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 (ARS)§ 18-104 and § 18-105. REFERENCE STATEWIDE POLICY FRAMEWORK P8280 ACCEPTABLE USE.

2. **PURPOSE**

The purpose of this policy is to provide a framework for the protection of data that is created, stored, processed or transmitted STATEWIDE. The classification of data is the foundation for the specification of policies, procedures, and controls necessary for the protection of Confidential Data.

3. **SCOPE**

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

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

   a. (P) Policy statements preceded by “(P)” are required for BU information systems categorized as Protected.

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

   c. (P-PHI) Policy statements preceded by “(P-PHI)” are required for BU information systems with protected healthcare information.
d. (P-FTI) Policy statements preceded by “(P-FTI)” are required for BU 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 subject matter experts 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:
   a. Be ultimately responsible for the correct and thorough completion of Statewide 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 all state BU activities and documentation provided to ensure compliance with statewide IT PSPs throughout all state BUs;

b. Review and approve or disapprove all state BU security and privacy PSPs and exceptions to existing 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 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of BU PSPs;

b. Ensure compliance with BU PSPs;

c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets; and

d. Be the data owner for all Confidential Data sets or shall delegate a data owner for each set of Confidential Data.

5.5 BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of BU IT PSPs; and

b. Ensure BU PSPs are periodically reviewed and updated to reflect changes in requirements.

5.6 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 BU PSPs;

c. Request changes and/or exceptions to existing PSPs from the State CISO; and

d. Ensure all personnel understand their responsibilities with respect to securing agency information systems, including classification of data and handling.
5.7 Data Owner shall:
   a. Assign classification of data;
   b. Assign data custodians and ensure data custodian is familiar with the protection requirements for Confidential Data;
   c. Participate in establishing, approving and maintaining policies for the protection of data within state agency; and
   d. Promote data resource management within the state agency.

5.8 Data Custodian shall:
   a. Ensure implementation of controls according to BU PSPs.

5.9 Supervisors of agency employees and contractors shall:
   a. Ensure users are appropriately trained and educated on BU PSPs; and
   b. Monitor employee activities to ensure compliance.

5.10 System Users of agency information systems shall:
   a. Become familiar with this and related PSPs; and
   b. Adhere to PSPs regarding classification of data and handling within agency information systems.

6. STATEWIDE POLICY

6.1 Data Classification - Data created, stored, processed or transmitted on agency information systems shall be classified according to the impact to the state or citizens resulting from the disclosure, modification, breach or destruction of the data.

6.2 Data Classification Categories - All agency data shall be classified as one of the following categories: [National Institute of Standards and Technology Special Publication (NIST SP) 800-53 RA-2]

6.2.1 Confidential Data - Data that shall be protected from unauthorized disclosure based on laws, regulations, and other legal agreements. Examples of Confidential Data include:
   a. System Security Parameters and Vulnerabilities
      1. System security vulnerabilities
      2. Generated security information
3. Information regarding current deployment, configuration, or operation of security products or controls

b. Health Information
   1. Protected Health Information [Health Insurance Portability and Accountability Act (HIPAA) - PL 104-191, Sections 261 - 264, 45 CFR Part 160 and 164]
   3. Child immunization data [A.R.S. § 36-135]
   4. Chronic disease information [A.R.S. § 36-133]
   5. Communicable disease information [A.R.S. § 36-664, A.R.S. § 36-666]
   6. Developmental disabilities service records [A.R.S. § 36-568.01, A.R.S. § 36-568.02]
   7. Emergency medical service patient records [A.R.S. § 36-2220]
   8. Genetic testing records [A.R.S. § 12-2801, A.R.S. § 12-2802]
   9. Home health service records [A.R.S. § 36-160]
  10. Midwifery patient records [A.R.S. § 36-756.01]
  11. State trauma registry [A.R.S. § 36-2221]
  12. Tuberculosis control court hearing information [A.R.S. § 36-727]

c. Financial Account Data (on individuals)
   1. Card Holder Data (CHD) including Primary Account Number (PAN), Cardholder Name, Expiration Date, and Service Code [Payment Card Industry Data Security Standard (PCI DSS) v3.2.1]
   2. Credit card, charge card or debit card numbers, retirement account numbers, savings, checking or securities entitlement account numbers [A.R.S. § 44-1373]

d. Criminal Justice Information
   2. Criminal history record information [A.R.S. § 41-619.54]
   3. Criminal Justice Information [A.R.S. § 41-1750]

e. Critical Infrastructure/Fuel Facility Reports [A.R.S. § 41-4273]


g. Risk Assessment and State Audit Records
   1. Auditor General Records [A.R.S. § 41-1279.05]
h. Personal Identifying Information (except as determined to be public record) [A.R.S. § 18-522, 18-551]
   1. Educational records [Family Educational Rights and Privacy Act (FERPA)]
   2. Social Security Number [A.R.S. § 44-1373]

i. Taxpayer Information - Federal Tax Information (FTI) [A.R.S. § 42-2001]
   [Internal Revenue Service Publication 1075 (IRS Pub 1075)]

j. Licensing, Certification, Statistics and Investigation Information (of a sensitive nature)
   1. Abortion reports [A.R.S. § 36-2161]
   2. Child Death Records [A.R.S. § 36-3503]
   3. Controlled substance records [A.R.S. § 36-2523]
   4. Emergency medical service investigation records [A.R.S. § 36-2220]
   5. Employment discrimination information [A.R.S. § 41-1482]
   7. Health Care Directives Registry Information [A.R.S. § 36-3295]
   8. Health care entity licensing information [A.R.S. § 36-2403, A.R.S. § 36-404]
   9. Medical Marijuana Records [A.R.S. § 36-2810]
   11. Nursing home certification records [A.R.S. § 36-446.10]
   12. Prescription information [A.R.S. § 36-2604]

k. Other State-owned Confidential Data, may include but not limited to:
   1. Archaeological discoveries [A.R.S. § 39-125]
   3. Tax Examination guidelines [A.R.S. § 42-2001]
   4. Unclaimed property reports [A.R.S. § 44-315]
   5. Vehicle information [A.R.S. § 41-3452]

l. Other Non-state-owned Confidential Data, may include, but not limited to:
   1. Attorney-Client Privileged Information [A.R.S. § 41-319]
   2. Bank Records [A.R.S. § 6-129]
   3. Trade secrets and proprietary information [Intellectual Property laws]
   4. Management and Support Information

m. Other records protected by law
6.2.2 Public Data - In accordance with Arizona public records law, data that may be released to the public and requires no additional levels of protection from unauthorized disclosure.

6.3 Identification - All data shall be identified as one of the following data classifications:
   a. Confidential; or
   b. Public (data that is not identified is assumed to be Public).

6.4 Collection
   a. (P) Limit Collection -
      1. Encrypt confidential data
      2. Properly dispose, destroy, or delete data
      3. Limit access to confidential information
      4. Securely store confidential data

6.5 Handling

6.5.1 (P) Need to Know - All Confidential Data shall only be given to those persons that have authorized access and a need to know the information in the performance of their duties. [HIPAA 164.308 (a)(3)(ii)(A) – Addressable] [PCI DSS 7]

6.5.2 (P) Hand Carry - All Confidential Data being hand-carried shall be kept with the individual and protected from unauthorized disclosure.

6.5.3 (P) Accounting - For bulk transfer of Confidential Data containing 500 or more records, the receipt and delivery of all Confidential Data shall be monitored and accounted for to ensure the data is not lost and potentially compromised.

6.5.4 (P) Guardian - When outside of controlled areas all Confidential Data shall not be left unattended, even temporarily. All Confidential Data shall remain either in a controlled environment or in the employee's physical control at all times. Mail, courier, or other mail services are considered controlled areas.

6.5.5 (P) Out-of-sight - All Confidential Data shall be turned over or put out of sight when visitors not authorized to view data are present.

6.5.6 (P) Conversations - Confidential Data shall not be discussed outside of controlled areas when visitors not authorized to hear Confidential Data are present.
6.5.7 (P) Movement - Unauthorized movement of Confidential Data from controlled areas shall be prohibited. [HIPAA 164.310 (d)(1)]

6.6 Transmission

6.6.1 (P) Encryption - Any external transmission of Confidential Data shall be encrypted either through link or end-to-end encryption. [HIPAA 164.308 (e)(2)(ii) – Addressable] [PCI DSS 4]

6.6.2 (P) Encryption Strength - Encryption algorithm and key length shall be compliant with current state agency minimum encryption standards as stated in the System and Communications Protection Standard [S8350].

6.7 Processing

6.7.1 (P) Approved Processing - Confidential Data shall be processed on approved devices.

6.8 Media Protection

6.8.1 (P) Confidential Data Protection - All Confidential Data shall be protected and implemented at minimum controls as stated in the Media Protection Policy P8250 and Media Protection Standard S8250. [HIPAA 164.310 (d)(2)] [PCI DSS 3, 9]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK P8110 DATA CLASSIFICATION

8.2 Statewide Policy Exception Procedure

8.3 Standard S8350, System and Communications Protections

8.4 Policy P8250, Media Protection Policy

8.5 Standard S8250, Media Protection Standard

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


9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8120): INFORMATION SECURITY PROGRAM

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration, 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 P8120 Information Security Program.

2. PURPOSE

The purpose of this policy is to establish the information security program and responsibilities within the Budget Unit (BU).

3. SCOPE

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

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

   a. (P) Policy statements preceded by “(P)” are required for BU information systems categorized as Protected.

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

   c. (P-PHI) Policy statements preceded by “(P-PHI)” are required for BU information systems with protected healthcare information.

   d. (P-FTI) Policy statements preceded by “(P-FTI)” are required for BU information systems with federal taxpayer information.
3.3 **Federal Government Information** - 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 and 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

   b. Ensure that by July 1 of each year all BUs have submitted the following information for approval:
1. A state information system inventory with a system classification assignment and system owner for each state information system
2. A system security plan and system security assessment plan for each Protected state information system
3. A Plan of Actions and Milestones (POAM) for each Protected state information system

c. Ensure that information security risks identified in Protected state information system risk assessment documentation are adequately addressed for all BUs.

5.2 State Chief Information Security Officer (CISO) shall:

   a. Provide a format for the required compliance documents;

   b. 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;

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

   d. Identify and convey to the State CIO the risk to state information systems and data based on a review of the BU-supplied state information system inventory, system security plans, system security assessment plans and the Plan of Actions and Milestones (POAM);

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

   f. Recommend a course of action where security risks are not adequately addressed. Course of action may include, but is not limited to, the following recommendations:

      1. Identify a plan to address the documented risks
2. Implement recommended security controls
3. Perform independent security assessment on selected state information systems or controls
4. Hosting of state information system or state information system components in a state approved solution(s)
5. Adopt any additional security requirements or procedures for the BU or selected BU state information systems, controls, or control environments

5.3 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards; and
   b. Advise the State CISO in determination of resources needed to implement the information security programs, and availability of planned expenditures.

5.4 BU Director shall:
   c. Be responsible for the correct and thorough completion of Information Technology PSPs within the BU;
   d. Ensure BU compliance with Information Security Program Policy; and
   e. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 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;
   b. Ensure all BU managed systems have submitted the following documents for approval by the State CIO or designated alternate by July 1 of each year:
      1. A complete list of information systems with a system classification assignment and system owner for each agency information system
      2. A system security plan and system security assessment plan for each Protected agency information system
      3. A Plan of Actions and Milestones (POAM) for each Protected agency information system
   c. Ensure information security risks to Protected agency information systems, are adequately addressed according to the Protected agency information system risk assessment documentation; and
   d. Be system owner for all agency information systems or delegates a system owner for BU agency information system.
5.6 BU Information Security Officer (ISO) shall:
   a. Advise the BU CIO on the completeness and adequacy of the BU provided documentation and reports and recommend a course of action where security risks are not adequately addressed;
   b. Ensure all system owners understand their responsibilities for the security planning, management, and authorization of agency information systems; and
   c. Ensure the correct execution of the system security assessment plans.

5.7 System Owner shall:
   a. Be responsible for the overall procurement, development, integration, modification, or operation and maintenance of the agency information system; [NIST SP 800-18]
   b. Advise BU ISO as to the agency information system categorization;
   c. Ensure creation of required system security plans, system security assessment plans, Plan of Actions and Milestones (POAM); and
   d. Ensure the implementation of information security controls as described in system security plans and POAM.

6. STATEWIDE POLICY

6.1 System Security Planning - The BU shall implement the following controls in the planning of system security:

6.1.1 System Security Plan - The BU shall develop, distribute, review annually, and update an agency information system security plan. The plan shall: [NIST 800-53 PL-2]
   a. Be consistent with the BU’s enterprise architecture (EA);
   b. Explicitly define the authorization boundary for the system including authorized connected devices (e.g., smart phones, authorized virtual office computer equipment, and defined external interfaces);
   c. Describe the operational context of the agency information system in terms of missions and business processes;
   d. Provide the security categorization of the information system;
   e. Describe the relationships with or connections to other information systems;
   f. Provide an overview of the security requirements for the system;
g. Describe the security controls in place or planned for meeting those requirements including rationale for the tailoring and supplementation decisions;

h. Be reviewed and approved by the BU CIO prior to plan implementation; and

6.1.2 (P) Coordinate With Other Organizational Entities - The BU shall plan and coordinate security-related activities affecting the agency information system with the BU CIO, BU ISO, and system owners of affected agency information systems before conducting such activities in order to reduce the impact on other organizational entities. [NIST 800-53 PL-2(3)] [IRS Pub 1075]

6.1.3 (P) Information Security Architecture – The BU shall: [NIST 800-53 PL-8][IRS Pub 1075]

a. Develop an information security architecture for the agency information system that describes:
   1. The overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information
   2. How the information security architecture is integrated into and supports the enterprise architecture
   3. Any information security dependencies on, and assumptions regarding, external services

b. Annually, review and update the information security architecture to reveal updates in the enterprise architecture; and

c. Ensure that planned information security architecture changes are reflected in the security plan and organizational procurements/acquisitions.

