Idaho Technology Authority (ITA)

ENTERPRISE POLICIES – P4500 SECURITY - COMPUTER AND OPERATIONS MANAGEMENT

Category: S6040 - FIREWALL CHANGE REQUEST

CONTENTS:

I. Definition
II. Rationale
III. Approved Standard(s)
IV. Approved Product(s)
V. Justification
VI. Technical and Implementation Considerations
VII. Emerging Trends and Architectural Directions
VIII. Procedure Reference
IX. Review Cycle
X. Contact Information
Revision History

I. DEFINITION

See ITA Guideline G105 (Glossary of Terms) for any definitions. G105-ITA Glossary of Terms

II. RATIONALE

Firewalls protect state systems by limiting network access and reducing exposure to threats. Because changes to Ports, Protocols, and Services (PPS) directly affect security risk, they must be carefully reviewed, documented, and approved. A standardized change process ensures consistent application of a deny-by-default posture, supports enterprise risk management, and maintains alignment with ITA policies and NIST guidance.

III. APPROVED STANDARD(S)

Firewall Change Request Process:

1. Risk Assessment: Agencies must perform an internal risk assessment for any new PPS policy or modification, documenting residual risk and business justification.

2. Submission: The request must be submitted by the agency's Cybersecurity Coordinator (or equivalent role) to initiate review.

3. Coordination: Coordination will involve relevant stakeholders across the security stack (e.g., network, firewall, LAN/WAN, cloud security) as appropriate for the request. Not all requests route through the Firewall Management Team initially; involvement depends on the devices and scope affected.

4. Approval Workflow:

   a. Standard changes follow the agency Change Advisory Board (CAB) process.
   b. Emergency changes may bypass formal CAB approval but still require informal approvals from ITS and other impacted security stack owners before implementation.
   c. The duration of emergency PPS changes is dependent on the nature of the request and subsequent approvals; some changes may extend beyond 10 working days if justified and documented.

5. Documentation: All approvals—formal or informal—must be documented in the change record for audit purposes.

IV. APPROVED PRODUCTS(S)

Refer to approved state contracts for IT Security Products:
https://purchasing.idaho.gov/statewide-contracts/

V. JUSTIFICATION

This standard establishes a uniform process for requesting and approving firewall changes across Executive Branch agencies. A consistent approach reduces configuration errors, promotes coordinated risk management, and ensures firewall modifications support statewide security objectives and ITA governance requirements.

VI. TECHNICAL AND IMPLEMENTATION CONSIDERATIONS

Agencies must confirm that requested PPS changes are accurate, necessary, and compatible with existing network and security architecture. Requests should include required documentation such as risk analysis, system dependencies, and rollback considerations. Implementation timelines may vary based on complexity and required coordination. All changes must be tested to verify proper function and prevent unintended exposure.

VII. EMERGING TRENDS AND ARCHITECTURAL DIRECTIONS

Firewall capabilities are shifting toward zero trust principles, cloud-native controls, and centralized policy management. Trends such as micro-segmentation, identity-aware enforcement, software-defined networking, and SASE will increasingly influence statewide architecture. Agencies should prepare for continued modernization and anticipate adjustments to firewall change processes as enterprise security evolves.

VIII. PROCEDURE REFERENCE

Firewall Change Request: https://idahoits.servicenowservices.com

NIST SP 800-30 (Most current) (Guide for Conducting Risk Assessments)

NIST SP 800-41 (Most current) (Firewall Policy)

Enterprise ITA Policy P4570 (Firewall Security)

Enterprise ITA Policy P4140 (Cybersecurity Framework)

Enterprise ITA Guideline G535 (Firewall Configuration Guidelines)

IX. REVIEW CYCLE

3 years

X. CONTACT INFORMATION

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

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

REVISION HISTORY

05/05/2026 – Was previously G536, updates finalize definitions, clarify standard and emergency change workflows, refine technical and documentation requirements, and align terminology and formatting.

Effective Date: May 5, 2026