerabilities in accordance with ITS policies and procedures

(k) Be subject to the following consequences for non-compliance:

1. Subject to disciplinary action for to take appropriate action upon discovering a breach or for failure to take required steps to prevent a breach from occurring or re-occurring
2. Consequences will be commensurate with the level of responsibility, type of data involved and the severity of the violation. The circumstances, including whether the behavior or action was intentional, will be considered in taking appropriate action. Any action taken must be consistent with law, regulation, applicable case law and any relevant collective bargaining agreement. Consequences can include suspension of access privileges, reprimand, suspension, demotion, removal, and criminal and civil penalties, including prison terms and fines

Related Policies	PL-04

(S.PS) Personnel Security Standards

(S.PS-01) Personnel Background Screening

Background Checks are required of all applicant finalists selected for new hire in regular full-time, regular part-time, time-limited, temporary, intermittent positions or contract services with ITS.

Background screening of ITS employees, contractors, and prospective employees will have the objective and focus on the following:

(a) Compliance with IRS Publication 1075 requirements for personnel who have been authorized to handle FTI data
(b) Compliance with all regulatory mandates and laws enforced by state and federal agencies
(c) Fulfilling other legal or contractual obligations
(d) Providing a safe work environment
(e) Protecting ITS assets
(f) Reducing risk of legal liabilities

Background investigations for any prospective employee must include, at a minimum:

(a) FBI fingerprinting (FD-258) - review of Federal Bureau of Investigation (FBI) fingerprint results conducted to identify possible suitability issues. (Contact the appropriate state identification bureau for the correct procedures to follow.) A listing of state identification bureaus can be found at: https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/identity-history-summary-checks/state-identification-bureau-listing
(b) This national agency check is the key to evaluating the history of a prospective candidate for access to FTI. It allows ITS to check the applicant's criminal history in all 50 states, not only current or known past residences
(c) Check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the last five (5) years, and if applicable, of the appropriate agency for any identified arrests
(d) The local law enforcement check will assist agencies in identifying trends of misbehavior that may not rise to the criteria for reporting to the FBI database but is a reliable source of information regarding an applicant
(e) Citizenship/residency – Validate the subject's eligibility to legally work in the United States (e.g., a United States citizen or foreign citizen with the necessary authorization

ITS must:

(a) To verify identification, state of residency and national fingerprint-based record checks must be conducted prior to granting access to State Data for all personnel who have unescorted access to unencrypted State Data or unescorted access to physically secure locations or controlled areas (during times of State Data processing). However, if the person resides in a different state than that of the assigned agency, the agency must conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening must be consistent with:
    1. 5 CFR 731.106
    2. Office of Personnel Management policy, regulations, and guidance
    3. ITS policy, regulations, and guidance
(b) All requests for access must be made as specified by the CISO. The CISO, or their designee, is authorized to approve access to State Data
(c) If a record of any kind exists, access to State Data must not be granted until the CISO reviews the matter to determine if access is appropriate:
    1. If a felony conviction of any kind exists, the Interface Agency must deny access to State Data,

(d) Require employees, contractors, and sub-contractors (if authorized), with access to FTI data must complete a background investigation that is favorably adjudicated. The policy will identify the process, steps, timeframes, and favorability standards that ITS has adopted. ITS may adopt the favorability standards set by the ITS or one that is currently used by another state agency, or ITS may develop its own standards to FTI access. The policy must establish a result criterion for each required element which defines what would result in preventing or removing personnel access to FTI
(e) Must initiate a background investigation for all personnel prior to permitting access to FTI
(f) Ensure a reinvestigation is conducted within five (5) years from the date of the previous background investigation for all personnel requiring access to FTI
(g) Make written background investigation policies and procedures as well as a sample of a completed personnel background investigations report, available for inspection upon request

Related Policies	PS-02, PS-03

(S.PS-02) Personnel Responsibilities

All personnel must actively participate in ensuring the security of ITS facilities.

All State personnel must:
(a) Observe their surroundings
(b) Report to Security Guards any unusual or suspicious activity
(c) Report any threats (actual or perceived) against ITS or any State personnel
(d) Always safeguard their badge
(e) Always display their badge between their neck and waist while at ITS Facilities or while representing ITS
(f) Report a loss or theft of badge immediately
(g) You may be subject to a repayment fee. The replacement fee is determined by the third-party vendor and is subject to change. You may pay this by check or money order
(h) Not allow another individual to “piggyback” or “tailgate” through security checkpoints (e.g., doors that require badge access)
(i) Never share their badge

(S.PS-03) Ethical Responsibilities

To establish a culture of openness, trust and to emphasize the employee’s and consumer’s expectation to be treated to fair business practices. This standard will serve to guide business behavior to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every ITS employee.

ITS is committed to protecting employees, partners, vendors, and ITS from illegal or damaging actions by individuals, either knowingly or unknowingly. When ITS addresses issues proactively and uses correct judgment, it will help set us apart agencies.

ITS will not tolerate any wrongdoing or impropriety at any time. ITS will take the appropriate measures and act quickly in correcting the issue if the ethical code is broken.

Executive Leadership Commitment to Ethics:
(a) Executive Committee Members within ITS must set a prime example. In any business practice, honesty and integrity must be top priority in leadership
(b) Executive Committee Members must have an open-door policy and welcome suggestions and concerns from personnel. This will allow personnel to feel comfortable discussing any issues and will alert executives to concerns within the work force
(c) Executive Committee Members must disclose any conflict of interests regarding their position within ITS

Personnel Commitment to Ethics:

(a) State personnel will treat everyone fairly, have mutual respect, promote a team environment, and avoid the intent and appearance of unethical or compromising practices
(b) Personnel need to apply effort and intelligence in maintaining ethics value
(c) Personnel must disclose any conflict of interest regarding their position within ITS
(d) Personnel will help ITS to increase customer and vendor satisfaction by providing quality customer service
(e) Personnel should consider the following questions to themselves when any behavior is questionable:
    - Is the behavior legal?
    - Does the behavior comply with all appropriate ITS policies?
    - Does the behavior reflect ITS values and culture?
    - Could the behavior adversely affect company stakeholders?
    - Would you feel personally concerned if the behavior appeared in a news headline?
    - Could the behavior adversely affect ITS if all employees, did it?

ITS' Commitment to Ethics:

(a) ITS will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the agency
(b) ITS will reinforce the importance of the integrity message and the tone will start at the top

(S.SC) System and Communication Protection Standards

(S.SC-01) System Allocation

Any deviations from this standard must be approved by the appropriate authority.

(S.SC-01a) System Allocation

ITS Systems are issued to personnel based on their roles and responsibilities. UEM must be notified on all personnel transfers to ensure the issued system meets the configuration required for the new role.

Personnel will be issued one (1) ITS supported information system only if they have:

- Valid business needs
- Valid access authorization
- Read, understand, and signed an acknowledgment that they understand and will abide by ITS' policies, procedures, standards, and guidelines
- Two or more system allocations must have:
    - Appropriate authority
    - Valid business need

(S.SC-01b) System Replacement

- Service Desk and UEM are responsible for managing the replacement process
- Systems will be replaced every four (4) years, unless exceptional circumstances warrant an earlier replacement

(S.SC-01c) System Reallocation

All ITS Systems issued to personnel must be returned to ITS once there is no longer a business need.

- Personnel returning ITS Systems to UEM must:
- Complete the ITS-01 Request for Computer form (Form must be printed and submitted along with the system)
- Submitting a service request ticketing system record
- System reallocation will happen if UEM follows the Reassessment Procedure and determine it is suitable for reallocation and System is sanitized appropriately

(S.SC-01d) Inventory Management

- Team leads or managers must maintain an up-to-date inventory of all shared devices under their supervision. This inventory should include details such as device type, serial numbers, assigned users, and location
- UEM must:
    - Update the asset Inventory with the details of any computer's reassignment, including the new employee's information and the date of reassignment
    - Follow ITS policy (PM-05) System Inventory

Related Policies	SA-02, SC-06

(S.SC-02) Security Function Isolation

(a) Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server
(b) Firewall and router configurations need be configured to restrict connections between untrusted networks and any System components in ITS' trusted, internal network
(c) Firewall need be installed at all connections from an internal to any other internal or external network
(d) Demilitarized Zones (DMZs) need to be implemented to limit inbound traffic to only System components that provide authorized publicly accessible services, protocols, and ports
(e) Servers which access external networks or are accessed from external networks need to be logically isolated from the private intranet
(f) Networks need to be segregated or divided into separate logical domains, so access between domains can be controlled by means of secure devices
(g) Switched network technology need to be utilized, when possible, to prevent eavesdropping, session stealing, or other exploits based on the accessibility of network traffic
(h) Trust relationships should be strictly avoided between Systems with different risk profiles
(i) Systems with higher protection requirements for confidentiality should not have a trusted relationship with a System that has lower protection requirements
(j) If segmentation is used to isolate the sensitive networks from other networks, penetration tests must be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope Systems from in-scope Systems
(k) Use a Defense-in-Depth (DiD) architecture to protect the confidentiality, integrity, and availability of Systems and State Data, placing Systems that contain State Data in an internal network zone, segregated from the DMZ and other untrusted networks

(S.SC-03) Transmission Confidentiality and Integrity

(a) Accept only trusted keys and certificates
(b) Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard State Data during transmission over public or private network:
    1. Examples of public networks include, but are not limited to:
        i. The internet
        ii. Wireless technologies
        iii. Global System for Communications (GSM)
    2. Examples of private networks include, but are not limited to:
        i. Local Area Network (LAN)
        ii. Virtual Private Network (VPN)
(c) Verify that the proper encryption strength is implemented for the encryption methodology in use, based on documented vendor recommendations and industry-recognized leading practices
(d) Verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. For TLS implementations:
    1. Verify that HTTPS appears as a part of the browser Universal Record Locator (URL)
    2. Verify that no State Data is required when HTTPS does not appear in the URL
(e) Unless otherwise protected by ITS-defined alternative physical safeguards, Systems must:
    1. Implement cryptographic mechanisms to prevent unauthorized disclosure of information
    2. Detect changes to information during transmission

(S.SC-04) Cryptographic Key Establishment and Management

ITS must:

(a) Protect any keys used to secure State Data against disclosure and misuse
(b) Restrict access to cryptographic keys to the fewest number of custodians necessary
(c) Store cryptographic keys securely in the fewest possible locations and forms
(d) Change cryptographic keys that have reached the end of their crypto period (for example, after a defined period has passed and/or after a certain amount of ciphertext has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry-recognized leading practices and guidelines
(e) Retire or replace (e.g., archive, destroy, and/or revoke) keys as deemed necessary when the integrity of the key has been weakened (e.g., departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised
(f) Use archived cryptographic keys only for decryption/verification purposes
(g) Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption, including the following:
    1. Generation of strong cryptographic keys
    2. Secure cryptographic key distribution
    3. Secure cryptographic key storage
(h) Maintain a documented description of the cryptographic architecture that includes:
    1. Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date
    2. Description of the key usage for each key
    3. Inventory of any Hardware Security Modules (HSMs) and other Secure Cryptographic Devices (SCDs) used for key management
(i) Use split knowledge and dual control (e.g., require two or three people, each knowing only their own key component, to reconstruct the whole key) if manual, clear-text cryptographic key management operations are used. Examples include, but are not limited to:
    1. Key generation
    2. Transmission
    3. Loading
    4. Storage
    5. Destruction
(j) Prevent the unauthorized substitution of cryptographic keys
(k) Require cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities

(S.SC-05) Wireless Link Protection

ITS policy requires NetOps to:

(a) Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis:
    1. Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS
    2. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices
(b) Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:
    1. WLAN cards inserted into system components
    2. Portable wireless devices connected to system components (e.g., PCMCIA card, USB, etc.)
    3. Wireless devices attached to a network port or network device
(c) Maintains an inventory of authorized wireless access points including a documented business justification
(d) Implement incident response procedures in the event unauthorized wireless access points are detected

(e) Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities. If automated monitoring is utilized (e.g., wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel

(S.SI) System and Information Integrity Standards

(S.SI-01) Retention Schedule

The following schedule highlights suggested retention periods* for some of the major categories of data:
**Retention periods are measured in years, after the event occurrence (e.g., termination, expiration, filing, etc.)*

All EDMS implementations must comply with the State's Records Management Policies and statutes. Records management guidelines can be found at: Idaho Records Center Retention Schedules.

Storage objects of legal or long-term value must be saved on at least two (2) separate storage devices and maintained in separate locations.

Table 10 Record Retention Schedule

Category	Type of Records	Years
Business Records	Amendments	Permanent
	Annual Reports	Permanent
	Articles of Incorporation	Permanent
	Board of Directors (elections, minutes, committees, etc.)	Permanent
	Bylaws	Permanent
	Capital stock and bond records	Permanent
	Charter	Permanent
	Contracts and agreements	Permanent
	Copyrights	Permanent
	Correspondence (General)	5
	Correspondence (Legal)	Permanent
	Partnership agreement	Permanent
	Patents	Permanent
	Service marks	Permanent
	Stock transfers	Permanent
	Trademarks	Permanent
Category	**Type of Records**	**Years**
Financial Records	Audit report (external)	Permanent
	Audit report (internal)	3
	Balance sheets	Permanent
	Bank deposit slips, reconciliations, and statements	7
	Bills of lading	3
	Budgets	3
	Cash disbursement and receipt record	7
	Checks (canceled)	3
	Credit memos	3
	Depreciation schedule	7
	Dividend register and canceled dividend checks	Permanent
	Employee expense reports	3
	Employee payroll records (W-2, W-4, annual earnings records, etc.)	7
	Financial statements (annual)	Permanent
	Freight bills	3
	General ledger	Permanent

Category	Type of Records	Years
	Internal reports (work orders, sales reports, production reports)	3
	Inventory lists	3
	Investments (sales and purchases)	Permanent
	Profit/Loss statements	Permanent
	Purchase and sales contracts	3
	Purchase order	3
	Subsidiary ledgers (accounts receivable, accounts payable, etc.)	Permanent
	Tax returns	Permanent
	Vendor Invoices	7
	Worthless securities	7
Category	**Type of Records**	**Years**
Personnel Records	Accident report/injury claim	7
	Attendance Records	3
	Employee benefit plans	7
	Employment applications (not hired)	3
	Garnishments	3
	I-9 Forms	3
	Medical and exposure records - related to toxic substances	Permanent
	Agency Charts	Permanent
	OSHA Logs	5
	OSHA Training Documentation	5
	Patents	Permanent
	Pension plan agreement	Permanent
	Personnel files	4
	Profit sharing agreement	Permanent
	Timecards and daily time reports	3
	Security Awareness Training	7
Category	**Type of Records**	**Years**
Insurance	Fire inspection reports	7
	Group disability records	7
	HIPAA-related documentation	6
	Insurance policies	7
	Safety records	3
	Settled insurance claims	7
Category	**Type of Records**	**Years**
Policy Compliance	Server audit trail history	7
	Workstation audit trail history	7
	Router audit trail history	1
	Firewall audit trail history	1
	Visitor access logs	5
	Business Email	1
	Instant Messages	1
Category	**Type of Records**	**Years**
Federal Tax Information (FTI)	Audit Records	7
	Records of configuration-controlled changes to systems	3
	Visitor Access Records	5

Category	Type of Records	Years
	Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five (5) years after the disclosure is made, whichever is longer	5+/-
	Formal Agreements	5
	Logs of FTI (FTI log and FTI bulk transfer log)	5
	Converted Media	5
	State Auditor Disclosures	5
	Disclosure Awareness Certification	5
Category	**Type of Records**	**Years**
Social Security Administration (SSA)	Physical Access for entry and exit points	5
	Audit Records	3
	Security awareness training	5
	Non-disclosure agreements	5
Category	**Type of Records**	**Years**
Criminal Justice Information Services (CJIS)	Audit records	1
	Logs of access privilege changes	1
	Background checks	5

Related Policies | SI-12

(S.SI-02) Information Management and Retention

ITS policy requires the CISO to design, implement, and maintain a data retention program for the systematic retention and destruction of physical and digital documents based on statutory and regulatory record-keeping requirements and practical business needs that include:

(a) Determining which data output from the System is considered not publicly available
(b) Output handling and retention requirements must cover the full life cycle of the data, which in some cases, may extend beyond the disposal of the System
(c) ITS CISO must identify the correct records disposition for data outputs, including how to retain, transfer, archive, and dispose of them
(d) Records with expired retention periods must be disposed of in accordance with ITS guidelines
(e) When data (electronic or printed) no longer becomes necessary, the media must be destroyed in accordance with the media protection policy
(f) Records retention must be in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements
(g) Auto forwarding or redirecting of state issued email outside of the state-controlled service is prohibited
(h) Users may manually forward individual messages after determining the risk or consequences are low and forwarding will not violate any security controls
(i) When sending email to an address outside of the state-controlled email service, users must ensure that any sensitive information, particularly PII, is appropriately protected (i.e., encrypted)
(j) ITS will ensure that all personnel receive security awareness training on the proper handling and protection of data outputs
(k) Refer to Information Security – Awareness and Training Procedures for requirements on security awareness training

(S.SR) Supply Chain Risk Management Standards

(S.SR-01) Tamper Resistance and Detection

ITS policy makes SecOps, THT, CTO, and BusOps responsible for employing anti-tamper technologies and techniques throughout the multiple phases of the SDLC including design, development, integration, operations, and maintenance. To protect Systems that Handle State Data from tampering and substitution by:

(a) Maintaining a list of authorized devices
(b) Periodically inspecting Systems to look for tampering or substitution
(c) Training personnel to be aware of suspicious behavior and to report tampering or substitution of Systems
(d) Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices
(e) Not installing, replacing, or returning devices without verification
(f) Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices)

(S.ITS) ITS Policy Standards

(S.ITS-01) AI Usage Standard

(P.ITS-01) AI Usage Policy requires ITS to incorporate risk and trustworthiness in the use of AI tools. AI tools may only be used to conduct state business if:

(a) Responsibilities:

1. **AI Executive Committee:** The AI Executive Committee is established under the Idaho Technology Authority and shall be responsible for:
   i. Setting statewide priorities for AI implementation
   ii. Reviewing high-risk implementations
   iii. Advocating for shared resources for AI initiatives
   iv. Ensuring alignment with Idaho's broader technology strategy
   v. Reviewing proposed changes to standard governance processes
   vi. Coordinating Idaho's AI governance approach with relevant standards and guidelines
2. **Ethics Advisory Committee:** The Ethics Advisory Committee is established under the Information Technology Leadership Council and shall be responsible for:
   i. Advising on ethical risks, fairness concerns, and demographic impact
   ii. Providing specialized consultation on high-risk consultations
   iii. Reviewing privacy and fairness assessments for medium and high-risk systems
   iv. Developing ethical guidelines for AI development and use
3. **Technical Review Board:** The Technical Review Board shall be responsible for:
   i. Advising on technical issues related to AI proposals and implementations
   ii. Conducting technical reviews of medium and high-risk systems
   iii. Evaluating model development, platform standards, risk assessments, and digital infrastructure
   iv. Providing guidance on implementing appropriate technical safeguards
   v. Reviewing security controls and mitigation strategies
4. **AI Innovation Team:** The AI Innovation Team shall be responsible for:
   i. Providing implementation support to agencies and departments
   ii. Facilitating communities of practice around AI governance
   iii. Developing documentation standards and templates
   iv. Maintaining the state's AI system inventory
   v. Coordinating testing and evaluation of emerging AI technologies
   vi. Developing and distributing standardized implementation tools
   vii. Supporting agency and department-level AI Coordinators
5. **Information Owners:** Information owners shall:
   i. Validate decisions regarding assignment of security controls and access privileges
   ii. Execute formal information sharing agreements with other agencies and departments prior to exchanging AI-generated information
   iii. Perform periodic risk classification reviews based on changes in sensitivity, value, and impact to the agency or department
   iv. Classify AI systems based on the "high water mark" (highest impact level) if the system's associated information
   v. Ensure appropriate documentation and safeguards are implemented based on risk tier
6. **Agencies and Departments:** Agencies and departments shall:
   i. Establish policies and procedures for managing risk classification within the agency or department
   ii. Ensure that information belonging to different classification levels is appropriately protected

iii. Observe and maintain the appropriate security for classification levels assigned by another agency or department's information owner
iv. Provide training to information owners and handlers on this policy
v. Designate internal AI Coordinators for implementation coordination
vi. Ensure all AI systems are disposed of in accordance with established policies and regulations
vii. Maintain an inventory of AI systems used within the agency or department
viii. Implement appropriate incident response procedures for AI-related incidents

7. **AI Coordinators**: AI Coordinators designated by each agency and department shall:
   i. Serve as primary point of contact for agency and department AI implementations
   ii. Coordinate risk assessment and approval processes
   iii. Maintain agency and department-level AI documentation and inventory
   iv. Facilitate agency and department compliance with this policy
   v. Participate in cross agency and department AI communities of practice
   vi. Coordinate AI training for agency and department personnel
   vii. Liaise with the AI Innovation Team
8. **State Personnel**: All state personnel shall:
   i. Create an account specifically used for state business using their state issued email
   ii. Follow all AI policies, standards, and guidelines

(b) **Risk Classification Model**: All AI implementations must be classified according to a multi-factor risk classification model that aligns with existing ITS policy Security Classification (RA-02). This model evaluates AI systems across six dimensions and rates each dimension based on a four-point scale ("Low", "Medium", "High", and "Very High.").