6.2 System Security Policies – The BU shall develop, document and disseminate, to appropriate personnel and roles, the following policies and procedures for each agency information system. These policies shall be reviewed at least annually and updated when an environment, threat, or regulation prompts a change. [HIPAA 164.316 (a)] [PCI DSS 12.1.1]

a. Data Classification Policy and Procedures (P8110)

b. Information Security Program Policy and Procedures (P8120) [NIST 800-53 CA-1] [NIST 800-53 PL-1] [NIST 800-53 PM-1] [NIST 800-53 RA-1]

c. System Security Acquisition Policy and Procedures (P8130) [NIST 800-53 SA-1]
d.  Security Awareness Training Policy and Procedures (P8210) [NIST 800-53 AT-1]

e.  System Security Maintenance Policy and Procedures (P8220) [NIST 800-53 CM-1] [NIST 800-53 MA-1] [NIST 800-53 SI-1]

f.  Contingency Planning Policy and Procedures (P8230) [NIST 800-53 CP-1]

g.  Incident Response Planning Policy and Procedures (P8240); [NIST 800-53 IR-1]

h.  Media Protection Policy and Procedures (P8250) [NIST 800-53 MP-1]

i.  Physical Security Protection Policy and Procedures (P8260) [NIST 800-53 PE-1]

j.  Personnel Security Policy and Procedures (P8270) [NIST 800-53 PS-1]

k.  Acceptable Use Policy, including Social Media and Networking Restrictions (P8280) [NIST 800 53 AC-1] [NIST SP 800 53 PL-4(1)]

l.  Account Management Policy and Procedures (P8310)

m.  Access Controls Policy and Procedures (P8320) [NIST 800-53 AC-1] [HIPAA 164.310 (a)(2)(ii)]

n.  System Security Audit Policy and Procedures (P8330) [NIST 800-53 AU-1]

o.  Identification and Authentication Policy and Procedures (P8340) [NIST 800-53 IA-1]

p.  System and Communication Protections Policy and Procedures (P8350) [NIST 800-53 SC-1]

q.  System Privacy Policy and Procedures (P8410)

r.  System Privacy Notice (S8410)

6.2.1 Policy Maintenance and Distribution – The BU shall: [HIPAA 164.316 (b)(1), (b)(2)]

a.  Maintain the organizational security policies and procedures;

b.  Retain these documents for six years from the date of its creation or the date it last was in effect, whichever is later. However, all State BUs must comply with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to http://apps.azlibrary.gov/records/general_rs/Management.pdf Records Series Number 10293.;
c. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains; and

d. Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the Confidential information.

6.3 Security Risk Management - To appropriately manage security risk to agency information systems, the following activities shall be performed for each agency information system:

[HIPAA 164.308 (a)(1)(i), (a)(1)(ii)(B)]

6.3.1 Impact Assessment - A potential impact assessment shall be performed for each agency information system to determine the system categorization. An impact assessment considers the data sensitivity and system mission criticality to determine the potential impact that would be caused by a loss of confidentiality, integrity, or availability of the agency information system and/or its data. Impact assessments result in the determination of impact based on the following definitions:

a. Limited Adverse Impact - The loss of confidentiality, integrity, or availability could be expected to have limited adverse effect on organizational operations, organizational assets or individuals. For example, it may:
   1. Cause a degradation in mission capability, to an extent and duration, that the organization is able to perform its primary function, but the effectiveness of the function is noticeably reduced;
   2. Result in minor damage to organizational assets;
   3. Result in a minor financial loss; or
   4. Result in minor harm to individuals.

b. Serious Adverse Impact - The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals. For example, it may:
   1. Cause a significant degradation in mission capability, to an extent and duration, that the organization is able to perform it primary function, but the effectiveness of the function is significantly reduced;
   2. Result in significant damage to organizational assets;
   3. Result in a significant financial loss; or
   4. Result in significant harm to individuals that do not involve loss of life or serious life threatening injuries.

NOTE: Impact assessment on agency information systems storing, processing, or transmitting Confidential Data may result in a serious adverse impact.
6.3.2 System Security Categorization – The BU shall categorize agency information systems, document the security categorization results (including supporting rationale) in the security plan for the agency information system; and ensure that the security categorization decision is reviewed by the BU CSO and approved by the BU CIO. All agency information systems are categorized according to the potential impact to the state or citizens resulting from the disclosure, modification, destruction, or non-availability of system functions or data. [NIST 800-53 RA-2]

6.3.3 System Categorization Levels - The following system categorization levels shall be applied to all agency information systems:
   a. Standard - Loss of confidentiality, integrity, or availability could be expected to have a limited adverse impact on the BU’s operations, organizational assets, or individuals, including citizens
   b. Protected - Loss of confidentiality, integrity, or availability could be expected to have serious, severe, or catastrophic adverse impact on organizational, assets, or individuals, including citizens

6.3.4 Security Risk Assessment - The BU shall: [NIST 800-53 RA-3]
   [HIPAA 164.308 (a)(1)(ii)(A)]
   a. Conduct an assessment of security risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, modification, or destruction of the agency information system and the information it processes, stores, or transmits;
   b. Document risk assessment results in a risk assessment report;
   c. Review risk assessment results annually;
   d. Disseminate risk assessment results to the BU CIO, BU ISO, agency information system owner, and other BU-defined personnel or roles; and
   e. Perform the risk assessment annually or whenever there are significant changes to the information system or environment of operations (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. [PCI DSS 12.2]

6.3.5 Vendor Risk Management – The BU shall protect against vendor (e.g., Cloud Service Providers, contractors, supply chain) threats to the information system, system component, or information service by employing a vendor risk management program as part of a comprehensive, defense in-breadth information security strategy. [NIST 800-53 SA-12]

6.3.6 (P) Third Party Risk Assessment – The BU shall conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use,
disclosure, modification, or destruction of third parties authorized by the BU to process, store, or transmit Confidential Data. [HIPAA 164.308 (a)(ii)(A)]

6.3.7 **Vulnerability Scanning** – The BU shall establish a process to identify security vulnerabilities implementing the following: [NIST 800-53 RA-5] [PCI DSS 6.1, 11.2]

a. use reputable outside sources for security vulnerability information, [PCI DSS 6.1]

b. assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities [PCI DSS 6.1]

c. Scan for vulnerabilities in the agency information system and hosted applications quarterly and when new vulnerabilities potentially affecting the system/applications are identified and reported from internal and external interfaces; [PCI DSS 11.2.3]

d. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations
   2. Formatting checklists and test procedures
   3. Measuring vulnerability impact

e. Analyze vulnerability scan reports and results from security control assessments;

f. Remediate legitimate vulnerabilities within 30 days in accordance with an organization assessment of risk;

g. Share information obtained from the vulnerability scanning process and security control assessments with BU-defined personnel or roles to help eliminate similar vulnerabilities in other agency information systems (i.e. systemic weaknesses or deficiencies.);

h. (P) Establish a process to identify and assign risk ranking to newly discovered security vulnerabilities; [PCI DSS 11.2]

i. (P) Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved according to vulnerability ranking. [PCI DSS 11.2.1]

   1. (P) Update tool capability - The BU shall employ vulnerability scanning tools that include the capability to readily update the agency information system vulnerabilities to be scanned; [NIST 800-53 RA-5(1)] [IRS Pub 1075]
2. (P) Update prior to new scans - The BU shall update the agency information system vulnerabilities scanned prior to new scans; [NIST 800-53 RA-5(2)] [IRS Pub 1075]

3. (P) Provide privileged access - The agency information system implements privileged access authorization to BU-defined components containing highly Confidential Data (e.g., databases); and [NIST 800-53 RA-5(5)] [IRS Pub 1075]

4. (P) Qualify scanning vendors - The BU shall employ an impartial and qualified scanning vendor to conduct quarterly external vulnerability scanning. The assessors or assessment team is free from any perceived or real conflict of interest with regard to the development, operation, or management of the BU information systems under assessment and is qualified in the use and interpretation of vulnerability scanning software and techniques. [PCI DSS 11.2.2]

6.4 Information Security Program Management - The BU shall implement the following controls in the management of the information security program:

6.4.1 Senior Information Security Officer - The BU shall appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain a BU-wide information security program. [NIST 800-53 PM-2] [EO 2008-10]

6.4.2 Information Security Resources - The BU shall include the resources needed to implement the information security program and document all exceptions to this requirement. This includes employing a business case to record the resources required, and ensuring that information security resources are available for expenditure as planned.

6.4.3 Plan of Action and Milestones Process - The BU shall: [NIST 800-53 PM-4]

   a. Implement a process for ensuring that plans of action and milestones for the security program and associated agency information systems are:
      1. Developed and maintained
      2. Reported in accordance with reporting requirements
      3. Documented with the remedial information security actions to adequately respond to risk to organizational operations, assets, individuals, other organizations, and the state

   b. Review plans of action and milestones for consistency with the organizational risk management strategy and BU-wide priorities for risk response actions.
6.4.4 **Information Systems Inventory** - The BU shall develop and maintain an inventory of its information systems, including a classification of all system components (e.g., Standard or Protected). [NIST 800-53 PM-5]

6.4.5 **Information Security Measures of Performance** - The BU shall develop, monitor, and report on the results of information security measures of performance. [NIST 800-53 PM-6]

6.4.6 **Enterprise Architecture** - The BU shall develop the enterprise architecture with consideration for information security and resulting risk to organizational operations, organizational assets, individuals, other organizations, and the agency. [NIST 800-53 PM-7]

6.4.7 **Critical Infrastructure Plan** – If applicable, the BU shall address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. [NIST 800-53 PM-8]

6.4.8 **Risk Management Strategy** - The BU shall:
   a. Develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the agency associated with the operation and use of agency information systems; and
   b. Implement this strategy consistently across the organization. [NIST 800-53 PM-9]

6.4.9 **Security Authorization Process** – The BU shall: [NIST 800-53 PM-10]
   a. Manage the security state of organizational information systems and the environments in which those systems operate through security authorization processes;
   b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
   c. Fully integrates the security authorization processes into an BU-wide risk management program.

6.4.10 **Mission/Business Process Definition** - The BU shall: [NIST 800-53 PM-11]
   a. Define mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the agency; and
   b. Determine information protection needs arising from the defined mission/business processes and revises the process as necessary, until achievable protection needs are obtained.
6.4.11 Insider Threat Program - The BU shall implement an insider threat program that includes a cross-discipline insider threat incident handling team. [NIST 800-53 PM-12]

6.4.12 Information Security Workforce – The BU shall establish an information security workforce development and improvement program. [NIST 800-53 PM-13]

6.4.13 Testing, Training, and Monitoring - The BU shall: [NIST 800-53 PM-14]
   a. Implement a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems are developed and maintained; and continue to be executed in a timely manner; and
   b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and BU-wide priorities for risk response actions.

6.4.14 Contacts with Security Groups and Associations - The BU shall establish and institutionalize contact with selected groups and associations within the security community to: [NIST 800-53 PM-15]
   a. Facilitate ongoing security education and training for BU personnel;
   b. Maintain currency with recommended security practices, techniques, and technologies; and
   c. Share current security-related information including threats, vulnerabilities, and incidents.

6.5 Security Assessments and Authorizations - The BU shall implement the following controls in the assessment and authorization of agency information systems:

6.5.1 Security Assessments – The BU shall: [NIST 800-53 CA-2] [HIPAA 164.308 (a)(8)]
   a. Develop a security assessment plan that describes the scope of the assessment including security controls under assessment, assessment procedures to be used to determine security control effectiveness, and assessment environment, assessment team, and assessment roles and responsibilities;
   b. Assess the security controls in the information system and its environment of operation periodically to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
   c. Produce a security assessment report that documents the results of the assessment; and
d. Provide the results of the security control assessment to the BU CIO, BU CSO and the State CSO.

