

Government
Information
Technology
Agency

Statewide
STANDARD
P800-S830

TITLE: Network Security
Effective Date: DRAFT

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (A.R.S. § 41-3504(A (1))), including, the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to coordinate agency and State efforts to provide secure and seamless interconnections of the State's heterogeneous systems and communications networks, including modems, routers, switches, and firewalls while protecting the State's computing resources and information from the risk of unauthorized access from external sources.

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology PSPs within each Agency.

4. STANDARD

The following network security standards provide minimum requirements for providing secure and seamless interconnection of communications networks and systems while protecting the State's computing resources and information. Multi-layered protection shall be deployed at the Internet gateway, the network server, and the desktop levels to prevent introduction of malicious code or unauthorized access into the State's information systems.

- 4.1. **Firewall Technology:** Firewall technology shall be employed at the edge of an agency's network, including the Internet Gateway, to protect sensitive internal information assets and infrastructure from unauthorized access. External traffic must be routed through secure gateways, such as firewalls.

4.1.1. Network traffic filtering rules shall include the following:

- An incoming packet must not have a source address of the internal network.,
 - An incoming packet must have a publicly registered destination address associated with the internal network, if NAT/PAT is employed.
 - An outgoing packet must have a source address of the internal network.,
 - An outgoing packet must not have a destination address of the internal network.,
 - An incoming or outgoing packet must not have a source or destination address that is private or listed in RFC 1918 reserved space.
- 4.1.2 Any source routed packets or any packets with the IP options field set shall be blocked.
- 4.1.3 Reserved, DHCP auto-configuration and multicast addresses should be blocked.
- 4.1.4 Firewall technologies shall have security logging turned on.
- 4.1.5 Firewall policies should be regularly reviewed, tested, and audited.
- 4.1.6 Server-to-server communications should be secure to protect transmission of confidential or business critical data.
- 4.1.7 Unneeded services should be turned off, unused ports disabled, and logging capability turned on.
- 4.1.8 Agencies may collectively establish inter-agency service agreements (ISAs) to implement and maintain a “trusted peer” relationship among multiple participants. Each participant in the agreement shall agree to conform to all applicable requirements set forth in the agreement to ensure sufficient and acceptable security protection for all other participating agencies.
- 4.2. **Access to Internetworking Devices and Shared Platforms:**
Internetworking devices (including routers, firewalls, switches, etc.) and shared platforms (including mainframes, servers, etc.) provide both access to and information about networks. They must be controlled to prevent unauthorized access.
- Simple Network Management Protocol (SNMP) and telnet access should be controlled.
 - Internetworking devices connected to the Internet should have RFC 1918 and RFC 2827 implemented for inbound traffic.
 - Terminal Access Control Access Control System (TACACS) must be used to access routers.
 - Internetworking devices should have unneeded services turned off, unused ports disabled, and logging capability turned on.

- 4.3. **Demilitarized Zone:** Services provided through the Internet (Web-enabled applications, FTP, Mail, DNS, etc.) shall be deployed on a Demilitarized Zone (DMZ) or proxied from the DMZ.
- All communication from servers on the DMZ to internal applications and services shall be controlled.
 - Remote or dial-in access to networks shall be authenticated at the firewall, or through services placed on the DMZ.
 - The DMZ is the appropriate location for web servers, external DNS servers, VPN, and dial-in servers.
- 4.4. **External Connection to Networks:** External connections to networks shall be routed through secure gateways (as required above) and protected by at least one of the following encryption methods, as appropriate:
- Secure Socket Layer (SSL) shall be employed between a web server and browser to authenticate the web server and, optionally, the user's browser. Implementations of SSL shall allow for client authentication support using the services provided by Certificate Authorities.
 - IP Security (IPSec) shall be used to extend the IP communications protocol, providing end-to-end confidentiality for data packets traveling over the Internet. The appropriate mode of IPSec shall be used commensurate with the level of security required for the data being transmitted: sender authentication and integrity without confidentiality or sender authentication and integrity with confidentiality.
 - Virtual Private Networks (VPNs) shall be used to connect two networks or trading partners that must communicate over insecure networks, such as the public Internet, by establishing a secure link, typically between firewalls, using a version of the IPSec security protocol. VPNs are acceptable for use in remote access.
 - Remote Authentication Dial-In User Service (RADIUS) shall be used for dial-up modem systems. The authentication, authorization, and accounting (AAA) facility shall be employed for strong authentication (see P800-S820, Authentication and Directory Services, for additional authentication requirements).
 - Dial-up desktop workstation modems should be disabled and removed. Use hardware and inventory scanning tools to verify the presence and configuration of dial utilities and modems.
 - Agencies using dial-up modem systems shall establish modem use policies which include:
 - A complete, current list of all authorized personnel having modem access privileges.
 - Automatic disconnection after a specified period of inactivity. Inactivity parameters shall be determined by the agency.
 - The recommended use of security tokens.

