Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINE – G500 SECURITY PROCEDURES

Category: G515 – Critical Security Controls (CSCs) 1-6 Written Policy Template

CONTENTS:

I. AUTHORITY

[insert language here to support authority of organization to create policy]

II. ABSTRACT

This policy establishes a baseline of template language for use by agencies for written policy development in support of CSCs 1-6

III. DEFINITIONS

See ITA Guideline G105 for any definitions.

IV. GUIDANCE

Agencies may use the below policy examples for use in their own agency written policy: (see appendix for policy examples)

V. APPENDIX

i. Example Policy #1 (Hardware Control)

[Agency Name]

ENTERPRISE POLICY – PXXXX SECURITY-GENERAL

Category: PXXXX – Hardware Control Policy

CONTENTS:

I. AUTHORITY

[Insert language to support authority of organization to create policy]

II. ABSTRACT

This policy is designed to use best practices within Agency's capacity to ensure an accurate and up-to-date inventory of all hardware assets to assure a thorough and secure asset management process.

III. DEFINITIONS

See G105 for any definitions.

IV. POLICY

Control 1: Inventory and Control of Hardware Assets

Agency will use best practices to ensure an accurate and up-to-date inventory of all hardware assets to assure a thorough and secure asset management process.

Hardware Asset Control and Management will consist of:

- Inventory of all hardware assets and the following Agency Information:
  - Network Address (IP address), Hardware address (MAC address), Machine/Device Name, and responsible party for asset.

- Ensuring unauthorized assets are removed from network or quarantined within [***a timely manner]*** of discovery.

- Where network discovery tools are available and practical; use of an active discovery tool to assist in the identification of assets.
  - DHCP logging or IP management tools used at Agency’s discretion.

With application of the following when feasible:

- Agency will use a passive discovery tool for an automated update of asset inventory.

- Agency will use client certificates as an authentication method for hardware assets to connect to Agency internal network.

- Agency will manage and control devices to connect to wireless network with port level access-control, referencing the asset to authenticate the trusted devices. (IAW 802.1X)

V. EXEMPTION PROCESS

Refer to [Agency Name] [exemption policy/procedure].

VI. PROCEDURE REFERENCE

- CIS Critical Security Controls v7.1

VII. CONTACT DATA

[Agency contact information]

REVISION HISTORY

Effective Date: xx/xx/xxxx

ii. Example Policy #2 (Software Control)

[Agency Name]

ENTERPRISE POLICY – PXXXX SECURITY-GENERAL

Category: PXXXX – SOFTWARE CONTROL POLICY

CONTENTS:

I. AUTHORITY

[Insert language to support authority of organization to create policy]

II. ABSTRACT

This policy is designed to actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.

III. DEFINITIONS

See G105 for any definitions.

IV. POLICY

Control 2: Inventory and Control of Software Assets

Agency will use best practices to ensure an accurate and up-to-date inventory of all software and applications to assure a thorough and secure asset management process.

At a minimum, Software Asset Control and Management will consist of:

- Tracking Inventory of all authorized software:
  - Name, Version, Publisher, Install date.
  - Tied to Hardware Asset Inventory for association

- Inventory of all software assets required for any business purpose on any device.
- Software is only permitted on Agencies domain when it is supported and receiving vendor updates.
  - Unsupported Software Applications / Operating systems will be tagged as unsupported.

- Ensuring unauthorized software are removed from devices or quarantined within [a timely manner] of discovery.

- The software inventory system should be tied into the hardware asset inventory, so all devices and associated software are tracked from a single location.

With application of the following where feasible:

- Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incurs higher risk for the organization.

- Utilize application whitelisting technology on all assets to ensure:

  - That only authorized software executes, and all unauthorized software is blocked from executing on assets.
  - The Agency's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.
  - The Agency's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1,*.py, macros, etc.) are allowed to run on a system.

V. EXEMPTION PROCESS

Refer to [Agency Name] [exemption policy/procedure].

VI. PROCEDURE REFERENCE

- CIS Critical Security Controls v7.1

VII. CONTACT DATA

[Agency contact information]

REVISION HISTORY

Effective Date: xx/xx/xxxx

iii. Example Policy #3 (Continuous Vulnerability Management)

[Agency Name]

ENTERPRISE POLICY – PXXXX SECURITY-GENERAL

Category: **PXXXX – CONTINUOUS VULNERABILITY MANAGEMENT POLICY**

CONTENTS:

I. AUTHORITY

[Insert language to support authority of organization to create policy]

II. ABSTRACT

This policy established to Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

III. DEFINITIONS

See G105 for any definitions.

IV. POLICY

Control 3: Continuous Vulnerability Management

Agency will use best practices to continuously detect, monitor and remediate vulnerabilities of all assets connected to the Agencies network.

The Agency's Continuous Vulnerability Management program will consist of:

- Deployment of an automated software update tool to:
  - To ensure that the operating systems are running the most recent security updates provided by the software vendor.

    - To ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.

- Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all assets on Agency's network:
    - At minimum of a weekly basis.
    - With use of a dedicated account for authenticated vulnerability scans.
        - The account is not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.

    - Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.
    - For regular comparisons of the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated within [*a timely manner*].
        - All critically rated vulnerabilities will be addressed within 30 days, and notification to [*Security Officer]* upon discovery and remediation date.

With application of the following where feasible:

- Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.

V. EXEMPTION PROCESS

Refer to [Agency Name] [exemption policy/procedure].