1. Risk Classification Factors:
   i. **Personal Data Sensitivity**: Assesses the nature of the data the system uses and maps directly to ITS policy Security Classification (RA-02) levels:
      (A) Level 1 (Unrestricted) data
      (B) Level 2 (Limited) data
      (C) Level 3 (Restricted) data
      (D) Level 4 (Critical) data
   ii. **Decision Impact**: Assesses how system outputs affect individuals, considering FIPS-199 impact levels (low, medium, high) as referenced in ITS policy Security Classification (RA-02).
   iii. **Autonomy Level**: Evaluates human oversight involvement, with fully autonomous systems carrying higher risk than those with human validation.
   iv. **Transparency**: Measures how understandable the system's logic and outcomes are to non-technical stakeholders, with "black box" models scoring higher.
   v. **Scope and Scale**: Considers system reach, from limited pilots to enterprise-wide deployments impacting thousands.
   vi. **Novelty and Complexity**: Evaluates whether the system uses well-established methods or introduces untested approaches with potential unforeseen risks.
2. **Risk Tiers**: The individual dimension ratings described in the previous section are weighted and combined to produce a total risk score. This score places systems into one of three governance tiers aligned with ITS policy Security Classification (RA-02) levels:
   i. **Tier 1: Low Risk**: These systems generally process non-sensitive information, have limited decision impact, maintain human oversight, and have a narrow scope of operation. Their overall risk profile typically aligns with Classification Levels 1-2 ("Unrestricted" or "Limited") from (RA-02).
   ii. **Tier 2: Medium Risk**: These systems may process some sensitive information, have moderate decision impact, operate with reduced human oversight, or serve a broader user base. Their overall risk profile typically aligns with Classification Level 3 ("Restricted") from (RA-02).
   iii. **Tier 3: High Risk**: These systems process highly sensitive information, have significant decision impact, operate with substantial autonomy, or serve large populations. Their overall risk

profile typically aligns with Classification Level 4 ("Critical") from (RA-02).

3. **Risk Classification Requirements:** All AI implementations must be classified according to the risk assessment methodology defined in P.ITS-01. The risk classification must align with ITS policy Security Classification Policy (RA-02). Classification Process:
   i. The completed assessment must use the State of Idaho Risk Classification Tool and be approved by ITS and the agency or department's designated AI Coordinator.
   ii. The assessment must evaluate each of the risk factors identified in P.ITS-01, including GenAI-specific factors when applicable.
   iii. The assessment must include justification for each factor and identification of specific concerns.
   iv. The assessment must document the data classification levels of information processed by the system according to ITS policy Security Classification (RA-02).
   v. The risk classification must be reviewed annually and when significant changes occur to the system's functionality, data sources, or operational context.
4. **Risk Management Alignment:** The risk assessment and management process must align with the four core functions of the NIST AI RMF:
   i. **Govern**: Establish and implement a governance structure that incorporates AI risk management into agency and department processes.
   ii. **Map**: Identify, analyze, and document context, capabilities, and potential risks of the AI system.
   iii. **Measure**: Assess and track AI risks and impacts using appropriate qualitative and quantitative tools.
   iv. **Manage**: Allocate resources to address and reduce AI risks throughout the system lifecycle.

CSF Core Function	Function Description	Closest AI RMF Function(s)	Rationale
Identify	Develop an organizational understanding to manage cybersecurity risk	Map, Govern	Both involve understanding systems, stakeholders, risk context, and governance structures
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services	Manage, Govern	Focus on risk mitigation strategies and protective measures for AI systems
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event	Measure, Manage	Relates to detecting anomalous or harmful AI behavior via measurement and monitoring
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident	Manage	Addresses how to take action on identified risks, including incident response and adaptation
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident	Manage, Govern	Supports continuity and system improvement through governance and resilience planning

5. **GenAI-specific Risk Factors**: For GenAI systems, additional risk factors must be evaluated:
   i. Potential for hallucinations or factual inaccuracies.
   ii. Vulnerability to prompt injection.
   iii. Data poisoning risks.
   iv. Copyright and intellectual property implications.
   v. Potential for misuse or unintended outputs.

(c) AI Data Management:

1. Data classified as:
   i. **Unrestricted Data (Classification Level 1)**: May be processed with approved GenAI tools with appropriate oversight.
   ii. **Limited Data (Classification Level 2)**: May be processed with approved GenAI tools with enhanced oversight and content review.
   iii. **Restricted Data (Classification Level 3)**: May only be processed with securely deployed, enterprise-approved GenAI solutions with stringent safeguards.
   iv. **Critical Data (Classification Level 4)**: Must not be processed with GenAI tools without explicit authorization for high-risk deployments, including AI Executive Committee review, and implementation of robust safeguards.
2. AI tools must have access to and use only data sources they need and respects users' rights and privacy.
3. Institute proper data and information management controls, procedures, and processes for data set selection, evaluation, and preparation for use with AI tools.
4. Data used to train AI systems will be screened for biases and corrected where necessary.
5. Data storage, transfer, and processing will follow all regulatory and internal data management standards.
6. Employees should be aware of when the use of an AI tool may result in the creation of a public record that must be retained under Idaho Public Records Law Idaho Code §§74-101 through 74-127.

(d) AI System Governance:

1. **Approval Requirements**: Idaho designates specific approval authorities that align with the appropriate level of oversight for each risk tier. The level of review and approval depends on the system's risk classification:
   i. **Tier 1: Low Risk** systems require ITS and agency (or department) IT leader approval. The AI Innovation Team receives notification for inventory purposes only.
   ii. **Tier 2: Medium Risk** systems require ITS and agency (or department) leadership approval with advisory input from the AI Innovation Team and Technical Review Board. Information Owners manage information sharing agreements and security controls as required by (RA-02).
   iii. **Tier 3: High Risk** systems require ITS and agency (or department) leadership approval with mandatory consultation from the Ethics Committee, Technical Review Board, and Executive Committee. Information Owners maintain enhanced oversight of classification and security controls for critical data as required by (RA-02).
2. These authorities exercise responsibility across key lifecycle activities aligned with the NIST AI RMF functions of GOVERN, MAP, MEASURE, and MANAGE. Idaho implements these functions through:
   i. **Initial Planning and Design (GOVERN, MAP)**: ITS and agency (or department) sponsors with Information Owner classification guidance.
   ii. **Development and Testing (MAP, MEASURE)**: Risk-appropriate authority approves resources with security validation.
   iii. **Technical Evaluation (MEASURE)**: Technical Review Board verifies integration and proper data separation.
   iv. **Deployment Decision (MANAGE)**: Risk-appropriate authority approves launch with security verification.
   v. **Monitoring and Evaluation (MANAGE)**: Implementation teams oversee performance with periodic

reviews.

3. **Documentation Requirements**: Documentation requirements scale with risk classification. All AI systems must maintain basic documentation including purpose, data sources, and risk classification. Medium and high-risk systems require additional documentation including privacy impact assessments, security controls, fairness evaluations, and human oversight mechanisms, where appropriate. Agencies and departments can obtain standard templates for required documentation from the AI Innovation Team.
   i. **All AI Systems (Tier 1-3)**
      (A) AI Concept Brief documenting purpose, anticipated benefits, and alignment with agency or department mission.
      (B) Risk Classification Assessment results and approval.
      (C) Data sources, classification levels, and information handling procedures.
      (D) System performance metrics and evaluation criteria.
      (E) User guidance and support materials.
      (F) AI Fact Sheet with standardized system information.
      (G) Human oversight mechanisms and procedures.
      (H) Specific responsibility assignments using the Shared Responsibility model.
      (I) Any deviations from the standard responsibility framework with justification.
      (J) Contact information for all roles.
      (K) Approval signatures from both Agency (or Department) leadership and ITS.
   ii. **Medium-Risk Systems (Tier 2)**: Systems classified as medium-risk must maintain all requirements from Section (d.3.i) plus:
      (A) Privacy Impact Assessment addressing data collection, use, storage, and sharing.
      (B) Security controls implementation documenting technical and administrative safeguards.
      (C) Fairness evaluation results demonstrating testing across demographic groups.
      (D) Monitoring plan identifying performance indicators and review schedules.
      (E) Vendor assessment documentation (for third-party systems).
   iii. **High-Risk Systems (Tier 3)**: Systems classified as high-risk must maintain all requirements from Sections (d.3.i) and (d.3.ii)) plus:
      (A) Detailed model documentation including architecture, training methodology, and limitations.
      (B) Enhanced security assessment documenting specialized AI security controls.
      (C) Risk mitigation plan addressing identified concerns.
      (D) Incident response procedures for AI-specific failure modes.
4. **Implementation Lifecycle:** AI implementations must follow a structured governance process throughout their lifecycle:
   i. **Ideation and Concept Development**: Agencies and departments submit solution vetting requests through standard intake processes. For AI capabilities, the system gathers additional information for the AI Concept Brief. The Information Owner validates classification decisions and governance teams conduct preliminary risk screening.
   ii. **Project Proposal and Risk Assessment**: ITS conducts a formal risk assessment in collaboration with the Information Owner, documenting classification levels, security controls, and data separation methods.
   iii. **Implementation and Deployment**: Standard deployment processes incorporate additional verification of AI-specific controls. Governance and security teams validate privacy, fairness, and transparency requirements alongside classification-appropriate security controls.
5. **Monitoring and Continuous Improvement**: Standard monitoring processes incorporate AI-specific metrics from the Concept Brief. Information Owners conduct periodic classification reviews as required by ITS policy Security Classification (RA-02), with regular reassessment of risk classifications.

(e) **GenAI Requirements**: GenAI systems must adhere to additional requirements:

1. General Use Requirements:
   i. **ITS and Agency (or Department) Approval**: ITS, Agencies (or Departments, where appropriate) must explicitly approve specific GenAI tools for different use cases based on data classification levels:
      (A) **Unrestricted Data (Classification Level 1)**: May be processed with approved GenAI tools with appropriate oversight.
      (B) **Limited Data (Classification Level 2)**: May be processed with approved GenAI tools with enhanced oversight and content review.
      (C) **Restricted Data (Classification Level 3):** May only be processed with securely deployed, enterprise-approved GenAI solutions with stringent safeguards.
      (D) **Critical Data (Classification Level 4)**: Must not be processed with GenAI tools without explicit authorization for high-risk deployments, including AI Executive Committee review, and implementation of robust safeguards.
   ii. **Human Oversight**: All GenAI outputs used for official purposes must undergo human review before finalization or distribution.
   iii. **Content Identification**: AI-generated content must be clearly identified as such when distributed, both internally and externally.
   iv. **Tool Registration**: All GenAI tools must be registered in the agency or department's software inventory and the AI Innovation Team's AI system inventory.
   v. **Output Logging**: Agencies and Departments must maintain logs of significant AI-generated content, including prompts used and human review status.
2. **Acceptable Use Parameters**: Agencies and departments must establish clear parameters for appropriate and inappropriate use of GenAI. All GenAI applications must maintain human review of outputs used for official purposes.
3. **Acceptable Use Cases**: GenAI tools may be used for the following approved use cases:
   i. Content drafting and editing with appropriate human review, including first drafts of routine communications, summarization of non-sensitive documents, format conversion of public information, and language translation of appropriate content.
   ii. Research assistance with verified information, such as analysis of public documentation, suggestion of relevant policies or resources, or explaining complex topics for internal reference.
   iii. Code assistance and documentation, limited to generating code examples for public-facing applications, documenting existing code, and suggesting improvements to non-sensitive code.
   iv. Workflow optimization, including process documentation, meeting summarization (for non-sensitive meetings), and task organization and prioritization.
   v. Customer service enhancement, such as development of chatbot responses for public inquiries, creation of FAQ content, and generation of information materials.
4. **Prohibited Use Cases**: GenAI tools must not be used for:
   i. Fully autonomous decision-making affecting individual rights, benefits, or services.
   ii. Processing or generating content involved data classified as "Critical" under ITS policy Security Classification Policy (RA-02).
   iii. Generating content for official state communications without human review and verification.
   iv. Creating or processing legal documents, contracts, or official opinions without legal review.
   v. Unauthorized disclosure of sensitive information, including personally identifiable information, protected health information, financial account information, law enforcement or security information, or information exempt from public disclosure.
   vi. Impersonation of state officials or misrepresentation of agency or department positions.
   vii. Generation of deceptive content or deepfakes.
5. **Technical Safeguards**: All GenAI implementations must implement:
   i. Content filtering mechanisms to prevent harmful, biased or inappropriate outputs.

ii. Prompt management practices, including documented prompt libraries for approved uses and monitoring and review of prompt effectiveness (e.g., prompt audit logging).
iii. Output review procedures for public-facing content.
iv. Logging and audit capabilities for all system interactions.
v. Security controls appropriate to the data classification level.
vi. Input validation to address potential prompt injection and other manipulation.

6. **Implementation Safeguards**: GenAI implementations must include content filtering, transparency measures, technical protections against misuse, and monitoring of outputs for quality and appropriateness.
7. **Transparency Requirements**: GenAI use must be transparent to both internal users and citizens:
8. **Public Disclosure**: When GenAI contributes to public-facing content, this must be disclosed in a clear and appropriate manner.
9. **Internal Attribution**: Internal documents created or substantially assisted by GenAI must clearly indicate this in the document.
10. **Decision Support Documentation**: When GenAI is used to support decision-making, this must be documented with information about the system used and how outputs were validated.

(f) Privacy and Security:

1. **Privacy Requirements**: AI systems must adhere to Idaho's privacy framework. Systems processing personal information must include privacy impact assessments and implement appropriate safeguards throughout the AI lifecycle.
2. **Security Requirements**: AI systems require safeguards that address both their technical architecture and operational behavior. In accordance with ITS policy Security Classification (RA-02) and (S.MP-01c), Idaho mandates a set of baseline controls for all AI implementations, with additional requirements for systems operating at medium- or high-risk. Over time, these controls will evolve to include protection against emerging threats such as model poisoning, prompt injection, and inference manipulation—security considerations unique to contemporary AI implementations:

i. A Secure by Design Approach to AI Security:

(A) Security for AI systems builds on existing enterprise cybersecurity best practices, standards, and programs. Rather than creating entirely new processes, agencies and departments shall extend their current efforts to address AI-specific concerns. For all AI systems, agencies and departments must implement:

1. Access controls for system administration and operation.
2. Integrity verification for deployed models.
3. Input validation and sanitization.
4. Basic monitoring of system access and operations.
5. Integration with enterprise security infrastructure.

(B) Security Requirements by Risk Tier:

1. **For Tier 1 (Low-Risk) Systems:**
   I. Apply standard IT security controls
   II. Implement basic access controls
   III. Validate user inputs
   IV. Maintain system logs
2. **For Tier 2 (Medium-Risk) Systems**: All Tier 1 measures, plus:
   I. Enhance access controls with stronger authentication
   II. Implement more robust monitoring
   III. Conduct periodic security testing
   IV. Develop specific incident response procedures
3. **For Tier 3 (High-Risk) Systems**: All Tier 2 measures, plus:
   I. Implement advanced security controls
   II. Conduct regular penetration testing
   III. Develop comprehensive monitoring and alerting

IV. Establish specialized incident response plans

3. **Third-Party Requirements**: When acquiring AI capabilities from vendors, agencies and departments remain responsible for verifying compliance state security and privacy standards and implementing compensating controls where necessary. Specific vendor assessment procedures and contracting requirements are detailed in (SA-04).

(g) **AI Procurement**: All AI systems (including pilots or free tools) must be reviewed and approved via ITS processes. Agencies and departments shall adhere to specific guidelines when procuring AI systems or services:

1. **Pre-Procurement Vendor Assessment**: Before procurement, agencies and departments must:
   i. Evaluate vendor AI governance and risk management practices
   ii. Verify adherence to relevant security and privacy standards
   iii. Assess model development methodologies and testing procedures
   iv. Review known limitations, biases, or ethical concerns
   v. Verify vendor compliance with state security and privacy standards.
   vi. Obtain documentation for model development and training methods, data sources and privacy protections, security testing procedures and results, and known limitations or biases.
   vii. Assess alignment with state AI ethical principles.
   viii. Review vendor incident history and remediation practices.
   ix. Complete the standardized Solution Security Questionnaire.
2. **Contractual Requirements**: AI procurement contracts must include:
   i. Specific security and privacy requirements aligned with system risk classification
   ii. Clear delineation of data ownership and usage rights
   iii. Performance metrics and quality standards
   iv. Incident reporting and response obligations
   v. Compliance verification and audit provisions
   vi. Requirements for ongoing support and updates
   vii. Monitoring and reporting obligations.
   viii. Audit rights for system review and compliance verification.
   ix. Warranty provisions for system performance and security.
   x. Requirements for ongoing updates and maintenance.
   xi. Transparency requirements regarding system capabilities and limitations.
3. **Ongoing Vendor Management**: After procurement, agencies and departments must:
   i. Monitor vendor compliance with contractual requirements
   ii. Document and track system updates and changes
   iii. Partner with ITS to periodically reassess system risk classification
   iv. Maintain appropriate vendor management documentation
   v. Regular review of vendor performance and compliance.
   vi. Reassessment of risk classification, where appropriate.
   vii. Validation of continued security compliance.
   viii. Monitoring for reported issues or incidents with the vendor's AI systems.