6.5.2 **(P) Independent Assessors** - The BU shall employ impartial assessors or assessment teams to conduct security control assessments. The assessors or assessment team is free from any perceived or real conflict of interest with regard to the development, operation, or management of the BU information systems under assessment. [NIST 800-53 CA-2(1)] [IRS Pub 1075]

6.5.3 **(P) Third Party Security Assessment** - The BU shall conduct a security assessment with third parties authorized by the BU that process, store, or transmit Confidential Data. [HIPAA 164.308 (a)(8)]

6.5.4 **(P) Wireless AP Testing** - The BU shall test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. [PCI DSS 11.1]

6.5.5 **System Interconnections** – The BU shall: [NIST 800-53 CA-3]

   a. Authorize connections from the agency information system to other information systems through the use of Interconnection Security Agreements;

   b. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

   c. Review and update Interconnections Security Agreements annually:

   1. **(P) Restrictions on External System Connections** - The BU shall employ a “deny-all, permit-by-exception” policy for allowing Protected agency information systems to connect to external information systems. [NIST 800-53 CA-3(5)] [IRS Pub 1075]

   2. **(P) Third Party Authorization** – The BU shall permit a third party, authorized by the BU to process, store, or transmit Confidential data, to create, receive, maintain, or transmit Confidential information on the BU’s behalf only if covered entity obtains satisfactory assurances that the third party will appropriately safeguard the information. The BU documents the satisfactory assurance through a written contract or other arrangement with the third party. [HIPAA 164.308 (b)(1) and (b)(2)]

6.5.6 **Plan of Action and Milestones** - The BU shall: [NIST 800-53 CA-5]

   a. Develop a plan of action and milestones for the agency information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security
controls and to reduce or eliminate known vulnerabilities in the system;
and
b. Update existing plan of action and milestones annually based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

6.5.7 Security Authorization – The BU shall: [NIST 800-53 CA-6]

a. Assign a senior-level executive or manager as the authorizing official for the information system;
b. Ensure the authorizing official authorizes the agency information system for processing before commencing operations; and
c. Update the security authorization every three years.

6.5.8 Continuous Monitoring - The BU shall develop a continuous monitoring strategy and implements a continuous monitoring program that includes: [NIST 800-53 CA-7] [HIPAA 164.308 (a)(1)(ii)(D)]

a. Establishment of security metrics to be monitored;
b. Establishment of frequencies for monitoring and frequencies for assessments supporting such monitoring;
c. Ongoing security control assessments in accordance with the BU continuous monitoring strategy;
d. Ongoing security status monitoring of the BU-defined metrics in accordance with the BU continuous monitoring strategy;
e. Correlation and analysis of security-related information generated by assessments and monitoring;
f. Response actions to address results of the analysis of security-related information; and
g. Reporting the security status of the BU and the information system to the State CISO quarterly.

6.5.9 (P) Penetration Testing - The BU shall conduct penetration testing annually and after significant infrastructure or application upgrade or modification on Protected agency information systems from internal and external interfaces. These penetration tests must include network-layer penetration tests, segmentation control tests, and application-layer penetration tests. [NIST 800-53 CA-8] [PCI DSS 11.3, 11.3.1, 11.3.2]

a. (P) Independent Penetration Agent or Team - The BU shall employ an impartial penetration agent or penetration team to perform penetration testing. The assessors or assessment team is free from any perceived or
real conflict of interest with regard to the development, operation, or management of the BU information systems under assessment. [NIST 800-53 CA-8]

b.  (P) Segmentation Testing – The BU shall ensure that penetration testing includes verification of segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all Protected systems and components systems from non-protected systems and components. [PCI DSS 11.3.4]

c.  (P) Address Penetration Testing Issues – The BU shall ensure that exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections. [PCI DSS 11.3.3]

6.5.10 Internal System Connections - The BU shall authorize internal connections of other agency information systems or classes of components (e.g., digital printers, laptop computers, mobile devices) to the agency information system and, for each internal connection, shall document the interface characteristics, security requirements and the nature of the information communicated. [NIST 800-53 CA-9] [IRS Pub 1075]

6.6 Establish Operational Procedures – The Agency BU shall ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. [PCI DSS 11.6]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 Statewide Policy Framework P8120 Information Security Program

8.2 Statewide Policy Exception Procedure

8.3 NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013, January 2012

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


8.7 Executive Order 2008-10

8.8 General Records Retention Schedule Issued to All Public Bodies, Management Records, Schedule Number GS 1005, Arizona State Library, Archives and Public Records, Item Number 16

9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State of Arizona CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
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 P8130 SYSTEM SECURITY ACQUISITION AND DEVELOPMENT.

2. PURPOSE

The purpose of this policy is to establish adequate security controls for the acquisition and deployment of agency information systems.

3. SCOPE

3.1 Application to Budget Units (BUs) - 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:
   a. Be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state budget units (BUs).

5.2 State Chief Information Security Officer (CISO) shall:
   a. Advise the State CIO on the completeness and adequacy of all state agency BU activities and documentation provided to ensure compliance with statewide IT PSPs throughout all state BUs;
   b. Review and approve all state agency BU security and privacy PSPs;
   c. Request exceptions from the statewide security and privacy PSPs; and
   d. 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 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 Budget Unit (BU) Director shall:
   b. Be responsible for the correct and thorough completion of BU PSPs;
   c. Ensure compliance with BU PSPs; and
   d. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 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 PSPs are periodically reviewed and updated to reflect changes in requirements.

5.6 BU Information Security Officer (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 Security Acquisition Policy for the BU; and
   c. Ensure all personnel understand their responsibilities with respect to secure acquisition of agency information systems and components.

5.7 BU Procurement Official shall:
   a. Provide advice and support with the procurement of goods and services in regards to request for information, request for proposal, evaluation of response, and contract awards; and
   b. Ensure compliance with Arizona procurement statutes and PSPs throughout the procurement process.

5.8 Purchaser shall:
   a. Abide by all PSPs throughout the procurement process.

6. STATEWIDE POLICY

6.1 Allocation of Resources - The BU shall: [NIST 800 53 SA-02]
a. Determine information security requirements for the agency information system or information system service in mission/business process planning;

b. Determine, document and allocate the resources required to protect the agency information system or information system service as part of its capital planning and investment control process; and

c. Establish a discrete line item for information security in organizational programming and budgeting documentation.

6.2 Technology Life cycle - The BU shall: [NIST 800 53 SA-03]

a. Manage the agency information system using a BU-defined technology life cycle that is based on industry standards or best practices and incorporates information security considerations; [PCI DSS 6.3]

b. Define and document information security roles and responsibilities throughout the technology life cycle;

c. Identify individuals having information security roles and responsibilities; and

d. Integrate the organizational information security risk management process into technology life cycle activities.

6.2.1 Software Development Process - The BU shall require developers of agency information systems or system components to implement the following software development processes: [PCI DSS 6.3]

a. Remove non-production application accounts, user IDs, and passwords before applications become active or are released to customers; and [PCI DSS 6.3.1]

b. Review custom code prior to release to production or customers in order to identify any potential coding vulnerability. Review shall be performed by someone other than the code author and by someone knowledgeable of code review techniques and secure coding practices; based on secure coding guidelines; and reviewed and approved by management. [PCI DSS 6.3.2]

6.2.2 (P) Change Control Procedures - The BU shall require developers of agency information systems, or system components to follow change control processes and procedures for all changes to system components. The process must ensure: [PCI DSS 6.4, 6.4.5]

a. Ensure separate development/test and production environments; [PCI DSS 6.4.1]
b. Ensure separation of duties between development/test and product environments; [PCI DSS 6.4.2]

c. Ensure production data is not used for testing or development; and [PCI DSS 6.4.3]

d. Ensure removal of test data and accounts before production systems become active. [PCI DSS 6.4.4]

e. Include documentation of the impact [PCI DSS 6.4.5.1]

f. Include documented change approval by authorized parties [PCI DSS 6.4.5.2]

g. Include functionality testing to verify that the change does not adversely impact the security of the system [PCI DSS 6.4.5.3]

h. Include back-out procedure; and [PCI DSS 6.4.5.4]

i. Upon completion of a significant change, all relevant security requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. [PCI DSS 6.4.6]

6.2.3 (P) Secure Coding Guidelines - The BU shall require developers of agency information systems, or system components, to develop applications based on secure coding guidelines to prevent common coding vulnerabilities in software development processes, to include the following: [PCI DSS 6.5]

a. Injection flaws, particularly SQL injection (also consider OS Command Injection, LDAP and XPath injection flaws, as well as other injection flaws); [PCI DSS 6.5.1]

b. Buffer overflow; [PCI DSS 6.5.2]

c. Insecure cryptographic storage; [PCI DSS 6.5.3]

d. Insecure communications; [PCI DSS 6.5.4]

e. Improper error handling; [PCI DSS 6.5.5]

f. All “High” vulnerabilities identified in the vulnerability identification process; and [PCI DSS 6.5.6]

g. For web applications and web application interfaces:
   1. Cross-site scripting (XSS) [PCI DSS 6.5.7]
   2. Improper Access Control (such as direct object references, failure to restrict URL access, and directory traversal) [PCI DSS 6.5.8]
   3. Cross-site request forgery (CSRF) [PCI DSS 6.5.9]
   4. Broken authentication and session management. [PCI DSS 6.5.10]
6.3 Acquisition Process - The BU shall include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: [NIST 800 53 SA-04]

a. Security functional requirements;
b. Security strength requirements;
c. Security assurance requirements;
d. Security-related documentation requirements;
e. Requirements for protecting security-related documentation;
f. Description of the information system development environment and environment in which the system is intended to operate; and
g. Acceptance criteria.

6.3.1 (P) Functional Properties of Security Controls - The BU shall require the developer of the agency information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. [NIST 800 53 SA-04(1)] [IRS Pub 1075]

6.3.2 (P) Design/Implementation Information for Security Controls - The BU shall require the developer of the agency information system, system component, or agency information system service to provide design and implementation information for the security controls to be employed that includes: [NIST 800 53 SA-04(2)] [IRS Pub 1075]

a. Security-relevant external system interfaces; and
b. High-level design.

6.3.3 (P) Services in Use - The BU shall require the developer of the agency information system component, or agency information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use. [NIST 800 53 SA-04(9)] [IRS Pub 1075]

6.4 State Information System Documentation - The BU shall: [NIST 800 53 SA-05]

a. Obtain administrator documentation for the agency information system, system component, or agency information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service
   2. Effective use and maintenance of security functions/mechanisms
3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions

b. Obtain user documentation for the agency information system, system component, or agency information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner
   3. User responsibilities in maintaining the security of the system, component, or service
   4. Protect documentation as required, in accordance with the risk management strategy
   5. Ensure documentation is available to BU-defined personnel or roles

6.5 (P) Security Engineering Principles - The BU shall apply information system security engineering principles in the specification, design, development, implementation, and modification of the agency information system. [NIST 800 53 SA-08] [IRS Pub 1075]

6.6 External Information System Services - The BU shall: [NIST 800 53 SA-09]

   a. Require that providers of external agency information system services comply with organizational information security requirements and employ security controls in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and guidance;

   b. Define and document government oversight and user roles and responsibilities with regard to external information system services; and

   c. Employ Service Level Agreements (SLAs) to monitor security control compliance by external service providers on an ongoing basis. [HIPAA 164.308(b)(1), 164.314(a)(2)(i)]

6.6.1 Identification of Services - The BU shall require providers of external agency information system services to identify the functions, ports, protocols, and other services required for the use of such services. [NIST 800 53 SA-09(2)] [IRS Pub 1075]

6.7 (P) Develop Configuration Management - The BU shall require the developer of the agency information system, system component, or agency information system service to: [NIST 800 53 SA-10] [IRS Pub 1075]

   a. Perform configuration management during system, component, or service (development, implementation, and operation);
b. Document, manage, and control the integrity of changes to configuration items under configuration management;

c. Implement only BU-approved changes to the agency information systems;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes, and;

e. Track security flaws and flaw resolution within the system, component, or service.

6.8 (P) Develop Security Testing and Evaluation - The BU shall require the developer of the agency information system, system component, or agency information system service to:

[NIST 800 53 SA-11] [IRS Pub 1075]

a. Create and implement a security assessment plan that provides for security testing and evaluation, at the depth of security-related functional properties, including:

1. Security-related externally visible interfaces
2. High-level design
3. At the rigor of demonstrating

b. Perform integration and regression testing for components and services and unit, integration, and system testing for systems;

c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

d. Implement a verifiable flaw remediation process; and

e. Correct flaws identified during security testing/evaluation.

6.8.1 (P) Public Web Application Protections - The BU shall require the provider of agency information system service for public-facing web applications to address new threats and vulnerabilities on an ongoing basis and to ensure that these applications are protected against known attacks by either of the following methods: [PCI DSS 6.6]

a. Reviewing public-facing web applications using manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or

b. Installing a web-application firewall in front of public-facing web applications.

6.8.2 (P) Threat and Vulnerability Analyses - The BU shall require the developer of the agency information system, system component, or agency information system service to perform threat and vulnerabilities analyses and subsequent testing/evaluation of the as-built system, component, or service. [NIST 800 53 SA-11(2)] [IRS Pub 1075]
6.8.3 (P) Independent Verification of Assessment Plans / Evidence - The BU shall require an independent agent to verify the correct implementation of the developer security assessment plan and the evidence produced during security testing/evaluation. [NIST 800 53 SA-11(3)] [IRS Pub 1075]

6.8.4 (P) Penetration Testing / Analysis - The BU shall require the developer of the agency information system, system component, or agency information system service to perform penetration testing to include black box testing by skilled security professionals simulating adversary actions and with automated code reviews. [NIST 800 53 SA-11(5)] [IRS Pub 1075] [PCI DSS 11.3.2]

6.9 Establish Operational Procedures – The BU shall ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. [PCI DSS 6.7]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY EXCEPTION PROCEDURE

8.2 STATEWIDE POLICY FRAMEWORK P8130 SYSTEM SECURITY ACQUISITION AND DEVELOPMENT


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


9. ATTACHMENTS

None.
### 10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Update for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8210): SECURITY AWARENESS TRAINING AND EDUCATION

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 8210 SECURITY AWARENESS TRAINING AND EDUCATION.