- Immediate termination of modem access privileges upon employment transfer, re-assignment, or termination.
 - Strong authentication, such as challenge/response devices, one-time passwords, tokens, and smart cards, shall be used once permission to connect has been granted.
 - External connections shall be removed promptly when no longer required. Key network components shall be disabled or removed to prevent inadvertent reconnection.
- 4.5. **Wireless Network Access:** The 802.1x security standards having centralized user authentication and automated key distribution shall be used with standard wireless networks (IEEE 802.11x for LAN and IEEE 802.16 for MAN).
- The IEEE 802.11 standard that defines Wired Equivalent Privacy (WEP) specifies only a 40-bit encryption key, which is unacceptably susceptible to compromise.
 - Once developed, the IEEE 128-bit encryption solution, Enhanced Security Network (ESN), shall be used for wireless networks.
- 4.6. **Intrusion Detection:** Intrusion detection mechanisms should be incorporated into all servers connected to WANs and to all firewalls that serve as gateways between WAN network segments.
- When used, intrusion detection systems shall be installed both external and internal to firewall technology protecting the network to monitor, block, and report unauthorized activity.
 - Intrusion detection mechanisms for servers shall include the use of software and review procedures that scan for unauthorized changes to files, including system files.
 - Software and review procedures shall examine network traffic for known, suspicious attack signatures or activities and look for network traffic indicative of devices that have been misconfigured.
 - Violations of set parameters shall trigger appropriate notification to security administrators or agency staff, allowing a response to be undertaken.
- 4.7. **Vulnerability Scanning:** Vulnerability scanners should be components of the State's comprehensive network security solutions. Such components allow security administrators to measure security, manage risk, and eliminate vulnerabilities, providing a more secure network environment. Scanners should have the ability to do the following:
- Map the network or inventorying systems and services on the agency's network,
 - Identify security holes by confirming vulnerabilities

- Provide effective analysis of vulnerability data using browsing techniques, and enforcing valid security policies when used during security device installation and certification.
- Provide comprehensive reports and charts for effective decision making and improved security, and
- Define and enforce valid security policies when used during security device installation and certification.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms for definitions and abbreviations.

6. REFERENCES

- 6.1. A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions”.
- 6.2. A. R. S. § 41-1335 ((A (6 & 7))), “State Agency Information”.
- 6.3. A. R. S. § 41-1339 (A), “Depository of State Archives”.
- 6.4. A. R. S. § 41-1461, “Definitions”.
- 6.5. A. R. S. § 41-1463, “Discrimination; unlawful practices; definition”.
- 6.6. A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities”.
- 6.7. A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability”.
- 6.8. A. R. S. § 41-3501, “Definitions”.
- 6.9. A. R. S. § 41-3504, “Powers and Duties of the Agency”.
- 6.10. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition”.
- 6.11. A. R. S. § 44-7041, “Governmental Electronic Records”.
- 6.12. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office”.
- 6.13. Arizona Administrative Code, Title 2, Chapter 10, “Department of Administration Risk Management Section”.
- 6.14. Arizona Administrative Code, Title 2, Chapter 18, “Government Information Technology Agency”.
- 6.15. Statewide Information Technology Policy P100.
- 6.16. Statewide IT Security Policy P800.
- 6.17. Authentication and Directory Services Standards P800-S820.
- 6.18. State of Arizona Target Security Architecture,
http://gita.state.az.us/enterprise_architecture.

7. ATTACHMENTS

None.