(h) Transparency and Fairness:

1. **Transparency Requirements:**
   i. AI systems must provide appropriate transparency to both users and those affected by system decisions:
   ii. **AI Use Disclosure**: Clear notification when AI systems are being used, explanation of system capabilities and limitations, and attribution of AI-generated content
   iii. **Explanation Capabilities**: Documentation of system purpose and operation, plan language descriptions of how decisions are made, and explanation of key factors influencing outcomes
2. **Fairness Testing Requirements:**
   i. To ensure AI systems serve All Idahoans, without bias, agencies and departments must:

ii. Identify relevant demographic categories for fairness analysis based on system purpose and affected population, historical patterns of disparate impact in similar contexts, and legal and regulatory requirements.
iii. Establish appropriate fairness metrics, including statistical parity across groups where appropriate, equal error rates across population segments, consistency of decisions for similar cases.
iv. Document fairness testing methodologies and results, including testing datasets used and their representatives, statistical methods applied, and limitations of the analysis.
v. Implement mitigation strategies for identified biases, including model adjustments or constraints, procedural safeguards and human review, and monitoring mechanisms for ongoing assessment.

(i) AI System Monitoring and Maintenance:

1. **Continuous Monitoring Requirements**: Agencies and departments must implement continuous monitoring of AI systems based on risk tier:
   i. **Tier 1 Systems**: Quarterly performance review, annual risk reassessment, and operational metrics tracking.
   ii. **Tier 2 Systems**: Monthly performance review, semi-annual risk reassessment, regular bias and fairness testing, and security and access control verification.
   iii. **Tier 3 Systems**: Weekly performance monitoring, quarterly risk reassessment, comprehensive bias and fairness testing, proactive security testing.
2. **Maintenance Procedures**: All AI systems require documented maintenance procedures:
   i. **Version Control**: Documentation of all system changes, testing requirements before implementation, and approvals appropriate to risk tier.
   ii. **Performance Optimization**: Regular model retraining or updating, data quality verification, and effectiveness evaluation.
   iii. **Documentation Updates**: Maintenance of current system documentation, user guidance revisions, and training material updates.

(j) **Incident Response**: Agencies and departments must build upon existing incident response processes to include relevant AI-specific incident types, such as hallucinated outputs, misclassification of inputs, inference bias, or inappropriate content generation.

(k) Training and Awareness:

1. **Required Training Programs**: Agencies and departments must implement AI training programs:
   i. **Executive-level Training**: AI governance principles, risk management approach, and strategic considerations.
   ii. **AI Coordinator Training**: Implementation procedures, risk assessment methodology, documentation requirements, monitoring and oversight responsibilities.
   iii. **User-Level Training**: Appropriate AI use cases, security and privacy considerations, oversight responsibilities, and incident reporting procedures.
   iv. **Technical Implementation Training**: Security controls implementation, monitoring techniques, bias detection and mitigation, and system maintenance procedures.
2. **Specialized Training**: Additional specialized training is required for specific roles:
   i. **High-Risk System Operators**: Advanced risk management, fairness and bias mitigation, adversarial testing, and ethical considerations.
   ii. **AI Procurement Specialists**: Vendor assessment procedures, contractual requirements, and ongoing vendor management.
   iii. **GenAI Users**: Prompt engineering best practices, content review procedures, proper attribution and disclosure.

(l) **AI Shared Responsibility Model**: The State of Idaho adopts a shared responsibility model for AI governance to clearly delineate the roles and responsibilities between ITS and individual agencies or departments:

1. **ITS as the Foundation**: ITS serves as the central hub for AI governance, providing the foundation that agencies and departments can build upon. ITS shall be responsible for:

i. Establishing the statewide AI governance framework, policies, and standards
ii. Developing risk assessment methodologies and assigning risk scores
iii. Approving high-risk implementations in coordination with AI Executive Committee review
iv. Maintaining the state's AI system inventory
v. Coordinating enterprise-wide AI initiatives and shared services
vi. Developing standardized templates and assessment tools
vii. Providing technical consultation and advisory services

2. **Agencies and Departments as the Implementers**: Agencies and Departments shall be responsible for:
   i. Partnering with ITS to support risk assessments for their proposed AI implementations
   ii. Developing agency or department-specific use cases and implementation plans
   iii. Ensuring compliance with ITS policies and standards
   iv. Maintaining appropriate documentation for AI systems
   v. Implementing required security and privacy controls
   vi. Conducting ongoing monitoring and assessment of agency and department AI systems
   vii. Managing vendor relationships for agency and department-specific AI implementations
   viii. Ensuring proper training of agency and department personnel on responsible AI use
3. **Shared Responsibility Implementation**: The shared responsibility model defines how ITS, agencies and departments work together to implement AI governance. Appendix A outlines specific information on governance, risk management, implementation, and privacy and security activities, including who leads each activity and who assists (or provides input).

Related Policies	P.ITS-01

(S.ITS-02) Solution Vetting Process

(S.ITS-02a) Solution Vetting Board

(a) Solution Vetting Board (SVB) members must include at least one member from:
1. Enterprise Architecture (EA)
2. Governance, Risk, and Compliance (GRC)
3. Privacy (PRV)
4. Security (SEC)
5. The solution vetting process owner

(b) The SVB functions include:
1. Shareholder Communication: Serve as liaison maintaining alignment between teams and sharing experiences
2. Focus Group: Develop and enhance processes, standards, and guidelines applicable to existing and missing methodologies
3. Request Oversight: Oversee the progress of request through the Solution Vetting Process (SVP)

(S.ITS-02b) Solution Vetting Process

(a) Authorization:
1. All solutions must be processed through the SVP prior to being configured, deployed, or used
2. Unapproved Solutions:
   i. Must not be installed, executed, or used on any device that connects to or accesses the State network or State data, or used with any such device
   ii. Will be removed upon discovery

(b) Documentation Requirements:
1. All solution vetting submissions must include:
   i. Vendor Documentation, including:

(A) Contracts (EG: EULA, ToS, ToU, Privacy, Data Usage, etc.)
(B) Configuration/Installation requirements
(C) Vendor Solution Questionnaire
ii. Version details
iii. Intended data classification
iv. Intended use case
v. Requester's Solution Vetting Request questionnaire

(c) Vetting Process:
1. Contract Verification: Contracts must be reviewed to ensure compliance with ITS and legal requirements
2. Enterprise Requirements:
i. Solution Rationalization: Reduce solution redundancy by evaluating solutions against existing approved solutions and requester's need
ii. Fit for the State's Network: Evaluate if the solution fits the state architectural roadmap
iii. Vendor Reliability: Analysis of the solution vendor's reputation, support capabilities, and financial stability to mitigate risks of vendor failure or abandonment
3. Governance Requirements:
i. Data Governance: Examination of how the solution collects, stores, and processes data to ensure proper handling of sensitive data or personal information
ii. Policy Compliance: Verify solution complies with documented policies
iii. Regulatory Adherence: Asses to ensure the solution meets relevant legal and regulatory requirements
4. Privacy Requirements:
i. Data Protection: Solution must comply with privacy requirements by ensuring:
(A) Data Minimization: Data must only be collected, retained, or used when it is necessary to meet the specific business purpose for which the solution is designed
(B) Transparency: Users and administrators are informed about how data is collected, processed, stored, and shared
(C) Consent Management: Mechanisms exist to obtain and manage user consent where required by regulations
(D) Reasonable Protection: Appropriate administrative and physical safeguards exist to protect State data
(E) Right to Erasure: Reasonable options exist for the deletion of State and account related data
(F) Right to Access: Reasonable options exist for the State to access State data
(G) Third-Party Sharing: Any sharing of State data with third parties is disclosed and complies with our contractual and legal obligations
5. Security Requirements:
i. Security Assessment: Solution evaluation must determine:
(A) Vulnerabilities
(B) Permission requirements
(C) Network requirements
(D) Fundamental behavior
ii. Configuration Check: Solution deployment and configuration must be evaluated
iii. Compatibility Check: Solutions must be evaluated for compatibility with existing supported information systems and infrastructure
iv. Accountability: Solution must be able to log events defined in (S.AU-01) Event Logging
v. Least Privilege: Solution must follow the practice of least privilege and not request access or preform actions unneeded for intended functionality as understood by the state
6. Risk Assessment:
i. Risk Reporting: Archive finding of vetting that can produce reporting that includes:
(A) Contract Risks: Issues with compliance or governance within the contract
(B) Data Risks: Potential threats to data integrity, confidentiality, and availability

(C) Architectural Risks: Vendor reliability, feature redundancy, deviation from ITS architectural plans
(D) Governance Risks: Issues with compliance or governance with solution use case
(E) Network Risks: Non-compliant protocols and configurations
(F) Security Risks: Exploitability and impact of misuse or misconfiguration

7. Functionality Testing: Solutions must be tested in a controlled environment to verify functionality and assess potential risks
8. Prohibition: Solutions suspected to have substantial risk(s) to Productivity, Compliance, Privacy, or Security will be marked as "Prohibited" based on the quantity and quality of the risks and the probability of those risks

(S.ITS-02c) Risk Variance or Exception Handling

(a) A Risk Variance may be submitted for solutions rejected by the SVB. The Risk Variance must contain:
1. Threat and Vulnerability Assessment (TVA) report
2. Risk Management Plan (RMP) to be enforced after variance approval
3. Risk Exit Strategy (RES) to be enforced after variance approval
4. Signed acknowledgement of completeness and correctness by each of the following:
   i. ITS Risk Officer
   ii. Requester
5. Signed acknowledgement of review of the variance and the individual's documented approval or denial decision by:
   i. Requesting agency's manager
   ii. Director or documented authorized proxy of all identified affected agencies
   iii. ITS Chief Information Security Officer (CISO)
   iv. ITS Chief Information Officer (CIO)
6. Section 4.b.2.v collections of signatures and decisions do not need to be completed if any person in section 4.b.2.v signs and enters a non-approving decision

(b) Exception Handling:
1. Requests for an exception to this policy must be submitted in writing with one individual solution per request

(S.ITS-02d) Solution Lifecycle

(a) Monitoring and Enforcement: ITS conducts regular audits to identify unauthorized software and ensure continued compliance with this policy

(b) Continuous Solution Validation:
1. Solutions approved through the vetting process will be regularly re-evaluated
2. Solutions approved through the risk variance process will be replaced by an appropriate solution per their RES
3. The frequency of re-evaluation for approved solutions is determined based off solution risk score

(c) Record Retention:
1. Decisions and documentation generated by the solution vetting process must follow the record retention schedule
2. Decisions and documentation generated by the risk variance process must follow the record retention schedule

Appendix

Appendix A – ITS Defined Timelines

Table 11 ITS Defined Timelines

Policy	What needs reviewed/updated/tested	Timeline
AC-02(u)	Disable accounts of users within thirty (30) minutes but no later than one (1) day of discovery of direct threats to the confidentiality, integrity, or availability of State Data	30 minutes
AC-07(a)1.	When the maximum number of unsuccessful attempts is exceeded for all accounts enforce a limit of three (3) consecutive invalid logon attempts by a user during a 120-minute period	120 minutes
AC-07(a)2.	When the maximum number of unsuccessful attempts is exceeded for all accounts automatically lock the account for fifteen (15) minutes; or until released by an administrator; delays next logon prompt when the maximum number of unsuccessful attempts is exceeded	15 minutes
AC-11(a)	System must prevent further access to the System by initiating a device lock after fifteen (15) minutes of inactivity; requiring the user to initiate a device lock before leaving the System unattended	15 minutes
AC-12(a)	Systems must be configured to automatically terminate a user session after thirty (30) minutes of inactivity	30 minutes
AC-17(g)	Provide the capability to disconnect or disable remote access to System within fifteen (15) minutes	15 minutes
AC-17(j)	Automatically disconnect remote sessions after fifteen (15) minutes of inactivity	15 minutes
SC-10	Configure Systems to terminate sessions and require users to re-authenticate to re-activate a terminal or session if a session has been idle for more than thirty (30) minutes	30 minutes
AC-02(q)	Require users to log out when users expect inactivity longer than four (4) hours	4 hours
AU-05(a)	Alert State personnel with audit and accountability responsibilities, SysAdmins, and NetOps within one (1) hour in the event of an audit logging process failure	1 hour
AU-05(c)	Provide a warning to the SecOps within twenty-four (24) hours when allocated audit record storage volume reaches (75%) of repository maximum audit record storage capacity	24 hours
IA-11(e)	Personnel must re-authenticate every twelve (12) hours	12 hours
IR-06(a)	All State personnel to report suspected security incidents to the Service Desk immediately but not to exceed one (1) hour after discovery	1 hour
PS-04(a)	Disable System access accounts within twenty-four (24) hours of the personnel termination	24 hours
PS-08(b)	Notify designated agency personnel within seventy-two (72) hours when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction	72 hours
SI-02(i)	Ensuring that, upon daily power up and connection to the ITS' network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than once every 24 hours (excluding weekends, holidays, etc.)	24 hours
P.ITS-01(j)3.	Vendors must report incident information immediately to ITS, but no later than twenty (24) hours after identification of a possible issue involving State data	24 hours
AC-02(h)1.	Notify account managers and designated agency officials within one (1) day when accounts are no longer required	1 day
AC-02(h)2.	Notify account managers and designated agency officials within one (1) day when users are terminated or transferred	1 day
AC-02(h)3.	Notify account managers and designated agency officials within one (1) day when system usage or need-to-know changes for an individual	1 day
AC-02(n)	Automatically disable and remove temporary and emergency accounts after two (2) business days	2 days
AC-02(o)4.i.	Disable accounts when that account has been inactive for ninety (90) days for non-privileged accounts	90 days
AC-02(o)4.ii.	Disable accounts when that account has been inactive for sixty (60) days for privileged accounts	60 days
AC-02(o)5.	Delete accounts within ninety (90) days after accounts have been disabled	90 days
AT-02(a)2.	Provide security and privacy literacy training to System users (including managers, senior executives, and contractors) when required by System changes, following assessment or audit findings, within thirty (30) days of any security or privacy incidents, or changes to applicable laws, executive orders, directives, regulations, polices, standards, and guidelines	30 days
AU-11(a)1.	For Systems where State Data is Handled log entries must be immediately available for a minimum of ninety (90) days (online)	90 days

Policy	What needs reviewed/updated/tested	Timeline
CP-03(a)i.	Provide contingency training to System users consistent with assigned roles and responsibilities within thirty (30) days of assuming a contingency role and responsibility	30 days
IA-04(e)1.	Disable identifiers after ninety (90) days of inactivity	90 days
IA-04(e)2.	Disable privileged accounts after sixty (60) days of inactivity	60 days
IR-02(a)1.	Provide incident response training to users consistent with assigned roles and responsibilities within thirty (30) days of assuming an incident response role or responsibility or acquiring system access	30 days
PS-05(b)	Initiate ITS-defined transfer or reassignment actions within five (5) days following the formal transfer action	5 days
PS-05(d)	Upon transfer or personnel, ITS Management must Notify designated agency personnel within five (5) business days, as required	5 days
PS-07(d)	Require external providers to notify ITS of any personnel transfers or terminations of external personnel who possess ITS credentials and/or badges, or who have information system privileges within three (3) business days	3 days
RA-05(d)1.	remediate critical legitimate vulnerabilities within fifteen (15) days	15 days
RA-05(d)2.	remediate high legitimate vulnerabilities within thirty (30) days	30 days
RA-05(d)3.	remediate medium legitimate vulnerabilities within sixty (60) days	60 days
RA-05(d)4.	remediate low legitimate vulnerabilities within ninety (90) days	90 days
RA-05(g)	Update the System vulnerabilities scanned at least every thirty (30) days; prior to a new scan, and when new vulnerabilities are identified and reported	30 days
RA-05(o)1.	For assets within scope for PCI DSS, ITS is required to perform external network vulnerability scans via an Approved Scanning Vendor (ASV), at least once every ninety (90) days or after any significant change in the network and include rescans until passing results are obtained, or all “High” vulnerabilities as defined in the PCI DSS are resolved	90 days
RA-05(o)2.	For assets within scope for PCI DSS, ITS is required to perform internal network vulnerability scans at least once every ninety (90) days or after any significant change in the network and include rescans until passing results are obtained, or all “High” vulnerabilities as defined in the PCI DSS are resolved	90 days
SA-04(j)7.	Require all data to be removed from the contractor’s System and returned to ITS within seven (7) calendar days prior to contract termination	7 calendar days
SC-07(r)	IRS-defined) ITS must block known malicious sites (inbound or outbound), as identified to ITS from US-CERT, MS-ISAC, or other sources, at each internet access point (unless explicit instructions are provided to agencies not to block specific sites). Blocking is to be accomplished within two (2) business days following release of such sites	2 days
SI-02(c)1.	Installing security-relevant software and firmware updates based on severity and associated risk to the confidentiality of data for critical within ten (10) days of release from the vendor	10 days
SI-02(c)2.	Installing security-relevant software and firmware updates based on severity and associated risk to the confidentiality of data for high within thirty (30) days of release from the vendor	30 days
SI-02(c)3.	Installing security-relevant software and firmware updates based on severity and associated risk to the confidentiality of data for medium within sixty (60) days of release from the vendor	60 days
SI-02(c)4.	Installing security-relevant software and firmware updates based on severity and associated risk to the confidentiality of data for low within ninety (90) days of release from the vendor	90 days
AU-13(a)	Monitor open-source information daily for evidence of unauthorized disclosure of agency information	Daily
PE-03(i)	Perform security checks at a minimum daily at the physical perimeter of the facility or supported	Daily
SC-45(a)	Compare the internal System clocks daily with the official NIST or USNO Internet Time Service	Daily
SI-02(e)	Determining if System components have applicable security relevant software and firmware updates installed using automated mechanisms at a minimum daily for network workstations and malicious code protection	Daily
SI-02(i)	Ensuring that, upon daily power up and connection to the ITS’ network, workstations (as defined in policy and including remote connections using GFE workstations) are checked to ensure that the most recent agency-approved patches have been applied and that any absent or new patches are applied as necessary or otherwise checked not less than once every 24 hours (excluding weekends, holidays, etc.)	Daily
AC-02(o)1.	Disable accounts within one (1) week when the account has expired	1 week
AC-02(o)2.	Disable accounts within one (1) week when the account is no longer associate with a user or individual	1 week
AC-02(o)3.	Disable accounts within one (1) week when the account is in violation of ITS policy	1 week
AC-02(o)4.i.	Disable accounts within one (1) week when the account has been inactive for ninety (90) days for non-privileged accounts	1 week
AC-02(o)4.ii.	Disable accounts within one (1) week when the account has been inactive for sixty (60) days for privileged accounts	1 week

