ARIZONA STATEWIDE INFORMATION SECURITY	**STATEWIDE POLICY**	**State of Arizona**

STATEWIDE POLICY (8350): SYSTEM AND COMMUNICATION PROTECTIONS

DOCUMENT NUMBER:	**P8350**
EFFECTIVE DATE:	**DRAFT SEPTEMBER 17, 2018**
REVISION:	**2.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 18-104 and § 18-105. REFERENCE STATEWIDE POLICY FRAMEWORK 8350 SYSTEM AND COMMUNCATION PROTECTIONS.

2. PURPOSE

The purpose of this policy is to establish the baseline controls for the protection of agency information systems and their communications.

3. SCOPE

3.1 **Application to Budget Units** (BU) - This policy shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 **Application to Systems** - This policy shall apply to all agency information systems:

a. **(P)** Policy statements preceded by "(P)" are required for agency information systems categorized as Protected.

b. **(P-PCI)**Policy statements preceded by "(P-PCI)" are required for agency information systems with payment card industry data (e.g., cardholder data).

c. **(P-PHI)** Policy statements preceded by "(P-PHI)" are required for agency information systems with protected healthcare information.

d. **(P-FTI)** Policy statements preceded by "(P-FTI)" are required for agency information systems with federal taxpayer information.

3.3 Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services

a. BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services, BU SMEs shall consider Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

4.2 BU has taken the following exceptions to the Statewide Policy Framework:

Section Number	Exception	Explanation / Basis

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of IT PSPs throughout all state BUs.

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the State CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Statewide Information Technology PSPs throughout all state BUs;

b. Review and approve BU security and privacy PSPs and requested exceptions from the statewide security and privacy PSPs; and

c. Identify and convey to the State CIO the risk to state information systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 BU Director shall:

- **a.** Be responsible for the correct and thorough completion of Agency Information Technology PSPs within the BU;
- **b.** Ensure BU compliance with System and Communication Protections Policy; and
- **c.** Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.4 BU Chief Information Officer (CIO) shall:

- **a.** Work with the BU Director to ensure the correct and thorough completion of Agency Information Technology PSPs within the BU; and
- **b.** Ensure System and Communication Protections Policy is periodically reviewed and updated to reflect changes in requirements.

5.5 BU ISO shall:

- **a.** Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with BU Information Technology PSPs;
- **b.** Ensure the development and implementation of adequate controls enforcing the System and Communication Protections Policy for the BU; and
- **c.** Ensure all personnel understand their responsibilities with respect to the protection of agency information systems and their communications.

5.6 Supervisors of agency employees and contractors shall:

- **a.** Ensure users are appropriately trained and educated on System and Communication Protections Policies; and
- **b.** Monitor employee activities to ensure compliance.

5.7 System Users of agency information systems shall:

- **a.** Become familiar with this policy and related PSPs; and
- **b.** Adhere to PSPs regarding the establishment and maintenance of user accounts for agency information systems.

6. STATEWIDE POLICY

6.1 **Network and Architectural Controls** - The BU shall ensure the agency information system implements the following network and network architectural controls.

6.1.1 (P) **Application Partitioning** - The BU shall ensure the agency information system separates user functionality (including user interface services) either physically or logically from agency information system management functionality (e.g., privileged access). [NIST 800 53 SC-2] [IRS Pub 1075]

6.1.2 **Boundary Protection** - The BU shall ensure the agency information system: [NIST 800 53 SC-7]

- **a.** Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;
- **b.** Implements sub-networks for publicly accessible system components that are logically separated from internal organizational networks; and
- **c.** Connects to external networks of information systems only through managed interfaces consisting of boundary protections devices arranged in accordance with organizational security architecture.

