Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G536 Firewall: Ports, Protocols and Services (PPS) Request

CONTENTS:

I. DEFINITIONS

Deny by Default: To block all inbound and outbound traffic that has not been expressly permitted by firewall policy.

Perimeter Firewall: A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.

Policy: A high-level directive that describes mandatory or prohibited actions, applicable to individuals who fall within the scope of the policy, which aim to protect State information assets.

II. RATIONALE

Firewalls are often placed at the perimeter of a network to restrict connectivity to and from internal networks preventing unauthorized access to the organization's systems and resources. Perimeter firewall filtering rules may also be applied to any internal firewall device or router connected to the state network to minimize internal threats and maintain the restrictive policy integrity down to security enclaves. To prevent exploitation of the inherent vulnerabilities associated with open Ports, Protocols, and Services (PPS), all non-required PPS should be blocked by the most restrictive rules possible, which is a deny-by-default policy.

If an agency's operations require a new firewall PPS policy, or a modification to an existing firewall PPS policy, some form of agency risk analysis must be performed on the information asset vulnerabilities associated with the policy in conjunction with the agency's operational requirement.

III. GUIDELINE

After an agency completes an internal risk assessment and the agency is reasonably sure that the new PPS policy does not pose a significant risk to its information assets, the agency must submit a Firewall Change Request (FCR) to the Office of IT Services (ITS) Firewall Security Coordinator (FSC). To mitigate insider threats, the FCR should be submitted by the agency's Information Security Coordinator (ISC).

Under normal circumstances, the FCR will be reviewed by the FSC for security and operational impacts to the State network. Low risk FCRs will be scheduled for the next PPS implementation cycle. If the operational impact to the state network is significant, the FCR will be routed to the state's Configuration Authorization Board (CAB) for final adjudication.

Normal PPS policy changes are implemented at 06:00 PM on each Thursday of each week.

Emergency PPS changes are implemented as required for a limited period of time (10 working days) or until the request can be reviewed by the CAB.

IV. PROCEDURE REFERENCE

Firewall Change Request:
http://www.its.idaho.gov/products_and_services/firewall_management.html

NIST SP 800-30 (Revision 1) (Guide for Conducting Risk Assessments)

NIST SP 800-41 (Revision 1) (Firewall Policy)

Enterprise ITA Policy P4570 (Firewall Security)

Enterprise ITA Policy P4140 (Cybersecurity Framework)

Enterprise ITA Guideline G535 (Firewall Configuration Guidelines)

V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

To report an incident, send email to: security@its.idaho.gov or call (208) 605-4000.

REVISION HISTORY

07/01/2018 – Changed "OCIO" to "ITS".

Effective Date: December 15, 2015