Policy	What needs reviewed/updated/tested	Timeline
AU-06(a)	Review and analyze System audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity	Weekly
CM-11(d)	(FBI-defined) Monitor policy compliance through automated methods at least weekly	Weekly
CP-09(a)	Conduct backups of user-level information contained in the System documentation, including security-related documentation, weekly	Weekly
CP-09(b)	Conduct backups of System-level information contained in the System weekly	Weekly
CP-09(c)	Conduct backups of System documentation, including security- and privacy- related documentation weekly	Weekly
SI-03(c)1.	Perform periodic scans of the System and implement weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with agency security policy	Weekly
AC-04(k)	ITS Management is responsible for implementing a review of firewall and router rule sets at least once every six (6) months to ensure least privileges and best practices are being followed	6 months
CA-05(d)	Enter all new weaknesses into appropriate POAMs within two (2) months for weaknesses identified during assessments	2 months
CA-08(g)	External and internal penetration testing must include reviews and considerations of threats and vulnerabilities experienced in the last twelve (12) months	12 months
PE-03(f)	Inventory ITS-defined physical access devices every twelve (12) months	12 months
PE-06(b)	Review physical access logs at a minimum monthly and upon occurrence of a potential indication of an event	Monthly
PE-08(b)	Review visitor access records at least monthly	Monthly
RA-05(a)	Monitor and scan for vulnerabilities in the System and hosted applications at a minimum of monthly for all Systems and when new vulnerabilities potentially affecting the Systems are identified and reported	Monthly
SI-02(e)	Determine if System components have applicable security relevant software and firmware updates installed using automated mechanisms at a minimum monthly, daily for network workstations and malicious code protection	Monthly
CA-05(d)	Review the content on the publicly accessible System for nonpublic information at a minimum quarterly and remove such information, if discovered	Quarterly
AT-02(g)	Distribute security and privacy awareness reminders/updates to all users on at least a quarterly	Quarterly
AT-02(h)	Conduct phishing email simulation exercises on at least a quarterly basis	Quarterly
CA-05(b)	Update existing POAMs quarterly, at a minimum, based on the findings from policy assessments, independent audits or reviews, and continuous monitoring activities	Quarterly
SC-40(a)	Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis	Quarterly
SC-40(e)	Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities. If automated monitoring is utilized (e.g., wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel	Quarterly
SI-08(c)	Automatically update spam protection mechanisms at minimum quarterly	Quarterly
XX-01(b)1.	Review ITS policies annually	Annually
XX-01(b)2.	Review ITS procedures annually	Annually
AC-02(j)1.	Review accounts for compliance with account management requirements annually for standard user accounts	Annually
AC-02(j)2.	Review accounts for compliance with account management requirements bi-annually for standard user accounts	Bi-Annually
AC-06(d)1.	Review of user privileges annually the privileges assigned to State Data to validate the need for such privileges	Annually
AT-02(a)3.	Provide security and privacy literacy training to System users (including managers, senior executives, and contractors annually	Annually
AT-02(c)	Update literacy training and awareness content annually and following System changes	Annually
AT-03(a)2.	Provide role-based security and privacy training to personnel with the roles and responsibilities defined in (S.AT-01) Role-Based Training Content annually	Annually
AT-03(b)	Update role-based training content annually and following System changes	Annually
AT-03(c)	Update literacy training and awareness content annually and following System changes	Annually
AT-04(c)	State personnel must acknowledge in writing or electronically, at least annually, that they have read and understand ITS' cybersecurity policies	Annually
AU-02(e)	Review and update the audited events at a minimum, annually	Annually
CA-02(d)	Assess the policies in the system and its environment of operation annually to determine the extent to which the policies are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements	Annually
CA-03(c)	Review and update information exchange agreements on an annual basis	Annually

Policy	What needs reviewed/updated/tested	Timeline
CA-07(a)	Develop a System-level continuous monitoring strategy and implement continuous monitoring in accordance with ITS' continuous monitoring strategy that establishes ITS-defined metrics to be monitored annually, at a minimum	Annually
CA-07(b)	Develop a System-level continuous monitoring strategy and implement continuous monitoring in accordance with ITS' continuous monitoring strategy that establishes ITS-defined frequency (no less than annually) for monitoring and ITS-defined frequencies (no less than annually) for ongoing assessment of security and privacy control effectiveness	Annually
CA-07(g)	Develop a System-level continuous monitoring strategy and implement continuous monitoring in accordance with ITS' continuous monitoring strategy that reporting the security and privacy status of the System to Executive Leadership annually	Annually
CA-08(i)	External and internal penetration testing must include internal and external testing that occurs at least annually and after any significant infrastructure or application upgrade or modification (such as an operating System upgrade, a sub-network added to the environment, or a web server added to the environment)	Annually
CA-09(d)	Review annually the continued need for internal connections	Annually
CM-02(b)1.	Review and update the baseline configuration of the System at a minimum annually	Annually
CM-05(b)1.	Review and reevaluate privileges semi-annually	Semi-Annually
CM-07(c)	Review the System annually to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services	Annually
CM-07(e)3.	Review and update the list of authorized software programs at a minimum annually	Annually
CM-07(f)3.	Review and update the list of authorized hardware components annually	Annually
CM-08(b)	Review and update the System component inventory at a minimum annually	Annually
CM-11(c)	Monitor policy compliance at a minimum annually	Annually
CP-02(d)	Review the contingency plan for Systems annually	Annually
CP-03(a)3.	Provide contingency training to System users consistent with assigned roles and responsibilities annually	Annually
CP-03(b)	Review and update contingency training content annually	Annually
CP-04(a)	Test the contingency plan for Systems at a minimum, annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan	Annually
CP-09(f)	Test backup information annually to verify media reliability and information integrity	Annually
IR-02(a)3.	Provide incident response training to users consistent with assigned roles and responsibilities annually	Annually
IR-03(a)	Test the effectiveness of the incident response capability for the System annually using tabletop exercises at least annually	Annually
IR-08(a)9.	Develop an incident response plan that is reviewed and approved by designated agency officials at a minimum on an annual basis	Annually
MA-03(b)	Review previously approved System maintenance tools on at least an annual basis	Annually
MA-04(e)	Conduct media inventories at least annually	Annually
PE-02(c)	Review access list detailing authorized ITS facility access by individuals at least annually	Annually
PE-03(g)4.	Change combinations and keys at least annually	Annually
PL-02(c)	Review security and privacy plans at a minimum annually (or as a result of a significant change)	Annually
PL-04(c)	Review and update the rules of behavior at a minimum annually	Annually
PL-08(b)	Review and update the security architectures at a minimum annually to reflect changes in the enterprise architecture	Annually
PM-11(c)	Review and revise the mission and business processes annually	Annually
PS-06(b)	Review and update access agreements, at least annually	Annually
PS-06(c)2.	Personnel must re-sign access agreements to maintain access to ITS Systems when access agreements have been updated or at least annually	Annually
RA-03(d)	Review risk assessment results at least annually	Annually
SA-15(c)	Developers must be properly trained in current, secure coding techniques	Annually
SC-03(j)	If segmentation is used to isolate the sensitive networks from other networks, penetration tests must be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope Systems from in-scope Systems	Annually
SC-07(e)5.	Review external telecommunications service exceptions to the traffic flow policy annually, after any incident, and after any major changes impacting the System, while removing exceptions that are no longer supported by an explicit mission or business need	Annually
SC-07(g)2.	Auditing must be performed semi-annually on each workstation with split tunneling enabled	Semi-annually
SC-07(k)2.	Prevent exfiltration by conducting exfiltration tests at least semi-annually	Semi-annually
SI-07(c)4.	Perform an integrity check of software, firmware, and information annually	Annually
SR-06	Assess and review the supply-chain related risks associated with suppliers or contractors and the system, system component, or system service they provide at a minimum annually	Annually
P.ITS-01(a)1.v.	Conduct risk assessments on GAI tools on the network	Annually

Policy	What needs reviewed/updated/tested	Timeline
AT-02(i)6.	Training certification and recertification must be documented and placed in ITS files for review and retained for at least five (5) years	5 years
AT-04(b)	Retain individual training records for five (5) years	5 years
CA-06(d)	Update the authorizations whenever there is a significant change to the System, or every three (3) years, whichever occurs first	3 years
CA-08	Conduct penetration testing every three (3) years on the ITS environment	3 years
CP-03(b)	Review and update contingency training content every three (3) years and following	3 years
IA-05(b)	Maintain a list of commonly used, expected, or compromised passwords and update the list every three (3) years and when ITS passwords are suspended to have been compromised directly or indirectly	3 years
PE-08(a)	Maintain visitor access records to the facility where Systems reside for five (5) year	5 years
PM-01(b)	Review the ITS-wide data Security Program Plan every three (3) years and following significant changes	3 years
PE-08(c)	Review and update the risk management strategy every three (3) years or as required, to address agency changes	3 years
PM-18(b)	Update the Privacy Program Plan every three (3) years and to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments	3 years
PM-21(c)	Retain the accounting of disclosures for the length of the time the PII is maintained or five (5) years after the disclosure is made, whichever is longer	5 years
PS-02(c)1.	Review and update position risk designations every three (3) years	3 years
PS-03(b)	Rescreen individuals in accordance with agency defined conditions requiring rescreening but no less than once every five (5) years	5 years
RA-03(f)	Update the risk assessment at least every three (3) years or when there are significant changes to the System, its environment of operation, or other conditions that may impact the security or privacy state of the System	3 years
RA-03(g)2.	Update the supply chain risk assessment every three (3) years, when there are significant changes to the relevant supply chain, or when changes to the System, environments of operation, or other conditions may necessitate a change in the supply chain	3 years
SR-02(b)	Review and update the supply chain risk management plan every three (3) years or as required, to address threat, organizational or environmental changes	3 years

Appendix B – Framework Mapping

The table below maps the frameworks ITS must be in compliance with to NIST SP 800-53 r5.

NIST	NIST SP 800-53 r5 / ITS Information Security Policy Manual 3.0
ITA	Idaho Technology Authority - Policies/Standards/Guidelines
CSF	NIST Cybersecurity Framework
FTI	IRS Publication 1075
CJI	FBI Criminal Justice Information Services Security Policy
SSA	Social Security Administration Technical System Security Requirements
PCI	Payment Card Industry Data Security Standard
PHI	Implementing the Health Insurance Portability and Accountability Act Security Rule
Privacy	NIST Privacy Framework
CUI	NIST SP 800-171
CSC	The 18 CIS Critical Security Controls

Table 12 Framework Mapping

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
AC-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03, PR.AA-01, PR.AA-05	4.1.AC-1	AC-1	2.1.AC-01	8.1, 8.4	164.312(a)(a)	PB,GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CT.PO-P2, CT.PO-P3, PR.AC-P3, PR.AC-P4	03.15.01	6.1, 6.2
AC-02	P4502, P4590, S6010	PR.AA-01, PR.AA-05, PR.DS-10, DE.CM-01, DE.CM-03	4.1.AC-2	AC-2	2.1.AC-02	8.1.3-8.1.5, 8.2.2, 8.2.6, 8.5, 8.5.1, 8.6, 8.7,	164.312(d), 164.312(a)(2)(iii), 164.308(a)(4(ii)(A) and (B) and (C)	CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4	03.01.01	4.3, 5.1, 5.3, 5.5, 5.6, 6.1, 6.2, 6.7, 6.8, 12.5
AC-03		PR.AA-05, PR.DS-10, PR.IR-01	4.1.AC-3	AC-3	2.1.AC-03	7.1, 7.1.1-7.1.4, 7.2, 7.2.1, 7.2.3	164.308(a)(4(i) and (ii)	PB, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.AC-P4, PR.PT-P2	03.01.02	3.3, 6.7
AC-04	P4501, P4570	ID.AM-03, PR.DS-10, PR.IR-01, DE.CM-09	4.1.AC-4	AC-4, 5.10.1		1.1.3, 1.1.6, 1.1.7, 1.3.1, -1.3.7		CT.DM-P2, PR.AC-P5, PR.DS-P5	03.01.03	3.8
AC-05		PR.AA-05	4.1.AC-5	AC-5, 5.13.6	2.1.AC-05	6.4.2		PR.AC-P4, PR.DS-P5	03.01.04	3.3, 6.8
AC-06	P4501, P4502	PR.AA-05	4.1.AC-6	AC-6, 5.13.6	2.1.AC-06	7.1, 7.1.2,		PR.AC-P4, PR.DS-P5	03.01.05 03.01.06 03.01.07	3.3, 3.14, 5.4, 6.8
AC-07	P4550, S2140, G540	PR.AA-03	4.1.AC-7	AC-7	2.1.AC-07	8.3.4			03.01.08	4.10
AC-08			4.1.AC-8	AC-8	2.1.AC-08			CM.AW-P1	03.01.09	
AC-09		DE.CM-09								
AC-10		PR.AA-05						PR.AC-P5		
AC-11			4.1.AC-11	5.5.AC-11	2.1.AC-11	8.1.8			03.01.10	4.3
AC-12		PR.AA-03	4.1.AC-12	5.5.AC-12		8.1.8, 12.3.8	164.312(a)(b)(iii)	PR.PT-p3	03.01.11	4.3

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
~~AC-13~~										
AC-14		PR.AA-01	4.1.AC-14	5.5.AC-14				PR.AC-P4, PR.AC-P6		
~~AC-15~~										
~~AC-16~~		PR.AA-05						CT.DM-P7, CT.DP-P5, CM.AW-P6, PR.AC-P4, PR.AC-P6		
AC-17	P4502	PR.AA-05	4.1.AC-17	5.5.AC-17	2.1.AC-17	8.1.5, 8.3.2, 12.3.8, 12.3.9, 12.3.10		PR.AC-P3, PR.PT-P3	03.01.12	3.10, 12.7, 12.8, 13.5
AC-18	P3020, P4540, P4570, S3530, G530	PR.AA-05	4.1.AC-18	5.5.AC-18, 5.13.1, 5.13.1.1, 5.13.1.3, 5.13.1.4		9.1.3, 11.1.1		PR.PT-P3	03.01.16	4.2, 12.6
AC-19	P1060, P4540, P4550, S3530, S2140, G540, G550	PR.AA-05	4.1.AC-19	5.5.AC-19, 5.13.1.2.1, 5.13.1.2.2, 5.13.1.4, 5.13.2, 5.13.3, 5.13.7.2.1, 5.13.7.3				PR.AC-P3	03.01.18	4.10, 4.11, 4.12, 6.4
AC-20	P4550, S2140, G540	ID.AM-02, ID.AM-04	4.1.AC-20	5.5.AC-20				PR.AC-P3	03.01.20	4.11, 15.2, 15.3, 15.5
AC-21			4.1.AC-21	5.5.AC-21, 5.1.1, 5.1.1.1 - 5.1.1.6, 5.1.1.8				CT.DM-P2, PR.PO-P6		15.2
AC-22	P5040		4.1.AC-22	5.5.AC-22, 5.10.1.1.6					03.01.22	14.5
AC-23			4.1.AC-23					CT.DP-P1, CT.DP-P2, CT.DP-P3		
~~AC-24~~		PR.AA-05						PR.AC-P4		
~~AC-25~~										
AT-01	P1010, P4130, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.2.AT-1	5.2.AT-1	2.3.AT-1	12.6		PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6	03.15.01	14.1
AT-02	P4505, P4590, S6010	PR.AT-01	4.2.AT-2	5.2.AT-2	2.3.AT-2	12.6.1	164.308(a)(5)(i), 164.308(a)(5)(ii)(A)	PB, GV.AT-P1	03.02.01	14.1, 14.2, 14.3, 14.4, 14.6, 14.7, 14.8
AT-03	P4505	PR.AT-01, PR.AT-02	4.2AT-3	5.2.AT-3	2.3.AT-3	6.5, 9.9.3, 12.6.1, 12.10.4		PB, GV.AT-P1, GV.AT-P2, GV.AT-P3, GV.AT-P4	03.02.02	14.9
AT-04			4.2.AT-4	5.2.AT-4	2.3.AT-4	12.6.2		PB		
~~AT-05~~										
AT-06			4.2.AT-6	3.2.10						
AU-01	P1010, P4140	GV.OC-03, GV.PO-01,	4.3.AU-1	5.4.AU-1	2.2.AU-1	10.1	164.312(b)	PB, GV.PO-P1, GV.PO-P3, GV.PO-	03.15.01	8.1

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
		GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03						P5, GV.MT-P2, GV.MT-P6, CT.DM-P8		
AU-02	P1030, P4501, P4502	PR.PS-04	4.3.AU-2	5.4.AU-2	2.2.AU-2	10.2.1		PB, CT.DM-P8	03.03.01	3.14, 8.1, 8.2, 8.6, 8.7, 8.8, 8.12
AU-03		PR.PS-04	4.3.AU-3	5.4.AU-3	2.2.AU-3	10.3, 10.3.1-10.3.6		PB, CT.DM-P8, CT.DP-P2	03.03.02	8.5
AU-04			4.3.AU-4	5.4.AU-4		10.7		PR.DS-P4		8.3
AU-05			4.3.AU-5	5.4.AU-5					03.03.04	
AU-06	P4570, P4590, S6010	PR.PS-04, DE.AE-02, DE.AE-03	4.3.AU-6	5.4.AU-6	2.2.AU-6	10.6, 10.6.1, 10.6.2, 10.6.3		ID.DE-P5, CT.DM-P8	03.03.05	8.9, 8.11, 13.1
AU-07		PR.PS-04, RS.AN-03, RS.AN-06, RS.AN-07	4.3.AU-7	5.4.AU-7	2.2.AU-7			CT.DM-P8	03.03.06	8.2, 8.4, 8.5, 8.11, 13.1
AU-08			4.3.AU-8	5.4.AU-8		10.4, 10.4.1-10.4.3			03.03.07	8.4
AU-09	P4502, P4505	PR.DS-10	4.3.AU-9	5.4.AU-9	2.2.AU-9	10.5, 10.5.1-10.5.5	164.312(c)(a)		03.01.05, 03.03.08	6.8
AU-10	P1030					10.5.5	164.312(c)(b)			
AU-11	P1030	PR.PS-04	4.3.AU-11	5.4.AU-11	2.2.AU-11	10.7		PB	03.03.03	3.1, 3.4, 8.10
AU-12		PR.PS-04, DE.CM-01, DE.CM-03, DE.CM-09	4.3.AU-12	5.4.AU-12	2.2.AU-12			CT.DM-P6, CT.DM-P8	03.03.03	3.14, 8.2, 8.5
AU-13	P4150, P4590, S6010	PR.DS-10, DE.CM-03				12.5.5		CT.DM-P8, PR.DS-P5		
AU-14								CT.DM-P8		
~~AU-15~~										
AU-16	P1080, P4120	PR.DS-02	4.3.AU-16					CT.DM-P8, CT.DP-P1, CT.DP-P3		
CA-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.4.CA-1	CA-1				PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6	03.15.01	
CA-02	P4130, P4520	ID.RA-01, ID.IM-01, ID.IM-02, ID.IM-03	4.4.CA-2	CA-2	2.12.CA-2			PB, ID.DE-P5, GV.MT-P3, CT.DM-P9, PR.PO-P5	03.12.01	