6.1.2.3 (P) **Implement DMZ (demilitarized zone)** - The BU shall ensure the agency information system prohibits direct public access between the Internet and any system component in the Protected agency information system. The DMZ: [PCI DSS 1.3]

- **a.** Limits inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [PCI DSS 1.3.1]
- **b.** Limits inbound Internet traffic to IP addresses within the DMZ; [PCI DSS 1.3.2]
- **c.** Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [PCI DSS 1.3.3]
- **d.** Does not allow unauthorized outbound traffic from the Protected agency information system to the Internet; [PCI DSS 1.3.4]
- **e.** Permits only “established” connections into the network. [PCI DSS 1.3.5]
- **f.** Places system components that store Confidential data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks; and [PCI DSS 1.3.6]
- **g.** Does not disclose private IP addresses and routing information to unauthorized parties (Note: methods to obscure IP addressing may include: Network Address Translations (NAT), placing servers behind proxy servers, removal route advertisements for private networks that employ registered addressing, or internal use of RFC 1918 address space instead of registered addresses). [PCI DSS 1.3.7]

6.1.2.4 (P) **Firewall Configuration Standards** - The BU shall establish and implement firewall and router configuration standards that include the following: [PCI DSS 1.1]

- **a.** A formal process for approving and testing all network connections and changes to the firewall and router configurations; [PCI DSS 1.1.1]
- **b.** Current network diagrams that identifies all connections between the agency information system and other networks, including any wireless networks; [PCI DSS 1.1.2]
- **c.** Current diagram that shows all Confidential data flows across systems and networks; [PCI DSS 1.1.3]
- **d.** Requirements for a firewall at each Internet connection and between any DMZ and the Internal network zone; [PCI DSS 1.1.4]
- **e.** Description of groups, roles, and responsibilities for management of network components; [PCI DSS 1.1.5]
- **f.** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation for security features implemented for those protocols considered to be insecure. [PCI DSS.1.1.6]
- **g.** Requirement to review firewall and router rule sets at least every six (6) months. [PCI DSS 1.1.7]

6.1.2.5 (P) **Firewall Configuration** - The BU shall build firewall and router configurations that restrict access points between Non-Protected systems (Standard agency information systems or untrusted networks) and any system components in the Protected agency information system. The configurations: [PCI DSS 1.2]

- **a.** Restrict inbound and outbound traffic to that which is necessary for the Protected agency information system; [PCI DSS 1.2.1]
- **b.** Secure and synchronize router configuration files; and [PCI DSS 1.2.2]
- **c.** Implement perimeter firewalls between all wireless networks and the Protected agency information system, and these firewalls are configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the Protected agency information system. [PCI DSS 1.2.3]

6.1.3 (P) **Limit Access Points** - The BU shall limit the number of external network connections to the agency information system. [NIST 800 53 SC-7(3)] [IRS Pub 1075]

6.1.4 (P) **Deny by Default / Allow by Exception** - The BU shall ensure the agency information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception). [NIST 800 53 SC-7(5)] [IRS Pub 1075]

6.1.5 (P) **Network Disconnect** - The BU shall ensure agency information system terminates the network connections associated with a communications session at the end of the session or after 15 minutes of inactivity. [NIST 800 53 SC-10] [IRS Pub 1075]

6.2 Server Controls - The BU shall ensure the agency information system implements the following controls for servers and components of the agency information system:

6.2.1 (P) **Information in Shared Resources** - The BU shall ensure the agency information system prevents unauthorized and unintended information transfer using shared system resources. [NIST 800 53 SC-4] [IRS Pub 1075]

6.2.2 (P) **Prevent Split Tunneling for Remote Devices** - The BU shall ensure the agency information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating using some other connection to resources in external networks. [NIST 800 53 SC-7(7)] [IRS Pub 1075]

6.2.3 (P) **Single Primary Function (Database)** - The BU shall ensure agency information system components (e.g., servers) implementing a database implement only one primary function (the database) on this server. [PCI DSS 2.2.1]

6.2.4 (P-PCI) **Single Primary Function -** For agency information systems storing, processing, or transmitting cardholder data (CHD), the BU shall ensure all agency information system components (e.g., server) implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. [PCI DSS 2.2.1]