2. PURPOSE

The purpose of this policy is to ensure all agency employees and contractors are appropriately trained and educated on how to fulfill their information security responsibilities.

3. SCOPE

3.1 Application to Budget Unit (BU) - This policy shall apply to all BUs as defined in ARS § 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.

3.2 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 the mitigation options to improve security.

d. Provide a model for the implementation of security awareness training; and

e. Review and approve BU security training plans.

5.3 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of Information Technology PSPs;

b. Ensure BU compliance with security awareness training and education requirements, including training and education of personnel with significant information security responsibilities; and

c. Promote security awareness training and education efforts within the BU.

5.5 BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of Information Technology PSPs;

b. Ensure security awareness training and educational material is periodically reviewed and updated to reflect changes in requirements, responsibilities, and changes to information security threats, techniques, or other relevant aspects; and

c. Ensure those taking security awareness training and educational program have an effective way to provide feedback.

5.6 BU Information Security Officer (ISO) shall:

a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Information Technology PSPs;

b. Ensure the development of an adequate security awareness training and education program for the BU;

c. Coordinates the security awareness training and education program for BU;

d. Ensure all personnel understand their responsibilities with respect to security awareness training and education; and
e. Stay informed in the security community by establishing contact with selected groups and associations within the security community to facilitate training, and maintain currency with recommended practices, and techniques.

5.7 Supervisors of agency employees and contractors shall:
   a. Ensure users are appropriately trained and educated on their information security responsibilities; and
   b. Monitor employee activities to ensure compliance.

5.8 Users of agency information systems shall:
   a. Familiarize themselves with this policy and related PSPs; and
   b. Adhere to PSPs regarding security awareness training and education.

6. STATEWIDE POLICY

6.1 Security Awareness Program Development - The BU ISO or assigned delegate shall define, document, and develop a security awareness training and education program for the BU. The security training awareness and education program shall include the following elements: [PCI DSS 12.6]

6.1.1 (P) Identify Sensitive Positions - Identification of positions, systems, and applications with significant information security responsibilities and identification of specialized training required to ensure personnel assigned to these positions or having access to these systems and/or applications are appropriately trained. [HIPAA 164.308(a)(5)(i)]

   a. Role-based security training - Security training with appropriate content based on specific information security related assigned roles and responsibilities [NIST 800 53 AT-3 supplemental guidance].

6.1.2 The BU shall provide training to each member of the workforce.

6.1.3 (P-FTI) Security training granted access to SSA-provided information shall include all of the topics listed in 6.2.3.a.

6.1.4 (P-PCI) Payment Card Capture Device Training - For personnel working in areas with payment card data capture devices, the BU shall provide training for personnel to be aware of attempted tampering or replacement of devices. Training shall include: [PCI DSS 9.9, 9.9.3]

   a. verification of identity of third party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices
ARIZONA STATEWIDE INFORMATION SECURITY

STATEWIDE POLICY (8210): Security Awareness Training and Education

6.1.5 Security Topics - Coverage of information security topics and techniques sufficient to ensure trained personnel comply with information security PSPs.

6.1.6 (P) Periodic Security Reminders - Communication with employees and contractors providing updates to relevant information security topics or PSPs. [HIPAA 164.308(a)(5)(ii)(A)]

6.2 Security Awareness Program Operations – The BU ISO or assigned delegate shall operate the security awareness training and education program for the BU. The operations of the security training awareness and education program shall implement the following objectives:

6.2.1 Basic Security Awareness Training - All employees and contractors shall complete security awareness training prior to being granted access to agency information systems, when required by information system changes [NIST 800-53 AT-2 b], and at least annually thereafter. [PCI 12.6.1, NIST 800-53 AT-2 a, c]

6.2.2 (P) Basic Privacy Training - All employees and contractors shall complete privacy awareness training on the policies and procedures with respect to Personally Identifiable Information (PII) prior to being granted access to such data and upon a material change in the policies and procedures. [HIPAA 164.530(b)]

a. (P) Privacy Training – All individuals responsible for handling consumer inquiries about the BU’s privacy practices or the BU’s compliance with privacy regulations shall be informed of all the requirements in these regulations and how to direct consumers to exercise their rights under these regulations.

6.2.3 Specialized Security Awareness Training - All employees and contractors shall receive relevant specialized training within 60 days of being granted access to agency information systems.

a. (P-FTI) The BU shall establish and/or maintain an ongoing function that is responsible for providing security awareness training for employees
granted access to SSA-provided information. Training shall include discussion of:

- The sensitivity of SSA-provided information and address the Privacy Act and other Federal and State laws governing its use and misuse;
- Rules of behavior concerning use of and security in systems processing SSA-provided data;
- Restrictions on viewing and/or copying SSA-provided information;
- The employee’s responsibility for proper use and protection of SSA-provided information including its proper disposal;
- Security incident reporting procedures;
- The possible sanctions and penalties for misuse of SSA-provided information;
- Basic Understanding of procedures to protect the network from malware attacks; and
- Spoofing, phishing and pharming scam prevention.

b. (P-FTI) The BU shall provide security awareness training annually or as needed and have in place administrative procedures for sanctioning employees up to and including termination who violate laws governing the use and misuse of SSA-provided data through unauthorized or unlawful use or disclosure of SSA-provided information.

- Each user is required to sign an electronic version of the ADOA affirmation statement (terms and conditions for use) after reviewing the CBT and their agreement is captured and stored in a database.
- The User Affirmation Statement includes reference to state and federal law and sanctions that include dismissal and/or prosecution.

6.2.4 Security Responsibilities - All employees and contractors shall be trained and educated in their information security responsibilities.

6.2.5 Acceptable Use Rules - All employees and contractors shall understand the acceptable use requirements of the agency information system, available technical assistance, and technical security products and techniques.

6.2.6 Training Material - Information security awareness training and education material shall be developed, available for timely delivery, and generally available to all agency employees and contractors.

6.2.7 Training Delivery - Security awareness training and educational material shall be delivered in an effective manner.
6.3 Security Awareness Program Management and Maintenance - The BU ISO or assigned delegate shall manage and maintain the security awareness training and education program for BU. The security training awareness and education program management and maintenance activities shall include the following elements:

6.3.1 Tracking - Shall have effective tracking of security awareness training and education compliance for all employees and contractors with access to agency information systems which includes periodic refresher training and education. [NIST 800 53 AT-4]

a. Training Records - Training records shall be retained for three years. [NIST 800 53 AT-4 supplemental guidance] However, all State BUs must comply with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to http://apps.azlibrary.gov/records/general_rs/Administrative.pdf Record Series Number and http://apps.azlibrary.gov/records/general_rs/Human%20Resources-Personnel.pdf Record Series Number 20704-20706.

6.3.2 Acknowledgement - All employees or contractors who complete security awareness training and education programs shall acknowledge and accept that they have read and understand the agency information system requirements around information security policy and procedures. [PCI 12.6.2]

6.3.3 Program Updates - The security awareness training and education program shall be periodically reviewed and updated to reflect changes to information security threats, techniques, requirements, responsibilities, and changes to the rules of the system.

6.3.4 Security Groups and Associations – The BU ISO or assigned delegate shall stay informed in the security community by establishing contact with selected groups and associations within the security community to facilitate training, and maintain currency with recommended practices, and techniques. [NIST 800 53 AT-5]

6.3.5 Feedback - The BU ISO shall ensure an appropriate mechanism exists for feedback to the quality and content of the security awareness training and education program.

a. Attendee Review of Security Awareness Training - All employees or contractors who complete security awareness training and educational programs shall have an effective way to provide feedback. Contact information shall be made available to provide feedback at any time.
b. Lessons Learned - Lessons learned from incident response and investigations shall drive improvements to the security awareness training and education program where relevant.

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8210 Security Awareness Training and Education

8.2 Statewide Policy Exception Procedure


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


8.7 General Records Retention Schedule for All Public Bodies, Administrative Records, Schedule Number 000-12-15, Arizona State Library, Archives and Public Records, Item Number 25

8.8 General Records Retention Schedule for All Public Bodies, Human Resources / Personnel Records, Schedule Number GS 1006, Arizona State Library, Archives and Public Records, Item Number 12

9. ATTACHMENTS

None.
## 10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8220): SYSTEM SECURITY MAINTENANCE

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration, 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 8220 SYSTEM SECURITY MAINTENANCE.

2. PURPOSE

The purpose of this policy is to establish the baseline controls for management and maintenance of agency information system controls.

3. SCOPE

3.1 Application to Budget Units - 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 subject matter experts 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 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 Security Maintenance Policy; and

c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 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 Security Maintenance Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 BU Information Security Officer (ISO) shall:

a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Agency Information Technology PSPs;

b. Ensure the development and implementation of an adequate controls enforcing the System Security Maintenance Policy for the BU agency information systems; and

c. Ensure all personnel understand their responsibilities with respect to secure system management and maintenance.

6. STATEWIDE POLICY

6.1 System Configuration Management

6.1.1 Configuration Management Plan - The BU shall develop, document, and implement a configuration management plan for agency information systems that will:

a. Address the roles, responsibilities, and configuration management processes and procedures;
b. Establish a process for identifying configuration items throughout the software development lifecycle and for managing the configuration of the configuration items;

c. Define the configuration items for the agency information system and place the configuration items under configuration management; and

d. Protect the configuration management plan from unauthorized disclosure and modification. [National Institute of Standards and Technology (NIST) 800 53 CM-9]

6.1.2 **Baseline Configuration** - The BU shall develop, document, and maintain a current baseline configuration of each agency information system. [NIST 800 53 CM-2]

a. (P) **Baseline Configuration Reviews and Updates** - The BU shall review and update the baseline configurations for information systems, at least annually, upon significant changes to system functions or architecture, and as an integral part of system installations and upgrades. [NIST 800-53 CM-2 (1)] [Internal Revenue Service (IRS) Pub 1075]

b. (P) **Baseline Configuration Retention** - The BU shall retain at least one previous version of baseline configurations to support rollback. [NIST 800 53 CM-2 (3)] [IRS Pub 1075] However, all State BUs must comply with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to:

c. (P) **Baseline Configuration for High Risk Areas** - The BU shall establish separate baseline configurations for identified high risk areas. [NIST 800-53 CM-2 (7)] [IRS Pub 1075]

6.1.3 (P) **Change Control Board** - The BU shall: [NIST 800 53 CM-3] [IRS Pub 1075]

a. Determine the types of changes to the agency information system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the agency information system and approves or disapproves such changes with explicit consideration for security impact analysis;

c. Document configuration change decisions associated with the agency information system;

d. Implement approved configuration-controlled changes to the information system;

e. Retain activities associated with configuration-controlled changes to the agency information system in compliance with Arizona State Library, Archives and Public Records rules and implement whichever retention
period is most rigorous, binding or exacting. Refer to:  
http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf  Item 8; and

f. Coordinate and provide oversight for configuration control activities through an established configuration control board that convenes at least monthly to review the activities associated with configuration-controlled changes to agency information systems.

6.1.4 Change Approval - The BU shall review and approve/disapprove proposed configuration-controlled changes to the agency information systems. Security impact analysis shall be included as an element of the decision. [NIST 800 53 CM-4]

(P) Test, Validate, and Document Changes - Approved changes shall only be implemented on an operational system after the change control board ensures that the change has been tested, validated, and documented. [NIST 800 53 CM-4 (3)] [IRS Pub 1075]

6.1.5 (P) Change Restriction Enforcement - The BU shall ensure that adequate physical and/or logical controls are in place to enforce restrictions associated with changes to agency information systems. The BU shall permit only qualified and authorized individuals to access agency information systems for the purpose of initiating changes, including upgrades and modifications. [NIST 800 53 CM-5] [IRS Pub 1075]

6.1.6 Configuration Settings - The BU shall: [NIST 800 53 CM-6]

a. Establish and document configuration settings for information technology products employed within the agency information system using Statewide, BU-wide, or agency information specific security configuration checklists that reflect the most restrictive mode consistent with operational requirements;

b. Implement the configuration settings;

c. Identify documents, and approve any deviations from established configuration settings for all information system components for which security checklists have been developed and approved; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

6.1.7 Agency Information System Component Inventory - The BU shall develop and document an inventory of agency information system components (including authorized wireless access points and business justification for those access points) that accurately reflects the current agency information system, is consistent with the defined boundaries of the agency information system, is at the level of granularity deemed necessary for tracking and reporting hardware and software, and includes hardware inventory specifications (e.g., manufacturer, device type,
model, serial number, and physical location), software license information, software version numbers, component owners, and for networked components: machine names and network addresses. [NIST 800 53 CM-8] [PCI DSS 2.4 , 11.1.1]

**Inventory Reviews and Updates** - The BU shall review and update the information system component inventory annually and as an integral part of component installations, removals, and information system updates. [NIST 800 52 CM-8 (1)]

**(P) Inventory Automated Detection** - The BU shall employ automated mechanisms to detect, quarterly, the presence of unauthorized hardware, software, and firmware components within the agency information system and take actions to disable network access, isolate the component, or notify the appropriate BU personnel of the unauthorized component. [NIST 800 53 CM-8 (3)] [IRS Pub 1075]

**(P-PCI) Inventory Payment Card Data Capture Devices** - The BU shall maintain an up-to-date list of devices. The list shall include device make and model, device location, and device serial number (or other method of unique identification). [PCI DSS 9.9, 9.9.1]

**6.1.8 Software Usage Restrictions** - The BU shall use software and associated documentation in accordance with contract agreements and copyright laws; track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. [NIST 800 53 CM-10]

**6.2 Agency Information System Maintenance** - In addition to the change management requirements of Section 6.1, the following requirements apply to the maintenance of agency information systems:

**6.2.1 Controlled Maintenance** - The BU shall: [NIST 800 53 MA-2]

a. Schedule, perform, document, and review records of maintenance and repairs on agency information system components in accordance with manufacturer or vendor specifications and BU requirements;

b. Approve and monitor all maintenance activities whether performed onsite or remotely and whether the equipment is serviced onsite or removed to another location;

c. Explicitly approve the removal of the agency information system or system components from the BU facilities for offsite maintenance or repair;

d. Ensure equipment removed from the BU facilities is properly sanitized prior to removal. (Refer to Media Protection Policy P8250 for appropriate sanitization requirements and methods); and
e. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. These checks are documented in BU maintenance records.