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
CA-03	P4550, P4570, S2140, G540	ID.AM-03, PR.DS-01, PR.DS-02, PR.DS-10	4.4.CA-3	CA-3	2.12.CA-3				03.12.05	
~~CA-04~~										
CA-05		ID.IM-01, ID.IM0-2, ID.IM-03	4.4.CA-5	CA-5				PB, ID.RA-P5, GV.MT-P4	03.12.02	16.2
CA-06			4.4.CA-6	CA-6		12.3.1		PB		
CA-07	P4150	ID.RA-01, ID.RA-07, ID.IM-01, ID.IM-02, ID.IM-03, DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-06, DE.CM-09, DE.AE-02, DE.AE-03	4.4.CA-7	5.4.3,	2.12.CA-7	10.6, 10.6.1, 10.6.2		PB, ID.DE-P5, GV.MT-P1, GV.MT-P3, CT.DM-P9, PR.PO-P5, PR.PO-P6	03.12.03	3.13
CA-08		ID.RA-01, ID.IM-01, ID.IM-02, ID.IM-03	4.4.CA-8			11.3-11.3.3		PR.PO-P5		18.1
CA-09		ID.AM-03	4.4.CA-9	5.7.1.1, 5.7.1.2, 5.7.2		1.1.2,1.1.3				4.4, 13.4
CM-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03, PR.PS-01	4.5.CM-1	5.7.CM-1				PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P1	03.15.01	4.1
CM-02	S2140, P3030, G950	PR.PS-01	4.5.CM-2	5.7.CM-2		1.1.1, 1.2.2, 6.4.1 - 6.4.4		CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.DS-P7	03.04.01, 03.04.12	4.1, 4.2
CM-03		ID.RA-07, PR.PS-01, DE.CM-01, DE.CM-09	4.5.CM-3	5.7.CM-3		6.4.5, 6.4.6		CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, PR.PO-P1, PR.PO-P2	03.04.03	
CM-04		ID.RA-07, PR.PS-01	4.5.CM-4	CM-04		6.4, 6.4.5, 6.4.5.1-6.4.5.4		PB, GV.MT-P1, GV.MT-P5, CT.DM-P9, PR.PO-P1, PR.PO-P2	03.04.04	
CM-05	P4502	PR.PS-01	4.5.CM-5	5.7.CM-5		6.4.2, 6.4.4		PR.PO-P1	03.04.05	
CM-06		PR.PS-01, DE.CM-09	4.5.CM-6	5.7.CM-6				CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DP-P4, PR.PO-P1	03.04.02	4.1, 4.2, 4.8, 12.3, 13.9, 16.7
CM-07	P4501, P4502, P4520, P4570	PR.PS-01, PR.PS-03, PR.PS-05	4.5.CM-7	5.7.CM-7		7.1.1 - 7.1.4, 7.2.2		PR.PO-P1, PR.PT-P2	03.04.06, 03.04.08	2.1, 2.3, 2.5, 2.6, 2.7, 4.1, 4.2, 4.6, 4.8, 12.2,

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
										12.3, 13.9, 16.7
CM-08		ID.AM-01, ID.AM-02, PR.PS-01	4.5.CM-8	5.7.CM-8		2.4	164.310(d)(b)(iii)	ID.IM-P1, ID.IM-P2, ID.IM-P7, PR.DS-P3	03.04.10	1.1, 1.2, 1.4, 1.5, 2.1, 2.3, 2.4, 6.6, 12.1, 16.4
CM-09		ID.AM-08, PR.PS-01	4.5.CM-9	5.7.CM-9		6.4		CT.PO-P2, PR.PO-P1		4.1, 4.2
CM-10		PR.PS-01, DE.CM-03, DE.CM-09	4.5.CM-10	5.7.CM-10						2.3, 2.5, 9.1, 9.4
CM-11		PR.PS-01, PR.PS-02, DE.CM-03, DE.CM-09	4.5.CM-11	5.7.CM-11						2.3, 9.4
CM-12		ID.AM-07	4.5.CM-12	5.7.CM-12				ID.IM-P1, ID.IM-P7	03.04.11	3.1, 3.2, 3.8, 3.13
CM-13		ID.AM-07, ID.AM-08	4.5.CM-13					ID.IM-P1 ID.IM-P2, ID.IM-P3, ID.IM-P4, ID.IM-P5, ID.IM-P6, ID.IM-P7, ID.IM-P8, ID.RA-P1, ID.RA-P3, GV.MT-P1		
CM-14			4.5.CM-14							
CP-01	P1010, P2020, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, GV.SC-08, ID.IM-01, ID.IM-02, ID.IM-03, PR.IR-03	4.6.CP-1	5.18.CP-1			164.308(a)(7)(i) | 164.308(a)(7)(ii)	GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P7		
CP-02	P2020, P4590, S6010	GV.OC-04, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04, PR.IR-02, PR.IR-03, RC.RP-03, RC.CO-04	4.6.CP-2	5.18.CP-2	2.4.CP-2		164.308(a)(7)(ii)(C) 164.312(a)(b)(ii)	GV.PO-P3, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.DS-P4		11.1
CP-03	P2020	PR.IR-03	4.6.CP-3	5.18.CP-3				GV.AT-P3		
CP-04	P2020	ID.IM-02, PR.IR-03, RC.RP, RC.RP-03	4.6.CP-4	5.18.CP-4			164.308(a)(7)(ii)(D)	PR.PO-P3, PR.PO-P5, PR.PO-P8		11.5
~~CP-05~~										
CP-06	P2020	PR.DS-11, PR.IR-03, PR.IR-04		5.18.CP-6			164.310(a)(b)(i)	PR.PO-P3		11.4, 12.2
CP-07	P2020	PR.IR-03, PR.IR-04		5.18.CP-7				PR.PO-P7, PR.PT-P4		12.2
CP-08	P2020, P3010	PR.IR-03, PR.IR-04		5.18.CP-8				PR.PT-P3, PR.PT-P4		17.6
CP-09	P2020	PR.DS-01, PR.DS-10, PR.DS-11, PR.IR-03, RC.RP-03	4.6.CP-9	5.18.CP-9			164.308(a)(7)(ii)(A)	PR.PO-P3	03.08.09	11.2, 11.3, 11.5

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
CP-10	P2020	PR.IR-03, RC.RP, RC.RP-01, RC.RP-02, RC.RP-05	4.6.CP-10	5.18.CP.10				PR.PO-P7		11.1, 11.2
CP-11		PR.IR-03						PR.PT-P4		
CP-12		PR.IR-03						PR.PT-P4		
CP-13		PR.IR-03						PR.PT-P4		
IA-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03, PR.AA-01	4.7.IA-1	5.6.IA-1		8.1		GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.AC-P1, PR.AC-P6	03.15.01	
IA-02	P4502, G560	PR.AA-01, PR.AA-03	4.7.IA-2	5.6.IA-2, 5.13.7.1, 5.13.7.2	2.5.IA-2	8.1.1, 8.2, 8.3, 8.3.1, 8.3.2		PR.AC-P1, PR.AC-P6	03.05.01, 03.05.03, 03.05.04	6.3, 6.4, 6.5
IA-03		PR.AA-01, PR.AA-03	4.7.IA-3	5.6.IA-3, 5.13.7.1, 5.13.7.2.1, 5.13.7.3				PR.AC-P1, PR.AC-P6	03.05.02	
IA-04		PR.AA-01	4.7.IA-4	5.6.IA-4		8.1.1	164.312(a)(b)(i)	CT.DP-P2, PR.AC-P1, PR.AC-P6	03.05.05	6.1
IA-05	P4503, S6030	PR.AA-01, PR.AA-03	4.7.IA-5	5.6.IA-5, 5.13.1.1	2.5.IA-5	8.2.1 - 8.2.6, 8.3.1, 8.3.2, 8.6	164.308(a)(5)(ii)(D)	PR.AC-P1, PR.AC-P6	03.05.07, 03.05.12	33.10, 3.11, 4.7, 5.2, 6.1
IA-06		PR.AA-01	4.7.IA-6	5.6.IA-6					03.05.11	
IA-07		PR.AA-01, PR.AA-03	4.7.IA-7	5.6.IA-7, 5.10.1.2.1, 5.10.1.2.2				PR.AC-P1		
IA-08		PR.AA-01, PR.AA-03	4.7.IA-8	5.6.IA-8				CT.DP-P1, CT.DP-P3, PR.AC-P1, PR.AC-P6		6.6
IA-09		PR.AA-01, PR.AA-03	4.7.IA-9					PR.AC-P1, PR.AC-P6		
IA-10		PR.AA-01, PR.AA-03						PR.AC-P1, PR.AC-P6		
IA-11		PR.AA-01, PR.AA-03	4.7.IA-11	5.6.IA-11		8.1.8		PR.AC-P1, PR.AC-P6	03.05.01	
IA-12		PR.AA-02	4.7.IA-12	5.6.IA-12				PR.AC-P1, PR.AC-P6		
IR-01	P1010, P4110, P4140, P4590, S6010	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, GV.SC-08, ID.IM-01, ID.IM-02, ID.IM-03, PR.IR-03, RC.RP-04	4.8.IR-1	5.3.IR-1	2.6.IR-1	11.1.2, 12.5.3, 12.10	164.308(a)(6)(i)	PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CM.AW-P7, PR.PO-P7	03.15.01	17.1, 17.4, 17.5
IR-02	P4590, S6010	PR.IR-03	4.8.IR-2	5.3.IR-2	2.6.IR-2	12.10.4,		PB, GV.AT-P3, CM.AW-P7	03.06.04	
IR-03		ID.IM-02, PR.IR-03	4.8.IR-3	5.3.IR-3		12.10.2		PB, PR.PO-P5, PR.PO-P8	03.06.03	17.7

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
IR-04	P4590, S6010	ID.IM-01, ID.IM-02, ID.IM-03, PR.IR-03, DE.AE-02, DE.AE-03, DE.AE-06, DE.AE-08, RS.MA, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02, RC.RP-01, RC.RP-02, RC.RP-06, RC.CO-03, RC.CO-04	4.8.IR-4	5.3.IR-4, 5.13.5	2.6.IR-4	12.10.1, 12.10.3, 12.10.5, 12.10.6		PB, GV.MT-P6, CM.AW-P7	03.06.01	13.1, 17.8
IR-05	P4590, S6010	PR.IR-03, DE.AE-03, RS.MA-02, RS.MA-03, RS.MA-04	4.8.IR-5	5.3.IR-5		12.5.2, 12.10.5		PB	03.06.02	17.3
IR-06	P4590, S6010	PR.IR-03, RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.AN-06, RS.AN-07, RS.CO-02, RS.CO-03, RC.CO-03	4.8.IR-6	5.3.IR-6		12.10.1	164.308(a)(6)(ii)	PB, CM.AW-P7	03.06.02	17.2, 17.3, 17.4, 17.9
IR-07	P4590, S6010	PR.IR-03, RS.MA, RS.MA-01, RS.MA-04, RS.CO-02, RS.CO-03	4.8.IR-7	5.3.IR-7				PB, CM.AW-P8, PR.PO-P7	03.06.02	17.1
IR-08	P4590, S6010	ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04, PR.IR-03, DE.AE-03, DE.AE-08, RS.MA, RS.MA-01, RS.MA-05, RS.AN-08, RC.RP-01, RC.RP-02, RC.RP-04, RC.RP-06	4.8.IR-8	5.3.IR-8, 5.13.5	2.6.IR-8	12.8.3, 12.10, 12.10.1-12.10.6	164.308(a)(6)(ii)	PB, CM.AW-P7, PR.PO-P5, PR.PO-P6, PR.PO-P7	03.06.05	17.1, 17.3, 17.4, 17.5, 17.6, 17.9
IR-09		PR.IR-03, RS.MA	4.8.IR-9			12.10, 12.10.1-12.10.6		PR.PO-P7		
~~IR-10~~										
MA-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.9.MA-1	5.16.MA-1			164.310(a)(b)(iv)	GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, ,GV.MT-P6 PR.MA-P1	03.15.01	

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
MA-02	P2030	ID.AM-08	4.9.MA-2	5.16.MA-2				PR.MA-P1		
MA-03		PR.PS-02	4.9.MA-3	5.16.MA-3				PR.MA-P1	03.07.04	2.1
MA-04			4.9.MA-4	5.16.MA-4		9.9.3		PR.MA-P2	03.07.05	4.6
MA-05			4.9.MA-5	5.16.MA-5				PR.MA-P1	03.07.06	
MA-06		ID.AM-08	4.9.MA-6	5.16.MA-6	8.6			PR.MA-P1		
MA-07										
MP-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.10.MP-1	5.8.MP-1		9.5, 9.6	164.308(a)(4)(ii)(B)	PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PT-P1	03.15.01	
MP-02	P1030		4.10.MP-2	5.8.MP-2	2.7.MP-2	9.7, 9.7.1	164.308(a)(4)(ii)(C)	PR.DS-P1, PR.PT-P1	03.08.02	3.3
MP-03	G505, P4120, P4130		4.10.MP-3			9.6.1		PR.DS-P1, PR.PT-P1	03.08.04	
MP-04	G550, P4130		4.10.MP-4	5.8.MP-4		9.5.1, 9.6.1, 9.6.2, 9.7.1	164.310(d)(b)(iv	PR.DS-P1, PR.PT-P1	03.08.01	
MP-05			4.10.MP-5	5.8.MP-5		9.6.1 - 9.6.3	164.310(d)(a)	PR.DS-P1, PR.PT-P1	03.08.05	3.9
MP-06	P4530, G550, G540, S2140		4.10.MP-6	5.8.MP-6	2.7.MP-6	9.8, 9.8.1, 9.8.2	164.310(d)(b)(i), 164.310(d)(b)(ii)	PB, CT.PO-P2, CT.DM-P5, PR.DS-P1, PR.DS-P3	03.08.03	3.5
MP-07			4.10.MP-7	5.8.MP-7				PR.DS-P1, PR.PT-P1	03.08.07	3.9, 10.3, 10.4
MP-08		PR.DS-01						PR.DS-P1, PR.PT-P1		
PE-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.11.PE-1	5.9.PE-1		9.1	164.310(a)(a)	GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P4, PR.AC-P2	03.15.01	
PE-02		PR.AA-06	4.11.PE-2	5.9.PE-2		9.2, 9.3, 9.4, 9.4.1	164.310(a)(b)(ii), 164.310(a)(b)(iii)	PR.AC-P2, PR.AC-P6	03.10.01	
PE-03		PR.AA-06, DE.CM-02	4.11.PE-3	5.9.PE-3	2.9.PE-3	9.1, 9.1.1, 9.1.2, 9.2, 9.4.2, 9.4.3, 9.5, 9.5.1, 9.6	164.310(a)(b)(iv)	PR.AC-P2	03.10.07	
PE-04		PR.AA-06	4.11.PE-4	5.9.PE-4		9.1.2, 9.1.3		PR.AC-P2	03.10.08	
PE-05		PR.AA-06	4.11.PE-5	5.9.PE-5				PR.AC-P2	03.10.07	

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
PE-06	P4590, S6010	PR.AA-06, DE.CM-02	4.11.PE-6	5.9.PE-6	2.9.PE-6			PR.AC-P2	03.10.02	
~~PE-07~~										
PE-08		PR.AA-06	4.11.PE-8	5.9.PE-8		9.4.4		PB, CT.DP-P2, PR.AC-P2		
PE-09		PR.IR-02		5.9.PE-9				PR.AC-P2		
PE-10		PR.IR-02		5.9.PE-10						
PE-11		PR.IR-02		5.9.PE-11				PR.DS-P4, PR.PT-P4		
PE-12		PR.IR-02		5.9.PE-12						
PE-13		PR.IR-02		5.9.PE-13						
PE-14		PR.IR-02		5.9.PE-14						
PE-15		PR.IR-02		5.9.PE-15						
PE-16			4.11.PE-16	5.9.PE-16				PR.DS-P3		
PE-17	P4590, S6010		4.11.PE-17	5.9.PE-17					03.10.06	
PE-18		PR.AA-06, PR.IR-02								
PE-19		PR.AA-06						PR.DS-P5		
PE-20		PR.AA-06, DE.CM-02						PR.DS-P3		
~~PE-21~~										
~~PE-22~~										
PE-23		PR.IR-02								
PL-01	P1010, P2010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.12.PL-1	5.17.PL-1	2.10.PL-1	12.1, 12.2		PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6	03.15.01	
PL-02	P1070, P2010, P4130	ID.AM-03, ID.AM-08, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04	4.12.PL-2	5.17.PL-2	2.10.PL-2			PB, PR.PO-P5	03.15.02	
~~PL-03~~										
PL-04	P5040		4.12.PL-4	5.17.PL-4		12.3, 12.3.1, 12.3.2, 12.3.5-6, 12.3.10, 12.4	164.310(b)	PB	03.15.03	
~~PL-05~~										
~~PL-06~~										
PL-07	P2030									
PL-08	P1070, P2010	ID.AM-03	4.12.PL-8	5.17.PL-8		1.1.1 - 1.1.7		PB, CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3, PR.PT-P4		12.2, 12.4, 16.10
PL-09				5.17.PL-9				PB		
PL-10				5.17.PL-10						
PL-11				5.17.PL-11						

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
PM-01	P1010, P4140, G501	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.13.PM-1	3.2.1		12.1	164.308(a)(1)(i) 164.316(a)-(b)	GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6		
PM-02		GV.RR-01, GV.RR-02	4.13.PM-2	3.2.1		12.5, 12.5.1 - 12.5.5	164.308(a)(2)	GV.PO-P3		
PM-03		GV.RM-03, GV.RR-03, PR.IR-04	4.13.PM-3					PB, GV.PO-P2, GV.PO-P3, GV.PO-P6		
PM-04		GV.OV-03, ID.IM-02, ID.IM-03	4.13.PM-4	5.11.3				PB, ID.RA-P5, GV.MT-P4		
PM-05	P4520	ID.AM-01, ID.AM-02	4.13.PM-5			12.3.3, 12.3.4		PB, ID.IM-P1, ID.IM-P6, ID.RA-P1, GV.MT-P1		1.1, 3.2, 12.4
PM-06		GV.OV-03					164.308(a)(8)	PB, PR.PO-P5		
PM-07	P1070	ID.AM-03	4.13.PM-7					PB, GV.PO-P6, CT.DP-P1, CT.DP-P3		12.2
PM-08		GV.OC-04, RC.RP-04				12.3	164.308(a)(8)	PB		
PM-09		GV.OC-02, GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.OV-01, GV.OV-02, GV.SC-03, GV.SC-09, ID.RA-04, ID.RA-06, PR.IR-04, DE.AE-04, RC.RP-04	4.13.PM-9			12.2	164.308(a)(1)(ii)(B)	PB, ID.RA-P5, ID.DE-P2, GV.PO-P6, GV.RM-P1, GV.RM-P2		
PM-10			4.13.PM-10					PB, GV.PO-P6		
PM-11		GV.OC-01, GV.OC-04, GV.OC-05, ID.RA-04, DE.AE-04, RC.RP-04						PB, ID.BE-P2, GV.PO-P6		
PM-12		ID.RA-03	4.13.PM-12							
PM-13		GV.RR-02, GV.RR-04						PB, GV.PO-P3, GV.AT-P1, GV.AT-P2, GV.AT-P3		14.1
PM-14			4.13.PM-14					PB, GV.AT-P1, GV.MT-P3, PR.PO-P8		
PM-15		ID.RA-02, DE.AE-06				5.1.2, 6.1 and 6.2	164.308(a)(5)(ii), (ii)(A)	GV.MT-P5, CM.AW-P2		
PM-16		ID.RA-02, ID.RA-03, ID.RA-05, DE.AE-03, DE.AE-06, DE.AE-07				12.6				
PM-17								PB		15.3