6.2.5 (P) **Minimum and Secure Services** - The BU shall ensure the agency information system component (e.g., server) enables only necessary and secure services, protocols, daemons, etc. as required for the function of the system. [PCI DSS 2.2.2]

a. (P-PCI) - For agency information systems with cardholder data (CHD) unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers must be removed. [PCI DSS 2.2.5]

b. (P) Otherwise Protected - For all other agency information systems unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers must be disabled or removed. [PCI DSS 2.2.2, 2.2.4]

c. Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. [PCI DSS 2.2.3]

6.2.6 (P) **Secure Configuration** - The BU shall configure the agency information system component (e.g., server) security parameters to prevent misuse. [PCI DSS 2.2.4]

6.3 Secure Services - The BU shall ensure the agency information system implements the following controls for services provided:

6.3.1 Denial of Service Protection - The BU shall ensure the agency information system protects against or limits the effects of the following types of denial of service attacks, defined in Standard 8350, System and Communication Protection, by employing boundary protection devices with packet filtering capabilities and, if required by the BU, employing increased capacity and bandwidth combined with service redundancy. [NIST 800 53 SC-5]

6.3.2 (P) **Cryptographic Services** - The BU shall ensure the agency information system implements the following cryptographic services:

a. (P) Cryptographic Protection - The agency information system shall implement Federal Information Processing Standards (FIPS) validated cryptography for the protection of Confidential information during transmission over open public networks and in accordance with applicable federal and state laws, Executive orders, directives, policies, regulations, and standards. [NIST 800 53 SC-13] [PCI DSS 4.1] [HIPAA 164.312(a)(2)(iv), (e)(2)(i)]

b. (P) Cryptographic Key Establishment and Management - The BU shall establish and manage cryptographic keys for required cryptography employed within the agency information system in accordance with statewide requirements for key generation, distribution, storage, access, and destruction. [NIST 800 53 SC-12]

6.3.2.1 (P) **Key Protection** - The BU shall protect all keys used to secure Confidential data against disclosure and misuse: [PCI DSS 3.5]

a. Restrict access to cryptographic keys to the fewest number of custodians necessary; and [PCI DSS 3.5.2]

b. Store secret and private keys used to encrypt/decrypt Confidential data in one (or more) of the following forms at all times: [PCI DSS 3.5.3]

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key

- Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device)
- As at least two full-length key components or key shares, in accordance with an industry accepted method

c. Store cryptographic keys securely in the fewest possible locations. [PCI DSS 3.5.4]

6.3.2.2 (P) **Key Management Process** - The BU shall fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of Confidential data including the following: [PCI DSS 3.6]

a. Generation of strong cryptographic keys; [PCI DSS 3.6.1]

b. Secure cryptographic key distribution; [PCI DSS 3.6.2]

c. Secure cryptographic key storage; [PCI DSS 3.6.3]

d. Cryptographic key changes for keys that have reached the end of their crypto-period, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines; [PCI DSS 3.6.4]

e. Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened, or keys are suspected of being compromised; [PCI DSS 3.6.5]

f. If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control; [PCI DSS 3.6.6]

g. Prevention of unauthorized substitution of cryptographic keys; and [PCI DSS 3.6.7]

h. Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. [PCI DSS 3.6.8]

6.3.2.3 (P) **Public Key Infrastructure Certificates** -The BU shall obtain public key certificates from an approved service provider. [NIST 800 53 SC-17] [IRS Pub 1075]

6.3.3 (P) **External Telecommunications Services** - The BU shall ensure: [NIST 800 53 SC-7(4)] [IRS Pub 1075]

a. Implement a managed interface for each external telecommunication service;

b. Establish a traffic flow policy for each managed interface;

c. Protect the confidentiality and integrity of the information being transmitted across each interface;

d. Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and

e. Review exceptions to the traffic flow policy annually and removes exceptions that are no longer supported by an explicit mission/business need.