6.2.2 (P) **Maintenance Tools** - The BU shall approve, control, and monitor agency information system maintenance tools. [NIST 800 53 MA-3] [IRS Pub 1075]

(P) **Tool Inspection** - Maintenance tools, and/or diagnostic and test programs carried into a BU facility by maintenance personnel shall be inspected for improper or unauthorized modifications including malicious code prior to the media being used in the agency information system. [NIST 800 53 MA-3(1)(2)] [IRS Pub 1075]

6.2.3 **Remote Maintenance** - The BU shall: [NIST 800 53 MA-4]

a. Approve and monitor remote maintenance and diagnostic activities;

b. Allow the use of remote maintenance and ensure diagnostic tools are consistent with BU policy and documented in the security plan for the agency information system;

c. Employ two-factor authentication for the establishment of remote maintenance and diagnostic sessions;

d. Maintain records for all remote maintenance and diagnostic activities in compliance with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to: http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf Item 3; and

e. Terminate network sessions and connections upon the completion of remote maintenance and diagnostic activities.

(P) **Remote Maintenance Policies and Procedures** - The BU shall document in the security plan for the agency information system the policies and procedures for the installation and use of remote maintenance and diagnostics are documented connections. (See Information Security Program Policy P8120) [NIST 800 53 MA-4(2)] [IRS Pub 1075]

6.2.4 **Maintenance Personnel** - The BU shall: [NIST 800 53 MA-5]

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Ensure non-escorted personnel performing maintenance on agency information systems have required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
6.3 System and Information Integrity [HIPAA 164.132(c),(1)]

6.3.1 Flaw Remediation - The BU shall: [NIST 800 53 SI-2]

a. Identify, report, and correct information system flaws;

b. Test software and firmware updates related to flaw remediation are tested for effectiveness and potential side effects prior to installation;

c. Install security-relevant software and firmware updates and patches within 30 days of release from the vendor; and [PCI DSS 6.2]

d. Incorporate flaw remediation into the organizational configuration management process.

6.3.2 (P) Automated Flaw Remediation System - The BU shall employ an automated mechanism monthly to determine the state of the information system components with regard to flaw remediation. [NIST 800 53 SI-2(2)] [IRS Pub 1075]

6.3.3 Malicious Code Protection - The BU shall: [NIST 800 53 SI-3] [HIPAA 164.308(a)(5)(ii)(B) - Addressable] [PCI DSS 5.1]

a. Employ centrally managed malicious code protection mechanisms at agency information system entry and exit points and all systems commonly affected by malicious software particularly personal computers and servers to detect and eradicate malicious code; [NIST 800 53 SI-3(2)] [PCI DSS 5.1, 5.1.1]

b. For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. [PCI DSS 5.1.2]

c. Update malicious code protection mechanisms automatically whenever new releases are available in accordance with the BU’s configuration management policy and procedures; [NIST 800 53 SI-3(1)]

d. Address the receipt of false positives during malicious code detection and eradication and resulting potential impact on the availability of the agency information system; and

e. Configure malicious code protection mechanisms to:

f. Perform periodic scan of the agency information system weekly and real-time scans of files from external sources at the endpoint, and network entry and exit points as the files are downloaded, opened, or executed; [PCI DSS 5.2]

g. Block and quarantine malicious code and/or send an alert to a system administrator in response to malicious code detection; and

h. Generate audit logs. [PCI DSS 5.2]

i. Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users unless specifically authorized by
management on a case-by-case basis for a limited time period. [PCI DSS 5.3]

6.3.4 Information System Monitoring - The BU shall: [NIST 800 53 SI-4a] [HIPAA 164.308(a)(1)(iii)(D)] [PCI DSS 11.4]

a. Monitor the agency information systems to detect attacks and indicators of potential attacks and unauthorized local, network, and remote connections;

b. Identify unauthorized use of the agency information system through BU-defined intrusion-monitoring tools;

c. Deploy monitoring devices strategically within the agency information system, including at the perimeter and critical points inside the environment to collect essential security-relevant data and to track specific types of transactions of interest to the BU; [PCI DSS 11.4]

d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

e. Heighten the level of monitoring activity within the intrusion monitoring systems whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the agency based on Confidential information;

f. Receive alerts from malicious code protection mechanisms;

g. Receive alerts from intrusion detection or prevention systems;

h. Receive alerts from boundary protection mechanisms such as firewalls, gateways, and routers; and

i. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal and state laws, Executive Orders, directives, policies, or regulations.

6.3.4.1. Updates - All intrusion detection systems and/or prevention engines, baselines, and signatures shall be kept up-to-date. [PCI DSS 11.4]

6.3.4.2. (P) Automated Tools - The BU shall employ automated tools to support near real-time analysis of events. [NIST 800-53 SI-4(2)] [IRS Pub 1075]

6.3.4.3. (P) Inbound and Outbound Traffic - The BU shall monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions. [NIST 800 53 SI-4(4)] [IRS Pub 1075]

6.3.4.4. (P) System Generated Alerts - The BU shall implement the information monitoring system to alert system administrators when the following indications of compromise or potential compromise occur. [NIST 800 53 SI-4(5)] [IRS Pub 1075] [PCI DSS 11.4]
6.3.5 **Security Alerts, Advisories, and Directives** - The BU shall implement a security alert, advisory and directive program to: [NIST 800 53 SI-5]

a. Receive information security alerts, advisories, and directives from Agency and additional services as determined necessary by the BU ISO on an on-going basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to appropriate employees and contractors, other organizations, business partners, supply chain partners, external service providers, and other supporting organizations as deemed necessary; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

6.3.6 **(P) Integrity Verification Tools** - The BU shall employ integrity verification tools to detect unauthorized changes to critical system files, configuration files, or content files. [NIST 800 53 SI-7] [IRS Pub 1075] [HIPAA 164.312(c)(1)] [PCI DSS 11.5]

6.3.6.1 **(P) Integrity Checks** - The BU shall ensure agency information systems will perform integrity checks at least weekly and at start up, the identification of a new threat to which agency information systems are susceptible, and the installation of new hardware, software, or firmware. [NIST 800-53 SI-7(1)] [IRS Pub 1075] [PCI DSS 11.5]

6.3.6.2 **(P) Incident Response Integration** - The BU shall incorporate the detection of unauthorized changes to critical system files into the BU incident response capability. [NIST 800-53 SI-7(7)] [IRS Pub 1075]

6.3.7 **Spam Protection** - The BU shall employ spam protection mechanisms at agency information system entry and exit points to detect and take action on unsolicited messages and updates spam protection mechanisms automatically updated when new releases are available. [NIST 800-53 SI-8, 8(2)] [IRS Pub 1075]

a. **Central Management** - Spam protection mechanisms are centrally managed. [NIST 800-53 SI-8(1)] [IRS Pub 1075]

6.3.8 **(P) Information Input Validation** - The BU shall ensure agency information systems check the validity of information system inputs from untrusted sources, such as user input. [NIST 800-53 SI-10] [IRS Pub 1075]

6.3.9 **Error Handling** - The BU shall ensure the agency information system generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries and reveals error messages only to system administrator roles. [NIST 800-53 SI-11] [IRS Pub 1075]
6.3.10 **Output Handling and Retention** - The BU shall handle and retain information within the agency information system and information output from the system in accordance with applicable federal and state laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. [NIST 800-53 SI-12] [ARS 44-7041] [Arizona State Library Retention Schedules for Information Technology (IT) Records]

6.4 **Establish Operational Procedures** – The BU shall ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. [PCI DSS 5.4]

7. **DEFINITIONS AND ABBREVIATIONS**

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. **REFERENCES**

8.1 STATEWIDE POLICY FRAMEWORK 8220 System Security Maintenance

8.2 Statewide Policy Exception Procedure

8.3 STATEWIDE POLICY FRAMEWORK P8250 Media Protection


8.5 ARS 44-7041

8.6 Arizona State Library Retention Schedules for Information Technology (IT) Records

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


8.10 General Records Retention Schedule for All Public Bodies, Information Technology (IT) Records, Schedule Number: 000-12-41, Arizona State Library, Archives and Public Records, Item Numbers 3 and 8

9. **ATTACHMENTS**
None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State of Arizona CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
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 8230 CONTINGENCY PLANNING.

2. PURPOSE

The purpose of this policy is to minimize the risk of system and service unavailability due to a variety of disruptions by providing effective and efficient solutions to enhance system availability. [NIST 800-34]

3. SCOPE

3.1 Application to Budget Units (BUs) - 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. 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
</table>

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:
   a. Be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state budget units (BUs).

5.2 State Chief Information Security Officer (CISO) shall:
   a. Advise the State CIO on the completeness and adequacy of all state BU activities and documentation provided to ensure compliance with statewide IT 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 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:
   b. Be responsible for the correct and thorough completion of BU PSPs;
c. Identify and convey contingency planning needs;

d. Ensure compliance with BU PSPs; and

e. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 The BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of Agency Information Technology PSPs within the BU;

b. Assign the necessary resources to document, implement, and maintain the contingency plan, including the following roles:

c. Recommend/Ensure continuity plans are documented in the contingency plan;

d. Approve developed and modified contingency plan; and

e. Ensure Contingency Planning Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 BU Information Security Officer (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 Contingency Planning Policy for the BU;

c. Ensure all personnel understand their responsibilities with respect to business continuity and disaster recovery planning; and

d. Work with project leader on security and privacy related issues involving the development, maintenance, or testing of the contingency plan.

5.7 Information System owners shall:

a. Participate in establishing, approving, and maintaining policies for the protection controls applicable to the agency information systems under their control; and

b. Work with the project leader on agency information system related issues involving the development, maintenance, or testing of the contingency plan.

5.8 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on the Contingency Planning Policy; and
b. Monitor employee activities to ensure compliance.

5.9 System Users of agency information systems shall:

a. Become familiar with this policy and related PSPs; and
b. Adhere to PSPs regarding the Contingency Planning Policy.

6. STATEWIDE POLICY

6.1 Develop Contingency Plan – The BU shall develop a contingency plan that: [National Institute of Standards and Technology (NIST) 800-53 CP-2] [Health Insurance Portability and Protection Act (HIPAA) 164.308(a)(7)(i), 164.308(a)(7)(ii)(b), 164.308(a)(7)(ii)(c), 164.310(a)(2)(i)]


b. Provides recovery objectives, restoration priorities, and metrics;

c. Addresses contingency roles, responsibilities, assigned individuals with contact information;

d. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

e. Addresses eventual, full information systems restoration without deterioration of the security safeguards originally planned and implemented;

f. (P) Addresses resumption of essential missions and business functions within a time frame specified by the BU CIO and based on mission needs, applicable regulations, Arizona State Library, Archives and Public Records requirements and applicable contracts and agreements with external BUs or other organizations. [NIST 800-53 CP-2(3)];

g. (P) Identifies critical information system assets supporting organizational missions and business functions; [NIST 800-53 CP-2(8)][HIPAA 164.308(a)(7)(ii)(E)]; and

h. (P) Includes procedures for obtaining necessary electronic protected health information during an emergency [HIPAA 164.312(a)(2)(ii)].

6.2 Manage Contingency Plan - The BU shall: [NIST 800-53 CP-2]

a. Distribute the contingency plan to key contingency personnel and organizational elements;
b. Coordinate contingency planning activities with security incident handling activities;

c. Review the contingency plan annually;

d. Revise the contingency plan to address changes to the organization, agency information systems, operational environment or problems encountered during plan implementation, execution or testing;

e. Communicate contingency plan changes to key contingency personnel and organizational elements; and

f. Protect the contingency plan from unauthorized disclosure and modification.