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
PM-18		GV.OC-02, GV.RM-06, GV.RM-07, GV.OV-01, GV.SC-03, ID.RA-06, DE.AE-04	4.13.PM-18					PB, GV.PO-P3, GV.PO-P4, GV.PO-P6		
PM-19		GV.RR-01, GV.RR-02, GV.OV-02, GV.SC-09	4.13.PM-19					PB, GV.PO-P3, GV.PO-P4, GV.PO-P6		
PM-20								PB, GV.MT-P7, CM.PO-P1, CM.AW-P1, CM.AW-P2		
PM-21			4.13.PM-21					PB, CM.AW-P4, CM.AW-P6		
PM-22		ID.AM-08						PB, GV.MT-P7, CT.PO-P2, CT.PO-P3, CM.AW-P5		
PM-23		GV.RR-01, GV.RR-02, ID.AM-08						GV.PO-P2, GV.PO-P6, CT.PO-P2		
PM-24		GV.RR-01, GV.RR-02						PB		
PM-25								PB		
PM-26								PB, GV.MT-P7, CM.AW-P2		
PM-27								PB, GV.MT-P4, CM.PO-P1		
PM-28		GV.OC-03, GV.RM-04, GV.RM-06, GV.RM-07, GV.SC-09, DE.AE-04						PB, ID.RA-P4, ID.RA-P5, GV.PO-P6, GV.RM-P1, GV.RM-P3		
PM-29		GV.RR-01, GV.RR-02	4.13.PM-29					GV.PO-P3, GV.PO-P4		
PM-30		GV.OC-02, GV.OC-04, GV.OC-05, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.OV-01, GV.OV-02, GV.SC-01, GV.SC-03, GV.SC-09, ID.RA-06, DE.AE-04						ID.DE-P1		15.1, 15.2
PM-31		GV.OV-01, GV.OV-02, GV.SC-03, GV.SC-09, GV.SC-10, ID.IM-02, ID.IM-03						PB, GV.MT-P3		
PM-32										
PS-01	P1010, P4140	GV.OC-03, GV.RR-04, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-	4.14.PS-1	5.12				GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PO-P9	03.15.01	

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
		01, ID.IM-02, ID.IM-03								
PS-02			4.14.PS-2					PR.PO-P9		
PS-03			4.14.PS-3	5.12.1	2.8.PS-3	2.8.PS-03		PR.PO-P9, PR.AC-P6	03.09.01	
PS-04			4.14-PS-4	5.12.2	2.8.PS-4	8.1.3, 9.3		PR.PO-P9	03.09.02	
PS-05			4.14.PS-5	5.12.3				PR.PO-P9	03.09.02	
PS-06			4.14.PS-6		2.8.PS-6			PB, PR.PO-P9, PR.DS-P5		
PS-07		GV.RR-04, DE.CM-06	4.14.PS-7		2.8.PS-7			ID.DE-P5, GV.PO-P3, GV.AT-P4, PR.PO-P9		
PS-08			4.14.PS-8	5.12.4				PR.PO-P9		
PS-09		GV.RR-04	4.14.PS-9					GV.PO-P3, PR.PO-P9		
PT-01		GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.15.PT-1	4.1				PB, ID.IM-P5, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, CT.PO-P1, CT.PO-P3, CM.PO-P1, CM.PO-P2		
PT-02		GV.OC-03	4.15.PT-2					PB, ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1		
PT-03	P1020	GV.OC-03		4.2.1, 4.2.2, 4.2.3				PB, ID.IM-P5, CT.PO-P1, CT.DM-P7, CM.PO-P1		
PT-04		GV.OC-03						PB, CT.PO-P1, CT.PO-P3, CM.AW-P8		
PT-05	P1020	GV.OC-03						PB, CM.PO-P1, CM.AW-P1, CM.AW-P3		
PT-06		GV.OC-03						PB, CM.PO-P1		
PT-07		GV.OC-3		4.1, 4.3				PB		
PT-08		GV.OC-3						PB		
RA-01	P1010, P2040, P4140, G215	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.16.RA-1	5.19.RA-1	2.11.RA-01	12.2		PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.PO-P6, GV.MT-P2, GV.MT-P6, PR.PO-P10	03.15.01	16.2
RA-02	P4120, P4130	ID.AM-05, ID.RA-04, ID.RA-05		5.19.RA-2		9.6.1		ID.RA-P4		3.2, 3.7
RA-03	P2040, P2045 G215	GV.RM-06, GV.RM-07, GV.SC-03, GV.SC-09, GV.SC-10, ID.AM-05, ID.RA-01, ID.RA-03, ID.RA-04, ID.RA-05, ID.IM-01, ID.IM-02, ID.IM-03, DE.AE-07, RS.AN-08	4.16.RA-3	5.19.RA-3		6.1, 12.2	164.308(a)(1)(ii)(A) and (B)	PB, ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, PR.PO-P10	03.11.01	16.14
~~RA-04~~										

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
RA-05	P2040, P2045, P4520	GV.SC-10, ID.RA-01, ID.RA-08, ID.IM-01, ID.IM-02, ID.IM-03	4.16.RA-5	5.19.RA-5	2.11.RA-05	11.2, 11.2.1 - 11.2.3, 11.3		PR.PO-P10	03.11.02	7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 16.2, 16.6
~~RA-06~~										
RA-07		GV.OC-05, GV.RM-01, GV.RM-03, GV.OV-01, GV.OV-02, GV.OV-03, GV.SC-03, GV.SC-09, GV.SC-10, ID.RA-05, ID.RA-06, ID.IM-01, ID.IM-02, ID.IM-03, RS.AN-08	4.16.RA-7	5.19.RA-7				PB, ID.RA-P5	03.11.04	
RA-08		ID.RA-04	4.16.RA-8					PB, ID.RA-P1, ID.RA-P3, ID.RA-P4, ID.RA-P5, ID.DE-P2, GV.PO-P6, GV.MT-P1, GV.MT-P5, CM.PO-P1		
RA-09		GV.OC-04, GV.SC-04, GV.SC-07, ID.AM-05, ID.RA-04		5.19.RA-9				ID.BE-P3		
RA-10		DE.AE-06, DE.AE-07								
SA-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.17.SA-1					PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6	03.15.01	
SA-02	P2010		4.17-SA-2	5.1.1 (2-6, 8)				PB, GV.PO-P2		
SA-03		ID.AM-08, PR.PS-06	4.17.SA-3			6.3		PB, GV.PO-P2, CT.PO-P4		4.1, 16.1
SA-04		GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10, ID.AM-08, ID.RA-09, ID.IM-03, DE.CM-06	4.17.SA-4	5.1.1 (2-6, 8), 5.7.1.1				PB, ID.DE-P3, CT.PO-P4		15.4
SA-05		ID.AM-02, ID.RA-09	4.17-SA-5	5.7.2						
~~SA-06~~										
~~SA-07~~										
SA-08	G530, G509A	ID.AM-08, ID.IM-01 ID.IM-02, ID.IM-03, PR.DS-10, PR.PS-06, PR.IR-03	4.17.SA-8			2.2		PB, CT.PO-P4, CT.DP-P1, CT.DP-P2, CT.DP-P3, CT.DP-P4, CT.DP-P5	03.16.01	4.1, 12.2, 16.9, 16.10

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
SA-09	P2040, P4130, G215	GV.OC-05, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10, ID.AM-02, ID.AM-04, DE.CM-06	4.17.SA-9	5.1.1.7, 5.1.1.8, 5.1.2, 5.1.2.1	2.15.SA-9	2.4, 2.6, 12.8, 12.8.1 - 12.8.4, 12.9	164.308(a)(2)(a), 164.308(a)(4)(a), 164.314(a), 164.308(b)(a), 164.314(a)(1)(i)-(ii), 164.314(a)(1)(ii)(A)-(B), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(ii)(a)-(b)	PB, ID.DE-P1, ID.DE-P3, ID.DE-P5, GV.AT-P4	03.16.03	15.2
SA-10		ID.RA-09, PR.PS-02, PR.PS-03, PR.PS-06	4.17.SA-10	5.10.4.1		6.4		CT.PO-P4, PR.PO-P1, PR.PO-P2, PR.DS-P8		4.1
SA-11		ID.RA-01, ID.RA-09, ID.IM-01, ID.IM-02, ID.IM-03, PR.PS-06	4.17.SA-11			6.3, 6.3.1, 6.3.2, 6.4, 6.4.4, 6.6		PB, ID.DE-P5, CT.PO-P4		16.12
~~SA-12~~										
~~SA-13~~										
~~SA-14~~										
SA-15	G591B	ID.RA-01, ID.RA-09, PR.PS-06	4.17.SA-15			6.3, 6.5, 6.5.1-6.5.10, 6.4 and 6.4.3		ID.DE-P2, CT.PO-P4		16.11, 16.12
~~SA-16~~										
SA-17		ID.RA-09, ID.IM-01, PR.PS-06						CT.PO-P4, CT.DP-P1, CT.DP-P3, CM.AW-P3		
~~SA-18~~										
~~SA-19~~										
~~SA-20~~										
~~SA-21~~								PR.PO-P9		
SA-22		ID.AM-08	4.17.SA-22	5.14.SA-22					03.16.02	2.2
~~SA-23~~										
SC-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.18.SC-1	5.10.SC-1				GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6	03.15.01	
SC-02			4.18.SC-2	5.10.SC-2		2.2, 2.2.1, 7.1.1,		CT.DP-P3		
SC-03	P4570, G535	PR.PS-03				2.2, 2.2.1, 7.1.1,				3.12
SC-04		PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01	4.18.SC-4	5.10.SC-4		2.6			03.13.04	3.13
SC-05		PR.IR-01, DE.CM-01		5.10.SC-5				PR.DS-P4, PR.PT-P3		
SC-06		PR.IR-03						PR.PT-P4		

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
SC-07	P3010, P3020, P4570	PR.DS-01, PR.DS-02, PR.DS-10, PR.IR-01, DE.CM-01	4.18.SC-7	5.10.SC-7	2.13.SC-7	1.1, 1.1.4, 1.2.1, 1.2.3 and 1.3, 1.4,		PB, CT.DM-P7, PR.AC-P5, PR.DS-P5, PR.PT-P3	03.13.01, 03.13.06	4.4, 4.5, 9.3, 9.5, 12.2, 13.4, 13.5, 13.10, 16.8
SC-08	P4130	PR.DS-02	4.18.SC-8	5.10.SC-8	2.13.SC-8	4.1, 4.1.1, 8.2.1,	164.312(e)(2)(i)	PR.DS-P2	03.13.08	3.10
~~SC-09~~										
SC-10			4.18.SC-10	5.10.SC-10		8.1.8, 12.3.8		PR.AC-P5, PR.PT-P3	03.13.09	
SC-11		PR.DS-02, PR.DS-10						PR.DS-P2, PR.PT-P3		
SC-12		PR.DS-01, PR.DS-02	4.18.SC-12	5.10.SC-12		3.5, 3.5.1-3.5.4, 3.6, 3.6.1 - 3.6.8			03.13.10	
SC-13		PR.DS-01, PR.DS-02, PR.DS-10	4.18.SC-13	5.10.SC-13	2.13.SC-13		164.312(e)(2)(ii)		03.13.11	
~~SC-14~~										
SC-15			4.18.SC-15	5.10.SC-15				PR.AC-P3	03.13.12	
SC-16		PR.DS-02						CT.DM-P7, CT.DM-P9, CM.AW-P6, PR.DS-P6		
SC-17			4.18.SC-17	5.10.SC-17						
SC-18			4.18.SC-18	5.10.SC-18					03.13.13	9.1, 9.4
~~SC-19~~										
SC-20			4.18.SC-20	5.10.SC-20				PR.AC-P5, PR.PT-P3		4.9
SC-21			4.18.SC-21	5.10.SC-21				PR.PT-P3		4.9
SC-22			4.18.SC-22	5.10.SC-22				PR.PT-P3		4.9
SC-23			4.18.SC-23	5.10.SC-23				PR.PT-P3	03.13.15	12.3, 12.6
SC-24		PR.DS-10, PR.IR-03								
SC-25										
SC-26										
SC-27										
SC-28	P4550, S2140, G540	PR.DS-01	4.18.SC-28	5.10.SC-28	2.13.SC-28	3.1		PR.DS-P1	03.08.05, 03.13.08	3.6, 3.11, 11.3
SC-29										
SC-30										
SC-31								PR.PT-P3		
SC-32		PR.DS-01, PR.DS-10		5.10.3.1		3.4.1				
~~SC-33~~										
SC-34		PR.PS-05, DE.CM-09								
SC-35		DE.CM-09	4.18.SC-35			5.10.4.2				9.3
SC-36		PR.IR-03								
SC-37								PR.PT-P3		
SC-38								PR.PT-P3		

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
SC-39		PR.DS-01, PR.DS-10, PR.PS-03, PR.IR-03	4.18.SC-39	5.10.SC-39						4.12
SC-40		PR.DS-02, PR.DS-10		5.13.1.4		11.1-11.1.2				
SC-41										
SC-42										
SC-43		PR.DS-01, PR.DS-02, PR.DS-10								
SC-44										
SC-45			4.18.SC-45							
SC-46										
SC-47								PR.PT-P3		
SC-48										
SC-49		PR.PS-03								
SC-50										
SC-51		PR.PS-03								
SI-01	P1010, P4140	GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.19.SI-1	5.15.SI.1				PB, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6	03.15.01	
SI-02	P4520	ID.IM-01, ID.IM-02, ID.IM-03, PR.PS-02	4.19.SI-2	5.15.SI-2	2.14.SI-2	6.2, 6.4.6		PR.PO-P10	03.14.01	7.3, 7.4, 7.7, 16.3
SI-03		PR.DS-01, PR.DS-02, PR.DS-10	4.19.SI-3	5.15.SI-3	2.14.SI-3	5.1.1, 5.1.2, 5.2, 5.3			03.14.02	9.6, 9.7, 10.1, 10.2, 10.4, 10.6
SI-04		ID.RA-01, ID.IM-01, ID.IM-02, ID.IM-03, PR.DS-01, PR.DS-02, PR.DS-10, DE.CM-01, DE.CM-06, DE.CM-09, DE.AE-02, DE.AE-03	4.19.SI-4	5.15.SI-4	2.14.SI-4	10.2, 10.2.1 - 10.2.7, 10.6.1		PR.PO-P6, PR.DS-P5	03.14.06	1.3, 1.5, 10.7, 13.1, 13.3, 13.5, 13.6, 13.8, 13.11, 15.5, 18.2
SI-05	P4590, S6010	ID.RA-01, ID.RA-02, ID.RA-03	4.19.SI-5	5.15.SI-5					03.14.03	
SI-06								CT.DM-P9		
SI-07	P4590, S6010	ID.RA-09, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-02, DE.CM-09	4.19.SI.7	5.15.SI-7		A3.5.1		PR.DS-P6		2.7, 12.8
SI-08			4.19.SI.8	5.15.SI-8		11.4				9.2, 9.6, 9.7
SI-09			—							
SI-10		PR.DS-10	4.19.SI-10	5.15.SI-10				CT.DM-P6, PR.DS-P6		
SI-11			4.19.SI-11	5.15.SI-11						

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
SI-12		ID.AM-07, ID.AM-08	4.19.SI-12	5.15.SI-12	2.14.SI-12	3.1, 10.7		PB, CT.PO-P2, CT.PO-P4, CT.DM-P4, CT.DM-P5, CT.DP-P2	03.14.08	3.1, 3.4
SI-13		PR.IR-03								
SI-14										
SI-15										
SI-16		PR.DS-10	4.19.SI-16	5.15.SI-16						9.7, 10.5
SI-17										
SI-18		ID.AM-08						PB, GV.MT-P7, CT.PO-P2, CT.PO-P3, CT.DM-P1, CT.DM-P2, CT.DM-P3, CT.DM-P4, CT.DM-P7, CM.AW-P5, CM.AW-P6, CM.AW-P8		
SI-19								PB, GV.MT-P5, CT.DM-P9, CT.DP-P2, CT.DP-P3		
SI-20										
SI-21										
SI-22										
SI-23										
SR-01		GV.OC-03, GV.PO-01, GV.PO-02, GV.OV-01, GV.SC-03, ID.IM-01, ID.IM-02, ID.IM-03	4.20.SR-1					ID.BE-P1, ID.DE-P1, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6	03.15.01	15.2
SR-02		GV.RM-01, GV.RM-03, GV.RM-04, GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-08, GV.SC-09, GV.SC-10, ID.AM-04, ID.IM-04	4.20.SR-2					ID.DE-P1, ID.DE-P2, ID.DE-P3	03.17.01	
SR-03		GV.OC-02, GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-05, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10, RS.MA-01, RS.CO-02, RS.CO-03	4.20-SR-3					ID.BE-P1, ID.DE-P1, ID.DE-P2, ID.DE-P3	03.17.03	
SR-04								ID.DE-P1, CM.AW-P6		
SR-05		GV.OC-02, GV.OC-05, GV.SC-02, GV.SC-05, GV.SC-06, GV.SC-09,						ID.DE-P1, ID.DE-P2, ID.DE-P3	03.17.02	15.3, 15.4

NIST	ITA	CSF	FTI	CJI	SSA	PCI	PHI	Privacy	CUI	CSC
		GV.SC-10, ID.AM-08, ID.RA-09, ID.IM-01, ID.IM-02, ID.IM-03								
SR-06		GV.OC-02, GV.OV-01, GV.OV-02, GV.OV-03, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-09, GV.SC-10, ID.RA-09, ID.RA-10	4.20-SR-6					ID.DE-P2	03.11.01	15.2, 15.4, 15.6
SR-07										
SR-08		GV.OC-02, GV.SC-08, RS.MA-01, RS.CO-02, RS.CO-03, RC.CO-03						ID.DE-P3		
SR-09						9.2.1.1, 9.5.1.3				
SR-10		GV.SC-05, ID.RA-09	4.20.SR-10							
SR-11		ID.RA-09	4.20.SR-11							16.5
SR-12		ID.AM-08						CT.DM-P5		3.5, 15.7

Appendix C – Enforcement and Penalties

Enforcement

The Director's Office, Human Resources, and the Chief Information Security Officer (CISO) may initiate reviews, assessments, or other means to ensure that policies, guidelines, or standards are being followed.

Any violation of this policy may result in disciplinary action, up to and including termination of employment. ITS reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. ITS does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, ITS reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

26 U.S. Code § 7213 - Unauthorized disclosure of information specifies that willful unauthorized disclosure of returns or return information by an employee or former employee is a felony.

Criminal Penalties

26 U.S. Code § 7213 specifies that willful unauthorized disclosure of returns or return information by an employee or former employee is a felony.

The penalty can be a fine of up to $5,000 or up to five (5) years in jail, or both, plus costs of prosecution.

Under 26 U.S. Code § 7213, willful unauthorized access or inspection (UNAX) of taxpayer records by an employee or former employee is a misdemeanor. This applies to both paper documents and electronic information.

Violators can be subject to a fine of up to $1,000 and/or sentenced to up to one year in prison.

Civil Penalties

A taxpayer whose return or return information has been knowingly or negligently inspected or disclosed by an employee in violation of IRC Section § 6103 may seek civil damages.

