Idaho Technology Authority (ITA)

ENTERPRISE POLICIES – P4500 SECURITY - COMPUTER AND OPERATIONS MANAGEMENT

Category: P4570 – FIREWALL SECURITY

CONTENTS:

I. Authority
II. Abstract
III. Definitions
IV. Policy
V. Exemption Process
VI. Procedure Reference
VII. Contact Information
VIII. Additional Information (if any)
Revision History

I. AUTHORITY

Authority: Idaho Code § 67-833

II. ABSTRACT

The Firewall Policy establishes standards for securing the agency's network perimeter, controlling inbound and outbound traffic, and enforcing least privilege access. It supports confidentiality, integrity, and availability by preventing unauthorized access, monitoring activity, and maintaining secure configurations. Roles, responsibilities, and change-management practices ensure consistent implementation and compliance with applicable regulations.

III. DEFINITIONS

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

IV. POLICY

1. Traffic Control. All inbound and outbound network traffic must pass through agency-approved firewalls configured in a deny-by-default posture. Exceptions must be documented, business-justified, and reviewed periodically.

2. Least Privilege. Firewall rules shall enforce the principle of least privilege, permitting only authorized traffic required for business operations. Quarterly audits must identify and remove obsolete or overly permissive rules.

3. Secure Configuration & Patch Management. Firewalls must be securely configured according to industry benchmarks (e.g., NIST, CIS). Firmware, OS, and security signatures must be updated promptly to address vulnerabilities. Automated tools should monitor for configuration drift.

4. Administrative Access Controls. Administrative access to firewalls must be restricted to authorized, secured management networks or hardened bastion hosts (jump servers) with centralized logging and session monitoring enabled. All administrative accounts must use multi-factor authentication (MFA), comply with strong credential policies, and follow the principle of least privilege.

5. Security Inspection. Allowed traffic must be inspected using layered security profiles, including intrusion prevention (IPS), anti-malware, URL filtering, and TLS/SSL decryption where feasible and compliant.

6. ICMP Controls (ITS-Supported Agencies Only). Inbound Internet Control Message Protocol (ICMP) traffic to ITS-managed state network perimeters shall be denied by default on agency-approved firewalls. Limited diagnostic exceptions may be authorized to permit ICMP Echo Reply (Type 0) and ICMP Time Exceeded (Type 11) messages inbound only to explicitly designated ITS-operated addresses or narrowly scoped subnets used by internal support teams. An ITS-controlled perimeter diagnostics host may be maintained with the sole capability of responding to ICMP Echo Requests (ping) for troubleshooting purposes.

7. Internal Segmentation. Agencies must implement internal segmentation (East-West controls) using firewalls or equivalent technologies to restrict lateral movement between network zones based on risk assessments.

8. Monitoring & Logging. Comprehensive logging of firewall events (traffic, management, and security) is required. Logs must be forwarded to a centralized SIEM, or log collector, for correlation and alerting. Alerts for critical anomalies must be defined and monitored continuously.

9. Change Management. Changes to firewall configurations require formal authorization, documentation, and testing prior to implementation. Emergency changes must follow expedited approval and post-change review.

V. EXEMPTION PROCESS

Refer to ITA Enterprise Policy P1010 (Information Technology Policies, Standards, and Guidelines Framework).

VI. PROCEDURE REFERENCE

G535 Firewall Configuration
S6040 Firewall Change Request
S6050 Security Firewall

VII. 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 - Updates streamline structure and definitions, strengthen technical requirements, and refine directive language.

07/01/18 – Changed “OCIO” to “ITS”.

02/23/16 – This policy replaces Enterprise ITA Standard S3200 (Firewall-Security) and provides high-level direction to state agencies regarding hardening and security best practices.

07/01/13 – Changed “ITRMC” to “ITA”.

06/16/09 – Added Procedure Reference and deleted Timeline.

04/25/05 – Added Cisco Firewall products.

Effective Date: October 2, 2001