6.3.4 (P) **Transmission Confidentiality and Integrity** - The BU shall ensure the agency information system protects the confidentiality and, if required, integrity of transmitted information. [NIST 800 53 SC-8] [IRS Pub 1075] [HIPAA 164.312(c)(1), (c)(2), (e)(1)]

6.3.4.1 (P) Cryptographic or Alternate Physical Protection - The BU shall ensure the agency information system prevents unauthorized disclosure of information and, if required, detects changes to information during transmission unless otherwise protected by BU-defined alternative physical safeguards. [NIST 800 53 SC-8(1)] [IRS Pub 1075] [HIPAA 164.312(c)(1), (c)(2), (e)(1)]

6.3.5 (P) **Mobile Code** - The BU shall: [NIST 800 53 SC-18] [IRS Pub 1075]

a. Define acceptable and unacceptable mobile code and mobile code technologies (e.g., Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript);

b. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorize, monitor, and control the use of mobile code within the agency information system.

6.3.6 **Collaborative Computing Devices** - The BU shall ensure the agency information system prohibits remote activation of collaborative computing devices with the following exceptions: cameras and microphones in support of remote conferences and training; and provides an explicit indication of use to users physically present at the devices. [NIST 800 53 SC-15]

6.3.7 (P) **Voice over Internet Protocol (VoIP)** - The BU shall establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and authorizes, monitors, and controls the use of VoIP within the prospective area. [NIST 800 53 SC-19] [IRS Pub 1075]

6.3.8 (P) **Session Authenticity** - The BU shall ensure the agency information system protects the authenticity of communication sessions. Note: This control addresses communications protections at the session, versus packet level and

establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted. Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions. [NIST 800 53 SC-23] [IRS Pub 1075]

6.3.9 Secure Name/Address Resolution Service - The BU shall ensure the agency information system implements the following with respect to secure name/ address resolution service:

a. Secure Name/Address Resolution Service (Authoritative Service) - The BU shall ensure the agency information system provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. [NIST 800 53 SC-20]

b. Secure Name/Address Resolution Service (Recursive or Caching Resolver) - The BU shall ensure the agency information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. [NIST 800 53 SC-21]

c. Architecture and Provisioning for Name/Address Resolution Service - The BU shall ensure the agency information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation. [NIST 800 53 SC-22]

6.3.10 (P) **Protection of Information at Rest** - The BU shall ensure the agency information system protects the integrity of audit log data at rest. [NIST 800 53 SC-28]

6.3.11 (P-FTI) **Protection of Taxpayer Information at Rest** - For systems with taxpayer information, The BU shall ensure the agency information system protects the confidentiality and integrity of taxpayer information at rest. [IRS Pub 1075]

6.4 Establish Operational Procedures – The BU shall ensure that security policies and operational procedures for managing firewalls (including managing vendor defaults and other security parameters and protecting Confidential data) are documented, in use, and known to all affected parties. [PCI DSS 1.5, 2.5, 3.7, 4.3]

6.5 Change Vendor Defaults – The BU shall ensure that vendor-supplied defaults are always changed and default accounts are removed or disabled before installing a system on the

network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, Simple Network Management Protocol (SNMP) community strings, etc.). [PCI DSS 2.1]

6.5.1 Change Wireless Vendor Defaults - For wireless environments connected to the agency information system or transmitting Confidential data change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. [PCI DSS 2.1.1]

6.6 Configuration Standards – The BU shall ensure that configuration standards for all system components are developed. The BU shall assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: [PCI DSS 2.2]

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- National Institute of Standards and Technology (NIST)

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET website.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8350 SYSTEM AND COMMUNICATIONS PROTECTION

8.2 Statewide Standard 8350, System and Communication Protection

8.3 Statewide Policy Exception Procedure

8.4 NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013.

8.5 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

8.6 Payment Card Industry Data Security Standard (PCI DSS) v3.2.1, PCI Security Standards Council, May 2018.

8.7 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2010.

9. ATTACHMENTS

None.

9. REVISION HISTORY

Date	Change	Revision	Signature
9/01/2014	Initial Release	Draft	Aaron Sandeen, State CIO and Deputy Director
10/11/2016	Updated all the Security Statutes	1.0	Morgan Reed, State CIO and Deputy Director