26 U.S. Code § 7213 allows a taxpayer to institute action in district court for damages where there is unauthorized inspection or disclosure. If the court finds there has been an unauthorized inspection or disclosure, the taxpayer may receive damages of $1,000 for each unauthorized access or disclosure, or actual damages, whichever is greater, plus punitive damages (in the case of willful or gross negligence), and costs of the action (which may include attorney's fees).

There is no liability under 26 U.S. Code § 7213 if the disclosure was the result of a good faith but erroneous interpretation of IRC Section § 6103.

Appendix D – References

- CIS Controls Version 8
- Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- Internal Revenue Service Publication 1075 Tax Information Security Guidelines. For Federal, State and Local Agencies. Safeguards for Protecting Federal Tax Returns.
- NIST SP 800-12, Rev. 1, An Introduction to Information Security
- NIST SP 800-30, Risk Management Guide for IT Systems
- NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments
- NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-50, Building an Information Technology Security Awareness and Training Program
- NIST SP 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementation
- NIST SP 800-53, Rev. 5, Recommended Security Controls for Federal Information Systems
- NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-63-3, Digital Identity Guidelines
- NIST SP 800-84 Guide to Test, Training, and Exercise Process for IT Plans and Capabilities
- NIST SP 800-88, Rev.1, Appendix A, Minimum Sanitization Recommendations
- NIST SP 800-100, Information Security Handbook: A Guide for Managers
- NIST SP 800-162, Guide to Attribute-Based Access Control (ABAC)
- NIST SP 800-178, A Comparison of Attribute Based Access Control (ABAC) Standards for Data Services
- SSA, version 10.3, Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration. Technical System Security Requirements (TSSR)
- https://compliancedictionary.com/

Appendix E – Record of Changes

Version	Date	Description	Author
1.2	29Mar22	Initial version for first publication	Elizabeth Knox
2.0	01Mar23	Updated intent language	Elizabeth Knox
2.0	01Mar23	Updated Role and Responsibilities table	Elizabeth Knox
2.0	01Mar23	Corrected formatting errors	Elizabeth Knox
2.0	01Mar23	Standardized	Elizabeth Knox
2.0	01Mar23	Updated Table 1 Security and Privacy Policy Families	Elizabeth Knox
2.0	01Mar23	Aligned (AC-01)(AC-02)(AC-03)(AC-04)(AC-05)(AC-06)(AC-07)(AC-08)(AC-11)(AC-12)(AC-14)(AC-17)(AC-18)(AC-19)(AC-20)(AC-21)(AC-22)(AC-23(AT-01))(AT-02)(AT-03)(AT-04)(AU-01)(AU-02)(AU-03)(AU-04)(AU-05)(AU-06)(AU-07)(AU-08)(AU-09)(AU-10)(AU-11)(AU-12)(AU-13)(AU-14)(AU-16)(CA-01)(CA-02)(CA-03)(CA-05)(CA-06)(CA-07)(CA-08)(CA-09)(CM-01)(CM-02)(CM-03)(CM-04)(CM-05)(CM-06)(CM-07)(CM-08)(CM-09)(CM-10)(CM-11)(CP-01)(CP-02)(CP-03)(CP-04)(CP-06)(CP-07)(CP-08)(CP-09)(CP-10)(IA-01)(IA-02)(IA-03)(IA-04)(IA-05)(IA-06)(IA-07)(IA-08)(IA-11)(IR-01)(IR-02)(IR-03)(IR-04)(IR-05)(IR-06)(IR-07)(IR-08)(IR-09(MA-01)(MA-02)(MA-03)(MA-04)(MA-05)(MA-06)(MP-01)(MP-02))(MP-03)(MP-04)(MP-05(PE-01)(PL-01)(PM-01)(PS-01)(RA-01)(SA-01)(SC-01)(SI-1) wording with NIST SP 800-53 r5	Elizabeth Knox
2.0	01Mar23	Added (PT) Personally Identifiable Information Processing and Transparency Family and (SR) Supply Chain Risk Management Family	Elizabeth Knox
2.0	01Mar23	Added policies (AC-23)(AT-06)(CM-12)(CM-13)(CM-14)(IA-09)(IA-12)(PL-10)(PL-11)(PM-03)(PM-10)(PM-12)(PM-14)(PM-18)(PM-19)(PM-21)(PM-23)(PM-29)(PS-09)(PT-01)(PT-02)(RA-07)(RA-08)(RA-10)(SC-35)(SC-45)(SR-1)(SR-2)(SR-3)(SR-6)(SR-9)(SR-10)(SR-11)	Elizabeth Knox
2.0	01Mar23	Former policy (AS-1) is now (S.PS-01)	Elizabeth Knox
2.0	01Mar23	Former policy (AS-2) is now (S.MP-02)	Elizabeth Knox
2.0	01Mar23	Former policy (FS-1) is now (S.PS-01)	Elizabeth Knox
2.0	01Mar23	Former policy (FS-2) is now (S.PE-01)	Elizabeth Knox
2.0	01Mar23	Former policy (FS-3) is now (S.PE-02)	Elizabeth Knox
2.0	01Mar23	Former policy (FS-4) is now (S.PE-03)	Elizabeth Knox
2.0	01Mar23	Former policy (RB-1) is now (S.PE-04)	Elizabeth Knox
2.0	01Mar23	Former policy (RB-2) is now (S.PS-02)	Elizabeth Knox
2.0	01Mar23	Former policy (RB-3) is now (S.PL-01)	Elizabeth Knox
2.0	01Mar23	Former policy (RB-4) is now (S.PL-02)	Elizabeth Knox
2.0	01Mar23	Former policy (RB-5) is now (S.PL-03)	Elizabeth Knox
2.0	01Mar23	Former policy (RB-6) is now (S.IA-01)	Elizabeth Knox
2.0	01Mar23	Former policy (RB-8) is now (S.PE-04)	Elizabeth Knox
2.0	01Mar23	Former policy (RB-9) is now (S.PL-04)	Elizabeth Knox
2.0	01Mar23	Removed former policy (AU-15)(IR-10)(PL-03)(RB-7)(SA-12)(SA-13)(SA-14)(SA-18)(SA-19)(SC-19)	Elizabeth Knox
2.0	01Mar23	Removed (AS) Agency Security Policies Family, (FS) Facilities Security Policies Family, (RB) Rules of Behavior Family	Elizabeth Knox
2.0	01Mar23	Replaced terms FTI, CJI, or HIPAA with Federal Data	Elizabeth Knox
3.0	31Oct24	Moved Definitions and acronyms to back of manual	Elizabeth Knox
3.0	31Oct24	Updated all mentions of 'controls' to 'policies'	Elizabeth Knox
3.0	31Oct24	Updated the statement 'ITS supported information systems (system/s) where data classified as Level X and higher is received, processed, stored, accessed, protected, and/or transmitted' to 'ITS supported information systems (System/s) where data classified as Level X and higher is received, processed, stored, accessed, protected, and/or transmitted (Handled).	Elizabeth Knox
3.0	31Oct24	Updated (AC-03)(AC-04)(AC-05)(AC-06)(AC-08)(AC-11)(AC-21)(AC-22)(AC-23)(AT-02)(AT-03)(AT-04)(AU-02)(AU-03)(AU-04)(AU-06)(AU-07)(AU-08)(AU-09)(AU-10)(AU-11)(AU-12)(AU-13)(AU-16)(CA-05)(CA-06)(CA-07)(CA-08)(CA-09)(CM-02)(CM-03)(CM-04)(CM-05)(CM-06)(CM-07)(CM-08)(CM-09)(CM-12)(CM-14)(CP-02)(CP-04)(CP-06)(CP-07)(CP-09)(CP-10)(IA-02)(IA-03)(IA-06)(IA-08)(IR-06)(MA-02)(MA-03)(MA-04)(MA-05)(MA-06)(MP-02)(MP-03)(MP-04)(MP-05)(MP-07)(PL-10)(PL-11)(PS-04)(RA-02)(RA-03)(RA-05)(RA-07)(RA-09)(RA-10)(SA-02)(SA-03)(SA-08)(SA-09)(SA-10)(SA-11)(SA-22)(SC-02)(SC-03)(SC-04)(SC-05)(SC-13)(SR-11) scopes from data classified as Level 2 to Level 1	Elizabeth Knox
3.0	31Oct24	Updated hyperlinks	Elizabeth Knox
3.0	31Oct24	Updated Cyber Roles and Responsibilities	Elizabeth Knox

3.0	31Oct24	Mapped the Cyber Security Framework v2 to ITS policies	Elizabeth Knox
3.0	31Oct24	Updated mapping to ITA policies to ITS policies	Elizabeth Knox
3.0	31Oct24	Updated mapping with the CSC Framework to ITS policies	Elizabeth Knox
3.0	31Oct24	Updated mapping with IRS Publication 1075 to ITS policies	Elizabeth Knox
3.0	31Oct24	Updated mapping with FBI CJIS Policies to ITS policies	Elizabeth Knox
3.0	31Oct24	Updated mapping to SSA Security Requirements to ITS policies	Elizabeth Knox
3.0	31Oct24	Updated PCI Data Security Standard to ITS policies	Elizabeth Knox
3.0	31Oct24	Mapped HIPAA Security Rule to ITS policies	Elizabeth Knox
3.0	31Oct24	Updated the Scope to (AC-01)(AT-01)(AU-01)(CA-01)((CM-01)(CP-01)(IA-01)(IR-01)(MA-01)(MP-01)(PE-01)(PL-01)(PM-01)(PS-01)(PT-01)(RA-01)(SA-01)(SC-01)(SI-01)(SR-01) to include low, moderate, or high baselines	Elizabeth Knox
3.0	31Oct24	Updated (AC-01)(AT-01)(AU-01)(CA-01)((CM-01)(CP-01)(IA-01)(IR-01)(MA-01)(MP-01)(PE-01)(PL-01)(PM-01)(PS-01)(PT-01)(RA-01)(SA-01)(SC-01)(SI-01)(SR-01) review cycle for policies and procedures from three (3) years to annually	Elizabeth Knox
3.0	31Oct24	Added the requirement (AC-02)(u) Disable accounts of users within thirty (30) minutes but no later than one (1) day of discovery of direct threats to the confidentiality, integrity, or availability of State Data	Elizabeth Knox
3.0	31Oct24	Added the requirement (AC-03)(d) Users having accounts with administrator access privileges may access those accounts only from ITS owned or authorized Systems	Elizabeth Knox
3.0	31Oct24	Removed the requirement (AC-05)(b) Document any separation of duties	Elizabeth Knox
3.0	31Oct24	Added the requirement (AC-11)(b) Retain the device lock until the user reestablishes access using established identification and authentication procedures	Elizabeth Knox
3.0	31Oct24	Added the requirement (AC-12)(b) Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to Systems that handle State Data	Elizabeth Knox
3.0	31Oct24	Updated (AC-17) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (AC-19) requirements to align with NIST 800-53 r5 moved the previous policy statements to standard (S.AC-02) Mobile Device Requirements	Elizabeth Knox
3.0	31Oct24	Updated (AC-20) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Combined policy requirements (AC-23)(d)(e)	Elizabeth Knox
3.0	31Oct24	(AT-02)(a)2 added the requirement to provide training within 30 days of any security incidents	Elizabeth Knox
3.0	31Oct24	Moved (AT-03)(b) to standard (S.AT-01) Role-Based Training Content	Elizabeth Knox
3.0	31Oct24	Updated (AU-02) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Moved (AU-02) Audit event requirements to standard (S.AU-01) Event Logging	Elizabeth Knox
3.0	31Oct24	Updated (AU-03) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Added (AU-03)(a)11. (FBI-defined)	Elizabeth Knox
3.0	31Oct24	Added the requirement (AU-05)(b)2. Restart all audit logging processes and verify System(s) are logging properly	Elizabeth Knox
3.0	31Oct24	Added the requirement (AU-06)(d) Integrate audit record review, analysis, and reporting processes using automated mechanisms to support ITS processes for investigation and response to suspicious activities	Elizabeth Knox
3.0	31Oct24	Added the requirement (AU-06)(f) Specify the permitted actions for each role or users associate with the review, analysis, and reporting of audit record information	Elizabeth Knox
3.0	31Oct24	Updated (AU-09) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Added the requirement (AU-09)(a) Protect audit information and audit tools from unauthorized access, modification, and deletion	Elizabeth Knox
3.0	31Oct24	Added the requirement (AU-09)(b) Alert the CISO upon detection of unauthorized access, modification, or deletion of audit information	Elizabeth Knox
3.0	31Oct24	Added the requirement (AU-09)(c) Authorize access to management of audit logging functionality to only authorized SysAdmins	Elizabeth Knox
3.0	31Oct24	Updated (AU-12) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (AU-13)(c) If an information disclosure is discovered follow ITS Incident Response Plan	Elizabeth Knox
3.0	31Oct24	Removed policy (AU-14)	Elizabeth Knox
3.0	31Oct24	Removed the requirement (CA-06) All new systems must be approved by the CTO	Elizabeth Knox
3.0	31Oct24	Combined policy requirements (CA-09)(a)(e)	Elizabeth Knox
3.0	31Oct24	Updated (CM-02) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Added the requirements (CM-03)(k) After-System changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the System	Elizabeth Knox
3.0	31Oct24	Updated (CM-04) to align with NIST 800-53 r5	Elizabeth Knox

3.0	31Oct24	Updated (CM-06) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Added the requirement (CM-06)(a) Establish and document configuration settings for components employed within the System that reflect the most restrictive mode consistent with operational requirements using Office of Safeguards–approved compliance tools	Elizabeth Knox
3.0	31Oct24	Updated (CM-07) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (CM-08) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (CM-09) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Added the requirement (CM-11)(d) (FBI-defined) Monitor policy compliance through automated methods at least weekly	Elizabeth Knox
3.0	31Oct24	Updated (CP-07) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (CM-08) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (IA-02) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (IA-03) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Added the requirement (IA-04)(b) Manage individual identifiers by uniquely identifying each individual with ITS-defined characteristics identifying individual status (e.g., Contractor)	Elizabeth Knox
3.0	31Oct24	(IA-04) Updated (d)1. From 120 days to 90	Elizabeth Knox
3.0	31Oct24	Updated (IA-05) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Added the requirement (IA-11)(b) Re-authenticate when roles, authenticators, or credentials change	Elizabeth Knox
3.0	31Oct24	Added the requirement (IA-11)(c) Re-authenticate when security categories of systems change	Elizabeth Knox
3.0	31Oct24	Added the requirement (IA-11)(d) Re-authenticate when execution of privileged functions occur	Elizabeth Knox
3.0	31Oct24	Added the requirement (IA-11)(e) Re-authenticate when every twelve (12) hours	Elizabeth Knox
3.0	31Oct24	Updated (IR-03)(IR-04)(IR-05)(IR-06)(IR-07)(IR-08)(IR-09) scope to include CSIRT	Elizabeth Knox
3.0	31Oct24	Removed the requirement (IR-03)(b)	Elizabeth Knox
3.0	31Oct24	Updated (IR-04) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (IR-06) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (MA-02) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (MP-06) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Added the requirement (MP-06)(a) Sanitize digital and non-digital media containing State Data prior to disposal, release out of organizational control, or release for reuse using NIST 800-88, Guidelines for Media Sanitization approved sanitization techniques and procedures	Elizabeth Knox
3.0	31Oct24	Added the requirement (MP-06)(b) Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information	Elizabeth Knox
3.0	31Oct24	Added the requirement (MP-06)(d) Clear or purge any sensitive data from the system BIOS or UEFI before a computer system is disposed of and leaves the agency. Reset the BIOS or UEFI to the manufacturer's default profile, to ensure the removal of sensitive settings such as passwords or keys	Elizabeth Knox
3.0	31Oct24	Added the requirement (MP-06)(e) Media provided by foreign visitors (end users) may only be loaded into a standalone agency system. The system must remain standalone until such time as it is sanitized. Additionally, no other media loaded into the standalone system can be loaded into a non-standalone agency system until sanitized	Elizabeth Knox
3.0	31Oct24	Added the requirement (PE-01)(d) Develop and implement a clean desk policy for the protection of State Data (e.g., paper output, electronic storage media) to preclude unauthorized disclosures	Elizabeth Knox
3.0	31Oct24	Updated (PE-03) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Defined (PE-09) Power Equipment and Cabling	Elizabeth Knox
3.0	31Oct24	Defined (PE-10) Emergency Shutoff	Elizabeth Knox
3.0	31Oct24	Defined (PE-11) Emergency Power	Elizabeth Knox
3.0	31Oct24	Defined (PE-12) Emergency Lighting	Elizabeth Knox
3.0	31Oct24	Defined (PE-13) Fire Protection	Elizabeth Knox
3.0	31Oct24	Defined (PE-14) Environmental Controls	Elizabeth Knox
3.0	31Oct24	Defined (PE-15) Water Damage Protection	Elizabeth Knox
3.0	31Oct24	Updated (PE-16) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Removed the requirement (PL-07)(d)	Elizabeth Knox
3.0	31Oct24	Defined (PL-09) Central Management	Elizabeth Knox
3.0	31Oct24	Removed the requirement (PM-01)(c)	Elizabeth Knox
3.0	31Oct24	Updated (PM-05) to align with NIST 800-53 r5	Elizabeth Knox