6.3 (P) Contingency Plan Coordination - The BU shall coordinate the development of the contingency plan for each agency information system with organizational elements responsible for related plans. [NIST 800-53 CP-2(1)]

6.4 Contingency Training - The BU shall provide contingency training to agency information system users consistent with assigned roles and responsibilities before authorizing access, when required by agency information system changes, and annually thereafter. [NIST 800-53 CP-3]

6.5 Test Contingency Plan - The BU shall test the contingency plan for the agency information system annually to determine the effectiveness of the plan and the organizational readiness to execute the plan, review the contingency plan test results, and initiate corrective action. [NIST 800-53 CP-4][HIPAA 164.308 (a)(7)(ii)(D)]

6.5.1 (P) Contingency Plan Test Coordination - The BU shall coordinate contingency plan testing for each agency information system with organizational elements responsible for related plans [NIST 800-53 CP-4(1)] [IRS Pub 1075]

6.6 (P) Alternate Storage Site - The BU shall establish an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information and ensure that the alternative storage site provides information security safeguards equivalent to those of the primary storage site. [NIST 800-53 CP-6]

6.6.1 (P) Separation from Primary Storage Site - The alternative storage site shall be separated from the primary storage site to reduce susceptibility to the same hazards. [NIST 800-53 CP-6(1)] [IRS Pub 1075]

6.6.2 (P) Accessibility - The BU shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. [NIST 800-53 CP-6(3)] [IRS Pub 1075]

6.6.3 Arizona State Library, Archive and Public Records is an alternative site by statute (A.R.S. 41-151.12)
6.7  (P) Alternate Processing Site - The BU shall: [NIST 800-53 CP-7] [IRS Pub 1075]

   a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of agency information system operations for essential missions/business functions with the BU’s defined time period consistent with recovery time and recovery point objectives when the primary process capabilities are unavailable;

   b. Ensure that equipment and supplies to transfer and resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the BU defined period for transfer/resumption; and

   c. Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site.

6.7.1  (P) Separation from Primary Site - The BU shall identify an alternative processing site that is separated from the primary site to reduce susceptibility to the same threats. [NIST 800-53 CP-7(1)] [IRS Pub 1075]

6.7.2  (P) Accessibility - The BU shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. [NIST 800-53 CP-7(2)] [IRS Pub 1075]

6.7.3  (P) Priority of Service - The BU shall develop alternative processing site agreements that contain priority of service provisions in accordance with the organization’s availability requirements. [NIST 800-53 CP-7(3)] [IRS Pub 1075]

6.8  (P) Alternate Telecommunication Site - The BU shall ensure alternate telecommunications services are established including necessary agreements to permit the resumption of agency information system operations for essential missions and business functions within the BU’s defined time period when the primary telecommunication capabilities are unavailable at either the primary or alternate processing or storage sites. [NIST 800-53 CP-8] [IRS Pub 1075]

6.8.1  (P) Priority of Service Provisions - The BU shall ensure primary and alternate telecommunications service agreements are developed that contain priority-of-service provisions in accordance with the BU’s availability requirements and requests telecommunication service priority for all telecommunications services used for national or state security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. [NIST 800-53 CP-8 (1)] [IRS Pub 1075]

6.8.2  (P) Single Points of Failure - The BU shall ensure alternate telecommunications services are obtained, with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunication services. [NIST 800-53 CP-8(2)] [IRS Pub 1075]
6.9 Agency Information System Backup - The BU shall: [NIST 800-53 CP-9] [HIPAA 164.308(7)(ii)(A)]

a. Conduct backups of user-level and system-level information contained in the agency information system, and agency information system documentation including security-related documentation within the BU’s defined frequency consistent with recovery time and recovery point objectives; and

b. Protect the confidentiality, integrity, and availability of the backup information at storage locations.

6.9.1 (P) Testing for Reliability/Integrity - The BU shall test backup information at least annually to verify media reliability and information integrity. [NIST 800-53 CP-9(1)] [IRS Pub 1075]

6.10 Information System Recovery and Reconstitution - The BU shall provide for the recovery and reconstitution of the agency information system to a known state after a disruption, compromise, or failure. [NIST 800-53 CP-10]

6.10.1 (P) Transaction Recovery - The BU shall implement agency information systems to perform transaction recovery for any system that is transaction-based. [NIST 800-53 CP-10(2)] [IRS Pub 1075]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8230 Contingency Planning

8.2 Statewide Policy Exception Procedure


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


8.6 Establishing an Essential Records List, Arizona State Library, Archives and Public Records
8.7 General Records Retention Schedule Issued to All Public Bodies, Management Records, Schedule Number: GS 1005, Arizona State Library, Archives and Public Records, Item Number 7

8.8 A.R.S. 41-151.12

9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8240): INCIDENT RESPONSE PLANNING

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 8240 INCIDENT RESPONSE PLANNING.

2. PURPOSE

The purpose of this policy is to increase the ability of the Budget Unit (BU) to rapidly detect incidents, minimize any loss due to destruction, mitigate the weaknesses that were exploited, and restore computing services.

3. SCOPE

3.1 Application to Budget Units (BUs) - 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:
   a. Be ultimately responsible for the correct and thorough completion of Statewide 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 all state BU activities and documentation provided to ensure compliance with statewide IT PSPs throughout all state BUs;
b. Review and approve or disapprove all state BU security and privacy PSPs and exceptions to existing 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 State Chief Privacy Officer (CPO) shall:

a. Advise the State CIO and the State CISO on the completeness and adequacy of the BU activities and documentation for data privacy provided to ensure compliance with Statewide Information Technology Privacy PSPs throughout all state BUs;  
b. Review and approve BU privacy PSPs and requested exceptions from the statewide privacy PSPs; and  
c. Identify and convey to the State CIO and the State CISO the privacy risk to state information systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

5.4 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.5 BU Director shall:

a. Be responsible for the correct and thorough completion of Agency BU PSPs;  
b. Ensure compliance with BU PSPs with Incident Response Planning Policy; and  
c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.6 BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of BU IT PSPs; and  
b. Ensure BU PSPs are periodically reviewed and updated to reflect changes in requirements, lessons learned from actual incidents, and advances the industry.

5.7 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 Incident Response Planning Policy for the BU; and
c. Ensure all personnel understand their responsibilities with respect to planning and responding to security incidents.

5.8 BU Privacy Officer shall: [EO 2008-10]

a. Advise the State CISO and the State CPO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with privacy laws, regulations, and statutes; and
b. Assist the agency to ensure the privacy of sensitive personal information within the agency’s possession.

5.9 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Incident Response Planning Policy; and
b. Monitor employee activities to ensure compliance.

5.10 System Users of agency information systems shall:

a. Become familiar with this policy and related PSPs; and
b. Adhere to PSPs regarding classification of incidents response planning within agency information systems.

6. STATEWIDE POLICY

6.1 Incident Response Training - The BU shall provide incident response training to agency information system users consistent with assigned roles and responsibilities before authorizing access to the agency information system or performing assigned duties, when required by agency information system changes, and annually thereafter. [NIST 800-53 IR-2] [IRS Pub 1075] [PCI DSS 12.10.4]

6.2 (P) Incident Response Testing – The BU shall test the incident response capability for the agency information system annually using checklists, walk-through, tabletop exercises, simulations or comprehensive exercises to determine the incident response effectiveness and document the results. [NIST 800-53 IR-3] [IRS Pub 1075] [PCI DSS 12.10.2]

6.2.1 (P) Coordinated Testing – The BU shall coordinate incident response testing with BU elements responsible for related plans. [NIST 800-53 IR-3(2)] [IRS Pub 1075]
6.2.2 (P) Incident Response Test Elements – The BU shall include the following elements (at a minimum) in the annual incident response test: [PCI DSS 12.10.2]

a. Incident response roles and responsibilities, communications, and contact strategies
b. Specific incident response procedures
c. Business recovery and continuity procedures
d. Data back-up processes
e. Legal requirement and breach notification analysis
f. Critical system component coverage and responses
g. Reference or inclusion of Incident response procedures from external entities

6.3 Incident Handling - The BU shall implement an incident handling capability for security incidents that includes: [NIST 800-53 IR-4] [IRS Pub 1075] [HIPAA 164.308(a)(6)(ii)] [PCI DSS 12.10.1]

a. Preparation, detection and analysis, containment, eradication, and recovery;
b. Incident handling activities with contingency planning activities; These activities shall address the following at a minimum:
   1. Unauthorized wireless access point detection [PCI DSS 11.1.2]
   2. Alerts generated by change detection solutions (e.g., unauthorized modification of critical files, configuration files or content files) [PCI DSS 11.5.1]
   c. Incident response procedures, training, and testing/exercises covering industry developments and lessons learned from ongoing incident handling activities that drive the modification and evolution of the incident response plan; [PCI 12.10.6]
   d. Industry developments; and
e. Implementation of industry development changes where applicable.

6.3.1 (P) Automated Incident Handling Processes - The BU shall employ automated mechanisms to support the incident handling process. [NIST 800-53 IR-4(1)] [IRS Pub 1075]

6.3.2 (P) Assign Incident Handling Role - The BU shall assign to an individual or team the information security management responsibility of implementing an incident
response plan and to be prepared to respond immediately to a system breach. [PCI DSS 12.10.1]

6.3.3 (P-PCI) **24x7 Availability** - The BU shall assign to specific personnel the information security management responsibility of being available on a 24x7 basis to respond to alerts. [PCI DSS 12.10.3]

6.3.4 (P) **Forensic Capability** - For agencies that provide a shared hosting service, the BU shall establish processes to provide for timely forensic investigation in the event of a compromise to any hosted service. [PCI DSS A.1.3]

6.4 (P) **Privacy Incident Response Handling** – The BU shall provide an organized and effective response to privacy incidents in accordance with the BU Privacy Incident Response Plan. [NIST 800-53 SE-2]

6.5 **Incident Monitoring** - The BU shall track and document agency information system security incidents. [NIST 800-53 IR-5] [IRS Pub 1075] [HIPAA 164.308(a)(6)(ii)]

6.5.1 (P) **Assign Incident Monitoring Role** - The BU shall assign to an individual or team the information security management responsibility of monitoring and analyzing security alerts and information and distributing alerts to appropriate personnel. [PCI DSS 12.5.2]

6.5.2 (P) **Incorporate Automated Alerts** - The BU shall implement the system to include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems. [PCI DSS 12.10.5]

6.6 **Incident Reporting** - The BU shall require personnel to report: [NIST 800-53 IR-6] [ARS 41-3507] [IRS Pub 1075] [EO 2008-10] [HIPAA 164.308(a)(6)(ii)] [HIPAA 164.314(a)(2)(i)(C)]

a. Suspected security incidents to the organizational incident response capability within one hour of knowledge of suspected incident as specified in the Statewide Standard 8240, Incident Response Planning:

b. (In the event of a security incident) Security incident information to the State CISO; and

c. (In the event of a privacy incident) Privacy incident information to the State Privacy Officer. See requirement 6.9.2: Privacy Incident Response Plan.

6.6.1 **Use of Statewide Incident Handling Program** – BUs utilizing the statewide incident handling program meet the requirement for reporting of security and privacy incidents that are visible within the program (e.g., part of the monitored systems and logs). However, BUs must implement a system to integrate the notification process for security incidents that originate outside of the monitored systems (e.g.,
employee reported malware, onsite physical threats, reported loss of laptop). [ARS 41-2507]

6.6.2 (P) Automated Incident Reporting - The BU shall employ automated mechanisms to assist in the reporting of security incidents. [NIST 800-53 IR-6(1) | IRS Pub 1075]

6.7 Incident Response Plan - The BU shall: [NIST 800-53 IR-8] [IRS Pub 1075] [PCI DSS 12.10, 12.10.1]

   a. Develop an incident response plan that:
      1. Provides the organization with a roadmap for implementing its incident response capability;
      2. Describes the structure and organization of the incident response capability;
      3. Provides a high-level approach for how the incident response capability fits into the overall organization;
      4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
      5. Defines reportable incidents;
      6. Provides metrics for measuring the incident response capability within the organization;
      7. Defines the resources and management support needed to effectively maintain and manage an incident response capability;
      8. (P-PCI) Describes the roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, specific incident response procedures, business recovery and continuity procedures, data backup processes, analysis of legal requirements for reporting compromises, coverage and responses of all critical system components, and reference or inclusion of incident response procedures from the payment brands. [PCI DSS 12.10.1]; and
      9. Is reviewed and approved by the BU Information Security Officer.
     10. Distribute copies of the incident response plan to incident response personnel and organizational elements;
     11. Review the incident response plan annually;
     12. Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
     13. Communicate incident response plan changes to Agency BU incident response personnel and the State CISO and State Privacy Officer.

6.8 Incident Response Assistance - The BU shall provide an incident response support resource, integral to the BU incident response capability that offers advice and assistance
to users of the information system for the handling and reporting of security incidents. [NIST 800-53 IR-7] [IRS Pub 1075]

6.8.1 (P) Automated Support for Availability of Information - The BU shall employ automated mechanisms to increase the availability of incident response-related information and support. [NIST 800-53 IR-7(1)] [IRS Pub 1075]

6.9 (P) Privacy Incident Response Plan - The BU shall develop and implement a Privacy Incident Response Plan. [NIST 800-53 SE-2]

6.9.1 Investigation - The BU shall promptly investigate potential privacy incidents upon awareness of unencrypted Personally Identifiable Information (PII) loss. [ARS 18-552.A]

   a. Breach Determination – The investigation shall determine if the security incident resulted in a system security breach. [ARS 18-552.A]

   b. Determination of No Substantial Economic Loss – If an independent third-party forensic auditor or law enforcement agency performed a reasonable investigation and has determined that the system breach has not resulted in or in not reasonably likely to result in substantial economic loss to affected individuals the BU is not required to make the notification as described below. [ARS 18-552.J]

6.9.2 Notification – The BU shall notify affected parties upon breach determination within 45 days after the determination. [ARS 18-551.B, 18-551.H][HIPAA 164.404(a)]

   a. Non-state Owned PII Notification - For PII not owned by the state, the BU shall notify and cooperate with the owner following the discovery of a breach as soon as practicable, including sharing information relevant to the breach. [ARS 18-552.C]

   b. Notification Exceptions - The BU may delay or potentially forgo notification in the following cases:

      1. if law enforcement determines notification will impede the investigation. The required notification shall be implemented within 45 days of being informed by law enforcement that notifications no would longer impede the investigation, [ARS 18-552.D] [HIPAA 164.412]

      2. Good Faith Exposure – No notification is required in the event the disclosure was unintentional or inadvertent by a workforce member acting in good faith and there is no further disclosure. [HIPAA 164.402.1.i-ii]
3. No Retention – No notification is required in the event the disclosure is to an unauthorized person but it is believed that there is no reasonable way for that person to retain the information. [HIPAA 164.402.1.iii]

4. Low Probability of Compromise – No notification is required in the event the disclosure is demonstrated to have a low probability of compromise based on a risk assessment that considers at least the following factors: [HIPAA 164.402.2]
   i. The nature and extent of the PHI involved (including identifier types, and likelihood of re-identification)
   ii. The unauthorized person to whom the PHI was exposed
   iii. Whether the PHI was actually acquired or viewed; and
   iv. The extent to which the risk to the PHI has been mitigated.