VI. PROCEDURE REFERENCE

- CIS Critical Security Controls v7.1

VII. CONTACT DATA

[Agency contact information]

REVISION HISTORY

Effective Date: xx/xx/xxxx

[Agency Name]

ENTERPRISE POLICY – PXXXX SECURITY-GENERAL

Category: **PXXXX – CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES POLICY**

CONTENTS:

I. AUTHORITY

[Insert language to support authority of organization to create policy]

II. ABSTRACT

This policy establishes security processes used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

III. DEFINITIONS

See G105 for any definitions.

IV. POLICY

Control 4: Controlled Use of Administrative Privileges

Agency will use best practices to continuously track and control of all administrative privileges on all Agency hardware and software assets.

Agency's Elevated Access and Administrator Control process is to consist of:

- Use of a dedicated account (and machine if applicable) for all administrative access or tasks requiring elevated privileges. This account and or machine will:

        - Not have access to the internet
        - Not be used for any personal activities (i.e. email or document creation)
        - (In the use of a dedicated machine) be segmented from the Agency's primary network and not be allowed Internet access.
        - Use multi-factor authentication and encrypted channels for all administrative account access.
            - Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system

        - Be configured to issue a log entry and alert:
            - When an account is added to or removed from any group assigned administrative privileges.
            - On unsuccessful logins to an administrative account.

- Before deploying any new asset on Agency's network, Agency will change all default passwords to have requirements consistent with administrative level accounts.

- Limiting access of scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.

- Use of an automated tool to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
    - Discovery of an unauthorized account is to be quarantined immediately and reported to [*Security Officer*] within [*a timely manner*] of discovery.

V. EXEMPTION PROCESS

Refer to [Agency Name] [exemption policy/procedure].

VI. PROCEDURE REFERENCE

- CIS Critical Security Controls v7.1

VII. CONTACT DATA

[Agency contact information]

REVISION HISTORY

Effective Date: xx/xx/xxxx

iv. Example Policy #5 (Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers)

[Agency Name]

ENTERPRISE POLICY – PXXXX SECURITY-GENERAL

Category: **PXXXX – SECURE CONFIGURATION FOR HARDWARE AND SOFTWARE ON MOBILE DEVICES, LAPTOPS, WORKSTATIONS AND SERVERS POLICY**

CONTENTS:

I. AUTHORITY

[Insert language to support authority of organization to create policy]

II. ABSTRACT

This policy is to establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

III. DEFINITIONS

See G105 for any definitions.

IV. POLICY

Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Agency will use best practices to manage configurations of hardware and software on all Agency's assets.

The Agency's Configuration Management Process will include:

- Documentation of security configuration standards for all authorized operating systems and software.

- Maintain secure images or templates for all systems in the enterprise based on the Agency's approved configuration standards.

- Storage of the master images and templates on securely configured servers.
    - Servers are to be validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
    - In the instance of an unauthorized change, Agency shall report to [Security Officer].

- Deployment of system configuration management tools that automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

- The use of Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements.
    - All exceptions to the security configurations are to be approved by [Security Officer] and recorded with the SCAP catalog approved exceptions.
    - Configurations are to be made to alert when unauthorized changes occur on monitored systems within the Agency's network.

V. EXEMPTION PROCESS

Refer to [Agency Name] [exemption policy/procedure].

VI. PROCEDURE REFERENCE

- CIS Critical Security Controls v7.1
- **The CIS Benchmarks™ Program** (https://www.cisecurity.org/cis-benchmarks/)
- **The NIST National Checklist Program** (https://nvd.nist.gov/ncp/repository)

VII. CONTACT DATA

[Agency contact information]

REVISION HISTORY

Effective Date: xx/xx/xxxx

v. Example Policy #6 (Maintenance, Monitoring and Analysis of Audit Logs)

[Agency Name]

ENTERPRISE POLICY – PXXXX SECURITY-GENERAL

Category: PXXXX – MAINTENANCE, MONITORING AND ANALYSIS OF AUDIT LOGS POLICY

CONTENTS:

I. AUTHORITY

[Insert language to support authority of organization to create policy]

II. ABSTRACT

This policy is to establish the collection, management and analyzing of audit logs of events that could help detect, understand and recover from an attack.

III. DEFINITIONS

See G105 for any definitions.

IV. POLICY

The Agency is to establish the collection, management and analyzing of audit logs of events. The Agency's Log management program will consist of:

- Ensuring that local logging has been enabled on all systems and networking devices. All logging shall include at minimum:
    - Event source, date, user, timestamp, source addresses, destination addresses

- Ensuring that all systems that store logs have adequate storage space for the logs generated.

    - Where applicable, systems are to notify user and administrator, when dedicated storage is within 75% of capacity.
- Systems are to use at least three approved synchronized time sources from which all servers and network devices retrieve time information.

- Ensuring that appropriate logs are being aggregated to a central log management system for analysis and review.
    - Logs are to be reviewed for anomalous or abnormal events on a regular basis, determined by Agency's [Security Officer]
    - Where applicable, the Agency is to deploy Security Information and Event Management (SIEM) or log analytic tools for log correlation and analysis.
    - The SIEM is to be tuned to decrease false positives and better assist in the identification of actionable events on a regular basis.

V. EXEMPTION PROCESS

Refer to [Agency Name] [exemption policy/procedure].

VI. PROCEDURE REFERENCE

- CIS Critical Security Controls v7.1

VII. CONTACT DATA

[Agency contact information]

REVISION HISTORY

Effective Date: xx/xx/xxxx