3.0	31Oct24	Defined (PM-06) Measures of Performance	Elizabeth Knox
3.0	31Oct24	Updated (PM-07) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Defined (PM-11) Mission and Business Process Definition	Elizabeth Knox
3.0	31Oct24	Defined (PM-13) Security and Privacy Workforce	Elizabeth Knox
3.0	31Oct24	Updated (PM-14) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (PM-18) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Removed the requirement (PS-05)(c)(d)	Elizabeth Knox
3.0	31Oct24	Removed the requirement (PS-06)(d)(e)	Elizabeth Knox
3.0	31Oct24	Updated (RA-03) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (RA-05) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Defined (RA-05)(d) remediation timelines	Elizabeth Knox
3.0	31Oct24	Defined (RA-09) Criticality Analysis	Elizabeth Knox
3.0	31Oct24	Added the requirement (SA-03)(f) Plan for and implement a technology refresh schedule for the system throughout the SDLC	Elizabeth Knox
3.0	31Oct24	Updated (SA-09) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (SA-22) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (SC-02) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Defined (SC-05) Denial-of-Service (DoS) Protection	Elizabeth Knox
3.0	31Oct24	Defined (SC-06) System Availability	Elizabeth Knox
3.0	31Oct24	Updated (SC-07) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (SC-08) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (SC-13) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (SC-39) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Updated (SI-07) to align with NIST 800-53 r5	Elizabeth Knox
3.0	31Oct24	Removed the requirement (SI-08)(d)	Elizabeth Knox
3.0	31Oct24	Defined (P.ITS-01) Generative AL Usage Policy	Elizabeth Knox
3.0	31Oct24	Defined (P.ITS-02) Delegated Access Policy	Elizabeth Knox
3.0	31Oct24	Defined (S.AC-02) Mobile Device Requirements	Elizabeth Knox
3.0	31Oct24	Defined (S.AC-03) ITS User Accounts	Elizabeth Knox
3.0	31Oct24	Defined (S.AT-01) Role-Based Training Content	Elizabeth Knox
3.0	31Oct24	Defined (S.AU-01) Event Logging	Elizabeth Knox
3.0	31Oct24	Defined (S.AU-02) Critical Security Control Systems	Elizabeth Knox
3.0	31Oct24	Defined (S.IA-01b) PIN Authentication requirements for voicemail	Elizabeth Knox
3.0	31Oct24	Defined (S.IA-01c) One-Time Passwords	Elizabeth Knox
3.0	31Oct24	Defined (S.IA-01e) Verified Push Authentication	Elizabeth Knox
3.0	31Oct24	Defined (S.IA-01f) Secure Access Markup Language	Elizabeth Knox
3.0	31Oct24	Defined (S.MP-01a) Data Classifications to align with ITA	Elizabeth Knox
3.0	31Oct24	Moved and renamed (S.PS-04) Rules of Behavior to (S.PL-01) Rules of Behavior	Elizabeth Knox
3.0	31Oct24	Defined (S.SC-01) System and Communication Protection Standards	Elizabeth Knox
3.0	31Oct24	Updated SSA and CJI retention requirements in (S.SI-01)	Elizabeth Knox
3.0	31Oct24	Defined (S.ITS) ITS Policy Standards	Elizabeth Knox
3.0	31Oct24	Updated Appendix A – Compliance Review Cycle	Elizabeth Knox
3.0	31Oct24	Updated Appendix B – Framework Mapping	Elizabeth Knox
3.0	31Oct24	Updated Appendix D - References	Elizabeth Knox
4.0	10July25	Updated all references ‘ITS Date’ to ‘State Data’	Elizabeth Knox
4.0	10July25	Updated all references ‘ITS Personnel’ to ‘State Personnel’	Elizabeth Knox
4.0	10July25	Defined GRC roles & responsibilities	Elizabeth Knox
4.0	10July25	Defined EA roles & responsibilities	Elizabeth Knox
4.0	10July25	Updated the purpose for every policy for better clarity	Elizabeth Knox
4.0	10July25	Updated the policy mapping in every policy for CJIS	Elizabeth Knox
4.0	10July25	Updated the policy mapping in every policy for SSA	Elizabeth Knox
4.0	10July25	Updated the policy mapping in every policy for PCI	Elizabeth Knox
4.0	10July25	Updated the policy mapping in every policy for CSF	Elizabeth Knox
4.0	10July25	Mapped Privacy Framework to every policy	Elizabeth Knox
4.0	10July25	Mapped CUI Framework to every policy	Elizabeth Knox
4.0	10July25	Updated the requirement of policy and procedure review from 3 years to 1	Elizabeth Knox
4.0	10July25	Updated (CM-13) Data Action Mapping	Elizabeth Knox
4.0	10July25	Updated (CP-03) Contingency Training	Elizabeth Knox
4.0	10July25	Updated (AU-13) Monitoring for Information Disclosure	Elizabeth Knox
4.0	10July25	Updated (PE-02) Physical Access Authorizations	Elizabeth Knox
4.0	10July25	Updated (PL-07) Security Concept of Operations	Elizabeth Knox
4.0	10July25	Updated (PL-11) Baseline Tailoring	Elizabeth Knox
4.0	10July25	Updated (PM-09) Risk Management Strategy	Elizabeth Knox

4.0	10July25	Updated (PM-12) Insider Theat Program	Elizabeth Knox
4.0	10July25	Updated (PM-13) Security and Privacy Workforce	Elizabeth Knox
4.0	10July25	Updated (PS-02) Position Risk Designation	Elizabeth Knox
4.0	10July25	Updated (PS-06) Access Agreements	Elizabeth Knox
4.0	10July25	Updated (PT-07) Specific Categories of PII	Elizabeth Knox
4.0	10July25	Updated (RA-03) Risk Assessment	Elizabeth Knox
4.0	10July25	Updated (SA-08) Security and Privacy Engineering Principals	Elizabeth Knox
4.0	10July25	Updated (SA-09) External Information System Services	Elizabeth Knox
4.0	10July25	Updated (SA-15) Development Process, Standards, and Tools	Elizabeth Knox
4.0	10July25	Updated (SC-03) Security Function Isolation	Elizabeth Knox
4.0	10July25	Updated (SC-07) Boundary Protection	Elizabeth Knox
4.0	10July25	Updated (SC-08) Transmission Confidentiality and Management	Elizabeth Knox
4.0	10July25	Updated (SC-12) Cryptographic Key Establishment and Management	Elizabeth Knox
4.0	10July25	Updated (SC-22) Architecture and Provisioning for Name/Address Resolution Service	Elizabeth Knox
4.0	10July25	Updated (SC-23) Session Authenticity	Elizabeth Knox
4.0	10July25	Updated (SC-40) Wireless Link Protections	Elizabeth Knox
4.0	10July25	Updated (SC-45) System Time Synchronization	Elizabeth Knox
4.0	10July25	Updated (SI-02) Flaw Remediation (Software Patching)	Elizabeth Knox
4.0	10July25	Updated (SI-04) System Monitoring	Elizabeth Knox
4.0	10July25	Updated (SI-11) Error Handling	Elizabeth Knox
4.0	10July25	Updated (SI-12) Information Management and Retention	Elizabeth Knox
4.0	10July25	Updated (SI-16) Memory Protection	Elizabeth Knox
4.0	10July25	Updated (SR-09) Tamper Resistance and Detection	Elizabeth Knox
4.0	10July25	Updated (P.ITS-01) AI Usage Policy	Elizabeth Knox
4.0	10July25	Updated (P.ITS-03) Solution Vetting Policy for Network Access	Elizabeth Knox
4.0	10July25	Updated (S.AT-01) Role-Based Training Content	Elizabeth Knox
4.0	10July25	Updated (S.MP) Media Protection Standards	Elizabeth Knox
4.0	10July25	Updated (S.ITS-01) AI Usage Standard	Elizabeth Knox
4.0	10July25	Defined (CP-08) Telecommunication Services	Elizabeth Knox
4.0	10July25	Defined (PM-20) Dissemination of Privacy Program Information	Elizabeth Knox
4.0	10July25	Defined (PM-26) Compliant Management	Elizabeth Knox
4.0	10July25	Defined (PM-27) Privacy Reporting	Elizabeth Knox
4.0	10July25	Defined (PM-30) Supply Chain Risk Management Strategy	Elizabeth Knox
4.0	10July25	Defined (PT-05) Privacy Notice	Elizabeth Knox
4.0	10July25	Defined (P.ITS-03) Solution Vetting Policy for Network Access	Elizabeth Knox
4.0	10July25	Defined (S.SC-01) System Allocation	Elizabeth Knox
4.0	10July25	Defined (S.SC-02) Security Function Isolation	Elizabeth Knox
4.0	10July25	Defined (S.SC-03) Transmission Confidentiality and Integrity	Elizabeth Knox
4.0	10July25	Defined (S.SC-04) Cryptographic Key Establishment and Management	Elizabeth Knox
4.0	10July25	Defined (S.SC-05) Wireless Link Protection	Elizabeth Knox
4.0	10July25	Defined (S.SI-02) Information Management and Retention	Elizabeth Knox
4.0	10July25	Defined (S.SR) Supply Chain Risk Management Standards	Elizabeth Knox
4.0	10July25	Updated Definition and Acronyms	Elizabeth Knox

Appendix F – Definitions

In the realm of Cybersecurity terminology, Unified Compliance, Compliance Dictionary and the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, Glossary of Key Cybersecurity Terms, are the primary reference documents that ITS uses to define common Cybersecurity terms.

Access Controls: Access controls are typically logical controls designed into the hardware and software of a computing system. Identification is accomplished both under program control and physical controls.

Access Point: A networking hardware device that allows other Wireless (Wi-Fi) devices to connect to the State network.

Authentication: To verify the identity of a user, user device, or other entity.

Authorization: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Availability: Ensuring timely and reliable access to and use of information.

Administrative Account: A user account with full privileges on a system.

Application: A software program hosted by an information system.

Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Authorized Access List: Roster of individuals authorized admittance to a controlled area.

Authorized Control List: A list of permissions associated with an object. The list specifies who or what can access the object and what operations are allowed to be performed on the object.

Availability: Ensuring timely and reliable access to and use of information.

Awareness (***Information Security***): Activities which seek to focus an individual's attention on an (information security) issue or set of issues.

Back Door: Typically, unauthorized hidden software or hardware mechanism used to circumvent security controls. An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.

Backup: A copy of files and programs made to facilitate recovery, if necessary.

Banner: Display on an information system that sets parameters for system or data use.

Baseline: Hardware, software, databases, and relevant documentation for an information system at a given point in time.

Baseline Configuration: A set of specifications for a system, or Configuration Item (CI) within a system, which has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Blacklisting: The process of the system invalidating a user ID based on the user's inappropriate actions. A blacklisted user ID cannot be used to log on to the system, even with the correct authenticator. Blacklisting and lifting of a blacklisting are both security-relevant events. Blacklisting also applies to blocks placed against IP addresses to prevent inappropriate or unauthorized use of Internet resources.

Boundary: Physical or logical perimeter of a system.

Business Owner: The cost center manager that owns the data, has the authority to authorize or deny access to the data, and is responsible for the accuracy, integrity, and timeliness of the data.

Cardholder Data Environment (*CDE*): A term describing the area of the network that possesses cardholder data or sensitive authentication data and those supported information systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates supported information systems that receive, store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment.

Chain of Custody: A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

Clear Text: Information that is not encrypted.

Collision: Two or more distinct inputs produce the same output.

Compromise: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Computer Forensics: The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Container: The file used by a virtual disk encryption technology to encompass and protect other files.

Contamination: Type of incident involving the introduction of data of one security classification or security category into data of a lower security classification or different security category.

Content Filtering: The process of monitoring communications such as email and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users.

Contingency Plan: Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise Risk Officers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions.

Continuous Monitoring: The process implemented to maintain a current security status for one or more supported information systems or for the entire suite of supported information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or

changes that affect IA risks, and 4) Publishing the current security status to enable information-sharing decisions involving the enterprise.

Controlled Access Area: Physical area (e.g., building, room, etc.) to which only authorized personnel are granted unrestricted access. All other personnel are either escorted by authorized personnel or are under continuous surveillance.

Cryptographic Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber-attacks.

Data: Electronic information in any form, regardless of source, which is created or obtained by ITS with a data classification of Private, Confidential, or FTI.

Data at Rest: Inactive data that is stored physically in any digital form.

Denial of Service (*DoS*): The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Disconnection: The termination of an interconnection between two or more IT supported information systems. A disconnection may be planned (e.g., due to changed business needs) or unplanned (i.e., due to an attack or other contingency).

Encryption: Conversion of plaintext to cipher text using a cryptographic algorithm.

Environment: Aggregate external procedures, conditions, and objects affecting the development, operation, and maintenance of an information system.

Event: An evident change to the normal behavior of a network, system, or user.

Facilities: Broadly interpreted to refer to any physical location where personnel perform work on the behalf of ITS without regard to the ownership of the physical property. This term includes alternate sites where ITS has approved for the personnel to work (e.g., a private residence).

False Positive: An alert that incorrectly indicates that malicious activity is occurring.

Federal Data: For this manual, Federal Data represents Federal Tax Information (FTI), Social Security Association (SSA), and Criminal Justice Information Services (CJIS).

Firewall: A gateway that limits access between networks in accordance with local security policy.

Hashing: The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

Honeypot: A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential hackers and intruders and has no authorized users other than its administrators.

Idaho Controlled Technical Information: Technical data, research, engineering specifications, or software developed, maintained, or utilized within Idaho.

Identification: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Handling: The mitigation of violations of security policies and recommended practices.

Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber-attacks against an organization's information system(s).

Information Security: The protection of information and supported information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Life Cycle: The phases through which an information system passes, typically characterized as initiation, development, operation, and termination (i.e., sanitization, disposal and/or destruction).

Information Technology (*IT*): Any related products, goods, equipment, hardware, supplies, software, services, or any other IT-related resource.

Internet of Things (IoT): Internet of Things are devices that communicate across a network without direct human interaction. These include but are not limited to smart assistants, lightbulbs, appliances, and televisions.

Integrity: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Least Privilege: The security objective of granting users only those accesses they need to perform their official duties.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.

Maintenance: The process of making repairs and keeping components of a system in good condition so that the system may remain in operating condition and last its entire useful life.

Media: Anything that can store data.

Monitoring: Determining the status of a system, a process, or an activity.

Need-To-Know: A method of isolating information resources based on a user's need to have access to that resource to perform their job but no more. The terms 'need-to know" and "least privilege" express the same idea. Need-to-know is applied to people, while least privilege is generally applied to processes.

Network: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network Access Credentials: Any information that has been issued by ITS that grants the user ITS network access and requires a password/PIN.

Non-Local Maintenance: Maintenance activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.

Non-Public Data: Data that is classified as Confidential or as Federal Tax Information per the General Security Policies Manual.

Open Source: Computer software in which source code is released under a license in which the copyright holder grants users the right to study, change, and distribute the software to anyone and for any purpose.

Patch: An update to an operating system, application, or other software issued specifically to correct problems with the software.

Personally Identifiable Information (*PII*): Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Personally Owned Device: Any device owned by an individual employee, rather than the agency itself.

Personnel: Employees, officers, agents, contractors, consultants, vendors, interns, or any other person performing work for ITS working on behalf of ITS regardless of employment status and includes contractual relationships for entities that provide goods or services.

Phishing: Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

Piggybacking: When a person tags along with another person who is authorized to enter a restricted area or pass a certain checkpoint. It can be either electronic or physical.

Plaintext: Data input to the Cipher or output from the Inverse Cipher.

Plan of Action and Milestones (POAM): A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Port: A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).

Privacy: Restricting access to subscribers or relying party information in accordance with federal law and agency policy.

Privilege: A right granted to an individual, a program, or a process.

Privileged Account(s): A system account with the authorizations of a privileged user.

Privileged User: A user who can alter or circumvent a system's security measures. This can also apply to users who have only limited privileges, such as software developers, who can still bypass security measures. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files, or applications.

Protected Health Information (PHI): Also referred to as personal health information, is the demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Public Key: The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Purge: Rendering sanitized data unrecoverable by laboratory attack methods.

Quarantine: Store files containing malware in isolation for future disinfection or examination.

Read Access: Permission to read information in an information system.

Remote Access: Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet).

Removable Media: Portable electronic storage media such as magnetic, optical, and solid-state devices, which can be inserted into and removed from a computing device, and that is used to store text, video, audio, and image information. Such devices have no independent processing capabilities. Examples include hard disks, floppy disks, zip drives, compact disks (CDs), thumb drives, pen drives, and similar USB storage devices.

Restricted Area: An area from which personnel are excluded for reasons of security or safety unless specially authorized: an off-limits area.

Risk: The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an information system.

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; and 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Sanitization: Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

Security Category: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on operations, assets, individuals, other organizations, and the State. There are four (4) classifications that ITS uses: *Level I–Public, Level II–Private, Level III–Confidential, and Level IV-Critical.*

Sniffing: A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.

Spam: The abuse of electronic messaging supported information systems to indiscriminately send unsolicited bulk messages.

Spillage: Security incident that results in the transfer of classified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

System: Broadly interpreted to refer to any computing device such as a server, pc, smart, mobile device, or any other device that can process or transmit information digitally.

Tailgating: The act of gaining unauthorized entry to a secure area by closely following someone with authorized access.

Telework: The ability for an organization's employees and contractors to perform work from locations other than the organization's facilities.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Unauthorized Access: Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.

Unauthorized Disclosure: An event involving the exposure of information to entities not authorized access to the information.

Validation: The process of demonstrating that the system under consideration meets in all respects the specification of that system.

Virus: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Whitelist: A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system.

Write Access: Permission to write to an object in an information system.

Appendix G – Acronyms

AAL: Authorized Access List

ACL: Access Control List

AD: Active Directory

AES: Advanced Encryption Standards

ARLs: Authority Revocation Lists

ASV: Approved Scanning Vendor

BCP: Business Continuity Plan

BYOD: Bring your own Device

C2: Command & Control

CAP: Corrective Action Plan

CCB: Configuration Control Board

CCO: Chief Compliance Officer

CDE: Cardholder Data Environment

CDI: Covered Defense Information

CIRT: Computer Incident Response Team

CISO: Chief Information Security Officer

CIO: Chief Information Officer

CJI: Criminal Justice Information

CJIS: Criminal Justice Information Services

CONOPS: Concept of Operations

COOP: Continuity of Operations Plan

CRLs: Certificate Revocation Lists

CSC: Critical Security Controls

CSRF: Cross-Site Request Forgery

CTI: Controlled Technical Information

CTO: Chief Technology Officer

CUI: Controlled Unclassified Information

DiD: Defense-in-Depth

DKIM: Domain Keys Identified Mail

DLP: Data Loss Prevention

DMARC: Domain-based Message Authentication, Reporting & Conformance

DMZ: Demilitarized Zone

DNS: Domain Name System

DoS: Denial of Service

DRP: Disaster Recovery Plan

EA: Enterprise Architect

EDMS: Electronic Document Management System

Email: Electronic Mail

ETL: Extract, Transform, Load

Fax: Facsimile Machines (analog and digital)

FBI: Federal Bureau of Investigations

FIM: File Integrity Monitoring

FTI: Federal Tax Information

GAI: Generative Artificial Intelligence

GPS: Global Positioning System

HIPAA: Health Insurance Portability and Accountability Act

HSMs: Hardware Security Modules

ICTI: Idaho Controlled Technical Information

IdP: Identity Provider

IM: Instant Messaging

IP: Internet Protocol

IRP: Incident Response Plan

IRS: Internal Revenue Services

ISA: Interconnection Security Agreement

ISCP: Information System Contingency Plan

ISMS: Information Security Management System

ITA: Idaho Technology Authority

ITS: Information Technology Services

LAN: Local-Area Network

MAC: Media Access Control

MDM: Mobile Device Management

MFA: Multi-factor Authentication

MOU: Memorandum of Understanding

MST: Mountain Standard Time

MTD: Maximum Tolerable Downtime

NAC: Network Access Control

NAT: Network Address Translation

NDA: Non-Disclosure Agreement

NetOps: Network Operations

NFC: Near Field Communication

NIST: National Institute of Standards and Technology

PANs: Primary Account Numbers

PCI: Payment Card Industry

PHI: Protected Health Information

PII: Personally Identifiable Information

PIO: Public Information Officer

PIN: Personal Identification Number

PKI: Private Key Infrastructure

POAM: Plan of Action and Milestones

POTS: Plain Old Telephone Service (Analog Lines)

RBAC: Role-Based Access Control

rDNS: Reverse DNS

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SAML: Security Assertion Markup Language

SCDs: Secure Cryptographic Devices

SDLC: Systems Development Life Cycle

SecOps: Security Operations

SIEM: Security Information and Event Management

SLAs: Service Level Agreements

SMS: Short Message Service

SPF: Sender Policy Framework

SSA: Social Security Administration

SSP: System Security Plan

SSR: Safeguard Security Report

SysAdmin: System Administrators

THT: Threat Hunter Team

TLS: Transport Layer Security

UEM: Unified Endpoint Management

USB: Universal Serial Bus

UTC: Coordinated Universal Time

VDI: Virtual Desktop Infrastructure

VoIP: Voice over Internet Protocol

VPN: Virtual Private Network

WAF: Web Application Firewall

WAP: Wireless Access Point

WLAN: Wireless Local-Area Network

XSS: Cross-Site Scripting

BLANK

Prepared by:
Elizabeth Knox