5. If the BU determines a Low Probability of Compromise the determination must be supported through a documented risk analysis process. See Attachment for Example Harm Analysis]

c. Notification Methods - The BU may use written notice via mail, telephone (but not through a prerecorded message), or email as a method of notification. [ARS 18-552.F]
   1. If the cost of notification via these methods would exceed $50,000 the notification method may be a written letter to the attorney general that demonstrates the facts necessary for substitute notice, and a conspicuous posting of the notice for at least 435 days on the BU website. [ARS 18-552.F.4]
   2. If the breach involves account login information (e.g., username and password or security questions) and not any other personal information, the notification may an electronic message that directs the user to re-secure the account (and all other accounts using the same password or security question) by changing the password and security question(s). [ARS 18-551.G]
   3. If the breach involves account login information with an email account the notification may be directed to the individual using a method other than the suspect email address:
i. Notification delivered online when the IP address or online location matches a known customary address or location for that account. [ARS 18-551.G]

d. (P-PHI) Notification Timing – The BU shall implement notifications without unreasonable delay and in no case later than 45 days after discovery of a breach or suspected breach of PHI. [ARS 18-552.B], [HIPAA 164.404(b), 164.406(b)]

e. Notification Elements – The notification shall include the following elements: [ARS 18-552.E]

1. Approximate date of breach
2. Brief description of personal information included in the breach
3. Toll-free numbers and addresses for the 3 largest nationwide consumer reporting agencies
4. Toll-free number, address and website address for the federal trade commission or any federal agency that assists consumers with identity theft matters.

f. (P-PHI) Additional Notifications – For a breach of unsecured PHI the following additional notifications must be implemented:

1. Breach Log - For breaches involving less than 500 residents of a State or jurisdiction the BU shall maintain a log of such breaches. [HIPAA 164.408(c)].

2. Media Notification - For PHI breaches involving more than 500 residents of a State or jurisdiction the BU shall notify prominent media outlets serving the State or jurisdiction. [HIPAA 164.406(a)].

3. (P-PII) Media Notification – For PII breaches involving more than 1000 individuals notify the 3 largest nationwide consumer-reporting agencies and the attorney general with a copy of the notification provided to the individuals. [A.R.S. 18-552.B.2]

4. HHS Secretary Notification – For any PHI breach the BU shall notify the Secretary of Health and Human Services. In addition each year the BU shall notify the HHS Secretary of the logged data of PHI breaches in the manner specified on the HHS website. [HIPAA 164.408(a), 164.408(b), 164.408(c)].

g. (P) Federal Regulators – A BU is compliant with the notification requirements if they are compliant with the notification requirements
established by their primary or functional federal regulator. [ARS 18-552.I]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8240 Incident Response Planning
8.2 Statewide Standard 8240, Incident Response Planning
8.3 Statewide Policy Exception Procedure
8.4 Incident Handling Program
8.6 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006
8.7 HIPAA HITECH (Health Information Technology for Economic and Clinical Health) Act February 17, 2010.

9. ATTACHMENTS

Example Risk of Harm Analysis Procedure:
https://aset.az.gov/resources/policies-standards-and-procedures

Effective: May 26, 2021
## REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8250): MEDIA PROTECTION

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the BU 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 P8250 MEDIA PROTECTION.

2. PURPOSE

The purpose of this policy is to increase the ability of the Budget Unit (BU) to ensure the secure storage, transport, and destruction of sensitive information.

3. SCOPE

3.1 Application to Budget Units (BUs) - 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, Agency 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.  ROLES AND RESPONSIBILITIES

5.1  State Chief Information Officer (CIO) shall:

a.  Be ultimately responsible for the correct and thorough completion of Statewide Information Technology (IT) PSPs throughout all state budget units (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 IT 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 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:
   a. Be responsible for the correct and thorough completion of Information Technology PSPs within the BU;
   b. Ensure BU compliance with Media Protection Policy; and
   c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 BU CIO shall:
   a. Work with the BU Director to ensure the correct and thorough completion of BU Information Technology PSPs; and
   b. Ensure Media Protection PSPs are periodically reviewed and updated.

5.6 BU Information Security Officer (ISO) shall:
   a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with IT PSPs;
   b. Ensure the development and implementation of an adequate controls enforcing Media Protection PSPs for the BU;
   c. Request changes and/or exceptions to existing Media Protection PSPs from the State CISO; and
   d. Ensure all personnel understand their responsibilities with respect to protection of removable media in connection with agency information systems and premises.

5.7 Supervisors of agency employees and contractors shall:
   a. Ensure users are appropriately trained and educated on Media Protection Policies; and
   b. Monitor employee activities to ensure compliance.

5.8 Users of agency information systems shall:
   a. Familiarize themselves with this policy and related PSPs; and
   b. Adhere to PSPs regarding protection of removable media in connection with agency information systems and premises.
6. STATEWIDE POLICY

6.1 Media Access - The BU shall restrict access to digital and non-digital media to authorized individuals. [NIST 800-53 MP-2] [HIPAA 164.308(a)(3)(ii)(A)] [PCI DSS 9.6] [IRS Pub 1075]

6.2 (P) Media Marking - The BU shall mark, in accordance with BU policies and procedures, information system digital and non-digital media containing Confidential information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information, as well as exempt removable digital media from marking as long as the exempted items remain with a controlled environment. [NIST 800-53 MP-3] [PCI DSS 9.6.1] [IRS Pub 1075]

6.3 (P) Media Storage - The BU shall physically control and securely store digital and non-digital media containing Confidential information within controlled areas. [NIST 800-53 MP-4] [ARS 39-101] [PCI DSS 9.5] [PCI DSS 9.7] [IRS Pub 1075]

6.4 (P) Media Inventories - The BU shall maintain inventory logs of all digital media containing Confidential information and conduct inventories annually. [PCI DSS 9.7.1]

6.5 (P) Media Transport – The BU shall protect and control digital and non-digital media containing Confidential information during transport outside controlled areas. [NIST 800-53 MP-5] [PCI DSS 9.6] [IRS Pub 1075]

6.5.1 (P) Cryptographic Protection - The BU shall employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside controlled areas. Cryptographic mechanisms must comply with System and Communication Protection Standard S8350. [NIST 800-53 MP-5(4)] [HIPAA 164.312(c)(2)] [IRS Pub 1075]

6.5.2 (P) Secure Delivery - The BU shall send confidential digital and non-digital media by secured courier or other delivery method. [PCI DSS 9.6.2]

6.5.3 (P-HIPAA) Record of Movement - The BU shall maintain a record, including the person(s) responsible, of the movements of hardware and digital media. [HIPAA 164.310(d)(2)(iii)]

6.5.3.1 (P) Data Backup - The BU shall create a retrievable, exact copy of Confidential data, when needed before movement of equipment. [HIPAA 164.310(d)(2)(iv)]

6.5.3.2 (P) Backup Storage - The BU shall store digital media backups in a secure location and review the location’s security, at least annually. [PCI DSS 9.5.1]

6.5.4 (P) Management Approval - The BU shall ensure management approves any media that is moved from a controlled area. [PCI DSS 9.6.3]
6.6 **Media Sanitization** - The BU shall sanitize digital and non-digital information system media containing Confidential information prior to disposal, release of organizational control, or release for reuse using defined sanitization techniques and procedures in accordance with the Media Protection Standard S8250. [NIST 800-53 MP-6] [HIPAA 164.310(d)(2)(i)] [HIPAA 164.310(d)(2)(ii)] [IRS Pub 1075] [PCI DSS 9.8, 9.8.1, 9.8.2]

6.6.1 **Secure Storage** - Secure storage containers used for materials that are to be destroyed. [PCI DSS 9.8.1]

6.7 **Media Use** – The BU shall restrict the use of [BU-specified type of digital media] on [BU-specified agency information systems and/or system components]. [NIST 800-53 MP-7] [IRS Pub 1075]

6.7.1 (P) **BU Restrictions** - The BU shall employ PSPs on the use of removable media in BU agency information systems. [NIST 800-53 MP-7(1)] [HIPAA 164.310(d)(1)]

6.7.2 (P) **Prohibition of Use without Known Owner** - The BU shall prohibit the use of removable media in BU agency information systems when the media has no identifiable owner. [NIST 800-53 MP-7(2)] [IRS Pub 1075]

7. **DEFINITIONS AND ABBREVIATIONS**

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. **REFERENCES**

8.1 STATEWIDE POLICY FRAMEWORK P8250 Media Protection

8.2 Statewide Policy Exception Procedure

8.3 Statewide Standard S8250, Media Protection

8.4 System and Communication Protection, Standard S8350


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


9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2017</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8260): PHYSICAL SECURITY PROTECTIONS

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 as authorized by Arizona Revised Statutes (A.R.S.) § 18-104 and § 18-105. REFERENCE STATEWIDE POLICY FRAMEWORK P8260 PHYSICAL PROTECTIONS.

2. PURPOSE

The purpose of this policy is to protect agency information systems and assets through limiting and controlling physical access and implementing controls to protect the environment in which agency information systems and assets are housed.

3. SCOPE

3.1 Application to Budget Units (BUs) - 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:
   a. Be ultimately responsible for the correct and thorough completion of Statewide Information Technology (IT) Policies, Standards and Procedures (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 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of Information Technology PSPs within the Agency BU;

b. Ensure BU compliance with Physical Protections Policy; and

c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 BU 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 Physical Security Controls Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 BU Information Security Officer (ISO) shall:

a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Agency Information Technology PSPs;

b. Ensure the development and implementation of an adequate controls enforcing the Physical Protections Policy for the BU; and

c. Ensure all personnel understand their responsibilities with respect to the physical protection of agency information systems and assets.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Physical Protections Policies; and

b. Monitor employee activities to ensure compliance.

5.8 Users of agency information systems shall:

a. Familiarize themselves with this policy and related PSPs; and
b. Adhere to PSPs regarding the physical protection of agency information systems and assets.

6. STATEWIDE POLICY

6.1 Physical Access Authorizations - The BU shall: [NIST 800-53 PE-2] [IRS Pub 1075] [HIPAA 164.310 (a)(2)(iii)] [PCI DSS 9.9, 9.3]

a. Develop and maintain a list of individuals with authorized access to controlled areas or facilities where the agency information system resides;

b. Issue authorization credentials based on job function; [PCI DSS 9.3]
c. Review and approve the access list and authorization credentials quarterly; and

d. Remove individuals access (including from the access list, keys, badges, and combination changes) when access is no longer required and immediately upon termination. [PCI DSS 9.3]

6.2 Standard Physical Access Control - The BU shall: [NIST 800-53 PE-3] [IRS Pub 1075] [AAC 2-10] [HIPAA 164.310(a)(1), (a)(2)(ii)]

a. Enforce physical access authorization at designated entry/exit points to the facility where the agency information system resides; [PCI DSS 9.1]

b. Verify individual access authorizations before granting access to the facility; [PCI DSS 9.1, 9.3.1]

c. Control ingress/egress to the facility using keys, locks, combinations, card readers, and/or guards; and

(d. (P-PCI) Provide cameras, monitoring by guards, or isolating selected agency information system components (or any combination) to control access to areas within the facility officially designated as publically accessible. Review collected data and correlate with other entries. Store at least three (3) months unless otherwise directed by law. [PCI DSS 9.1.1]

6.3 Protected Physical Access Control - For all Protected agency information systems and the server components of standard agency information systems for which additional physical protections apply, the BU shall: [NIST 800-53 PE-3] [IRS Pub 1075] [AAC 2-10] [HIPAA 164.310(a)(1), (a)(2)(ii)]

a. (P) Develop procedures to identify and authorize visitors [PCI DSS 9.4]

b. (P) Develop procedures to easily distinguish between onsite personnel and visitors. [PCI DSS 9.2];
c. (P) Give visitors a physical token that expires and that identifies the visitors as onsite personnel and ensure the visitor surrenders the physical token before leaving the facility or at the date of expiration; \[PCI DSS 9.4.2, 9.4.3.\]
d. Escort visitors and monitors visitor activity within controlled areas; \[PCI DSS 9.4.1\]
e. Secure keys, combinations, and other physical access devices;
f. Inventory keys and other physical access devices every quarter; keys and other physical access devices assigned to visitors are inventoried every day; and
g. Change combinations annually and combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or separated.

6.4 Monitoring Physical Access - The BU shall: \[NIST 800-53 PE-6\] \[IRS Pub 1075\]

a. Monitor physical access to the agency information system to detect and respond to physical security incidents;
b. (P) Use video cameras and/or access control mechanisms (or both) to monitor physical access to sensitive areas. \[PCI DSS 9.1.1\]
c. (P) Review physical access logs weekly and, upon occurrence of potential indications of events; \[PCI 9.1.1\]
d. (P) Coordinate results of reviews and investigations with the organizational incident response capability; and
e. (P) Store physical access monitoring data for at least three months. \[PCI 9.1.1\]

6.4.1 (P) Intrusion Alarms/Surveillance Equipment - The BU shall monitor real-time physical intrusion alarms and surveillance equipment. \[NIST 800-53 PE-6(1)\] \[IRS Pub 1075\]

6.4.2 (P-PCI) Inspect Payment Card Capture Devices - Periodically inspect device surfaces to detect tampering or substitution (for example, addition of card skimmers to devices, unexpected attachments or cables plugged into the device, missing, changed security labels, different colored casing, or changes to the serial number or other external markings). \[PCI 9.9.2\]

6.5 Visitor Control Records - The BU shall: \[PCI DSS 9.4.4\]

a. Maintain visitor access records to the controlled areas or facilities where the information system resides;
b. Review visitor access records monthly; \[NIST 800-53 PE-8\]
c. Maintain a visitor log that includes the visitor’s name, the firm represented, and the onsite personnel authorizing physical access; and

d. The logs shall be retained for a minimum of three months. [PCI 9.1.1]

6.6  (P) Access Control - The BU shall implement the following physical access controls:

6.6.1  (P) Transmission Medium - The BU shall control physical access to agency information system distribution and transmission lines within BU facilities using locked wiring closets; disconnected or locked spare jacks; and/or protection of cabling by conduit or cable trays. [NIST 800-53 PE-4] [IRS Pub 1075]

6.6.2  (P) Workstations - The BU shall implement physical safeguards for all workstations that access sensitive information to restrict access to authorized users. [HIPAA 164.310(b), 164.310(c)]

6.6.3  (P) Output Devices - The BU shall control physical access to agency information system output devices to prevent unauthorized individuals from obtaining output. [NIST 800-53 PE-5] [IRS Pub 1075]

6.6.4  (P-PCI) Network Jacks and Devices - The BU shall restrict physical access to publicly accessible network jacks, wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. [PCI 9.1.2, 9.1.3]

6.6.5  (P) Power Equipment and Cabling - The BU shall protect power equipment and power cabling for the agency information system from damage and destruction. [NIST 800-53 PE-9]

6.7  (P) Power - The BU shall implement the following physical controls for power:

6.7.1  (P) Emergency Shutoff - The BU shall: [NIST 800-53 PE-10]

   a. Provide the capability of shutting off power to the agency information system or individual system components in emergency situations;

   b. Place emergency shutoff switches or devices in data centers, server rooms, and computer rooms to facilitate safe and easy access for personnel; and

   c. Protect emergency power shut off capability from unauthorized activation.

6.7.2  (P) Emergency Power - The BU shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or a transition of the information system to long-term alternate power in the event of a primary power source loss. [NIST 800-53 PE-11]
6.8 **Emergency Lighting** - The BU shall employ and maintain automatic emergency lighting for the agency information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. [NIST 800-53 PE-12]

6.9 **Fire Protection** - The BU shall employ and maintain fire suppression and detection devices/systems for the agency information system that are supported by an independent energy source. [NIST 800-53 PE-13]

6.9.1 *(P) Detection Devices* - The BU shall employ fire detection devices/systems for the agency information system that activate automatically and notify the BU and emergency responders in the event of a fire. [NIST 800-53 PE-13(1)]

6.9.2 *(P) Suppression Devices* - The BU shall employ fire suppression devices/systems for the agency information system that provides automatic notification of any activation to the BU and emergency responders. [NIST 800-53 PE-13(2)]

6.9.3 *(P) Inspections* - The BU shall ensure the facility undergoes annual inspections by authorized and qualified inspectors and resolves identified deficiencies within 30 days. [NIST 800-53 PE-13(3)]

6.10 **Temperature and Humidity Controls** - The BU shall maintain defined temperature and humidity levels within the facility where the agency information system resides at data centers, server rooms and computer rooms; and monitors temperature and humidity levels daily. [NIST 800-53 PE-14]

6.11 **Water Damage Protection** - The BU shall protect agency information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. [NIST 800-53 PE-15]

6.12 **Delivery and Removal** - The BU shall authorize, monitor, and control agency information systems components entering and exiting the facility and maintains records of those items. [NIST 800-53 PE-16]

6.13 *(P) Alternate Work Site* - The BU shall: [NIST 800-53 PE-17]

   a. Define and employ minimum security controls at alternate work sites;

   b. Assess, as feasible, the effectiveness of security controls at alternate work sites; and

   c. Provide a means for employees to communicate with agency information security personnel in case of security incidents or problems.

6.14 *(P) Develop Operational Procedures* - The BU shall ensure that security policies and operational procedures for restricting physical access are documented, in use, and known to all affected parties [PCI DSS 9.10]
7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK P8260 Physical Protections
8.2 Statewide Policy Exception Procedure
8.4 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
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 P8270 PERSONNEL SECURITY CONTROLS.

2. PURPOSE

The purpose of this policy is to increase the ability of the Budget Unit (BU) to protect agency information systems and assets containing sensitive data through personnel security controls.

3. SCOPE

3.1 Application to Budget Units (BUs) - 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 - 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 - 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of Statewide 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 all state BU activities and documentation provided to ensure compliance with statewide IT PSPs throughout all state BUs;

b. Review and approve all state BU security and privacy PSPs;
c. Request exceptions from the statewide security and privacy PSPs; and

d. 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 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 Budget Unit (BU) Director shall:

b. Be responsible for the correct and thorough completion of BU PSPs;

c. Ensure compliance with BU PSPs; and

d. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 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 PSPs are periodically reviewed and updated to reflect changes in requirements.

5.6 The BU Information Security Officer (ISO) shall:

a. Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with Statewide IT PSPs;

b. Ensure the development and implementation of an adequate controls enforcing the Personnel Security Policy for the BU;

c. Ensure all personnel understand their responsibilities with respect to the protection of agency information systems and assets through personnel security controls.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on Personnel Security Policies; and

b. Monitor employee activities to ensure compliance.

5.8 Users of agency information systems shall:

a. Familiarize themselves with this and related PSPs; and
b. Adhere to PSPs regarding the protection of agency information systems and assets through personnel security controls.

6. STATEWIDE POLICY

6.1 Position Categorization - The BU shall:

a. Assign a sensitivity designation (e.g., Sensitive, Non-Sensitive) to all positions;

b. Establish screening criteria for individuals filling those positions; and

c. Review and revise position sensitivity designations annually. Sensitivity designations are based on the individual’s exposure to sensitive system information and/or administrative privileges to agency information systems. Examples of sensitive positions include: [NIST 800-53 PS-02] [IRS Pub 1075]

1. Firewall administrator

2. Members of the incident response team

3. Those with vulnerability scanning duties

6.2 Position Definition - The BU shall define information security responsibilities for all personnel. [HIPAA(a)(3)(ii)(A), (a)(3)(ii)(B) - Addressable] [PCI DSS 12.4, 12.5]. Specifically, the following information security responsibilities:

a. Individual or team responsible for establishing, documenting, and distributing security policies and procedures; [PCI DSS 12.5.1]

b. Individual or team responsible for monitoring and analyzing security alerts and information, and distributing to appropriate employees and contractors; [PCI DSS 12.5.2]

c. Individual or team responsible for establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations; [PCI DSS 12.5.3]

d. Individual or team responsible for administering user accounts, including additions, deletions, and modifications; and [PCI DSS 12.5.4]

e. Individual or team responsible for monitoring and controlling all access to data. [PCI DSS 12.5.5]

6.3 Personnel Screening - The BU shall screen individuals holding positions designated as sensitive prior to hiring or contracting; and rescreens individuals according to re-screening every three years. [NIST 800-53 PS-03] [IRS Pub 1075] [PCI DSS 12.7]
6.4 **Personnel Separation** - Upon separation of individual employment, the BU shall: [NIST 800-53 PS-04] [HIPAA(a)(3)(ii)(C)]
   
   a. Terminate agency information system access within 24 hours;
   
   b. Conduct exit interviews, if employee is available for interview;
   
   c. Retrieve all security-related agency information system-related property;
   
   d. Retain access to agency information system accounts formerly controlled by separated individual; and
   
   e. Allow the separated individual access to authorized services such as benefits, reimbursement, and retirement information, according to BU or State policies.

6.5 **Personnel Transfer** - The BU shall: [NIST 800-53 PS-05] [IRS Pub 1075]
   
   a. Review logical and physical access authorization to agency information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates returning old and reissuing new keys, identification cards, and building passes;
   
   b. Close previous information system accounts and establish new accounts;
   
   c. Change agency information system access authorizations;
   
   d. Provide access to official records to which the employee had access at the previous work location and in the previous agency information system accounts within 24 hours; and
   
   e. The BU may extend limited access for special purposes on an exception basis.

6.6 **Access Agreements** - The BU shall ensure that individuals requiring access to agency information systems acknowledge and accept appropriate access agreement prior to being granted access and reviews/updates the access agreements annually. [NIST 800-53 PS-06] [IRS Pub 1075] [PCI DSS 12.3].

6.7 **Third-Party Personnel Security** - The BU shall: [NIST 800-53 PS-07] [IRS Pub 1075] [HIPAA 164.314(a)(1)]
   
   a. Establish personnel security requirements including security roles and responsibilities for third-party providers;
   
   b. Documents personnel security requirements; and
   
   c. Monitor provider compliance.
6.8 Third-Party Contracts - The BU shall ensure that third party contractors specify the third-party will: [HIPAA 164.314(a)(2)(i)]
   a. Comply with the applicable security requirements;
   b. Ensure that any subcontractors that create, receive, maintain, or transmit sensitive information on behalf of the third-party agree to comply with applicable requirements; and
   c. Report to the BU any security incident of which it becomes aware, including breaches of unsecured sensitive information.

6.9 Personnel Sanctions - The BU shall employ a formal sanctions process for personnel failing to comply with established agency information security and privacy PSPs and document the sanctions applied. [NIST 800-53 PS-08] [IRS Pub 1075] [HIPAA 164.308(a)(1)(ii)(C)] [HIPAA 164.530(e)(1),(2)]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK P8270 Personnel Security Controls
8.2 Statewide Policy Exception Procedure
8.3 Executive Order 1403
8.4 A.R.S. 41-710

9. ATTACHMENTS
None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Update for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8280): ACCEPTABLE USE

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 (ARS) § 18-104 and § 18-105. REFERENCE STATEWIDE POLICY FRAMEWORK P8280 ACCEPTABLE USE.

2. PURPOSE

The purpose of this policy is to outline the acceptable use of agency information system assets to reduce the risks to agency information systems due to disclosure, modification, or disruption, whether intentional or accidental.

3. SCOPE

3.1 Application to Budget Unit (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. Policy statements preceded by “(P)” are required for agency information systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

3.3 Application to End User - The content of this policy is primarily focused towards the end-user, unless explicitly specified otherwise, as stated in Section 3.1.

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 - 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 - 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:
   a. Be ultimately responsible for the correct and thorough completion of Statewide 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 all state BU activities and documentation provided to ensure compliance with statewide IT 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 the mitigation options to improve security.

5.3 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:
   a. Be responsible for the correct and thorough completion of BU PSPs;
b. Ensure compliance with BU PSPs; and  
c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 BU CIO shall:
   a. Work with the BU Director to ensure the correct and thorough completion of Information Technology PSPs; and  
b. Ensure the Acceptable Use Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 BU Information Security Officer (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 BU PSPs;  
c. Request changes and/or exceptions to existing Statewide PSPs from the State CISO; and  
d. Ensure all personnel understand their responsibilities with respect to acceptable use of agency information systems and assets.

5.7 Supervisors of agency employees and contractors shall:
   a. Ensure users are appropriately trained and educated on acceptable use policies; and  
b. Monitor employee activities to ensure compliance.

5.8 System Users of agency information systems shall:
   a. Become familiar with this and related PSPs; and  
b. Adhere to PSPs regarding classification of data and handling within agency information systems.

6. STATEWIDE POLICY

6.1 Access Agreements - The BU Director shall ensure that individuals requiring access to organizational information and agency information systems acknowledge and accept appropriate access agreements (prior to being granted access) and shall review and, if necessary, update the access agreements annually. [NIST 800-53 PS-6] [PCI DSS 12.3].
6.1.1 **Assign Responsibility to Provide Policy** - The BU Director shall assign responsibility to a department, role, or named individual to provide acceptable use and other related information security policies to employees and contractors.

6.1.2 **Assign Responsibility to Keep Records** - The BU Director shall assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

6.2 **Access Agreement Contents** - The access agreements shall contain the following policy sections and statements:

6.2.1 **Expected Behaviors** - The following behaviors shall be required:

6.2.1.1 **Practice Safe Computing** - Those accessing agency information systems shall use caution and exercise good security practices to ensure the protection of agency information systems and data, including, but not limited to:

   a. **Opening Attachments or Links** - Use caution when opening email attachments or following hypertext links received from unknown senders.

   b. **Keep Passwords Secure** - Select strong passwords, do not write them down, change them frequently, and do not share them with anyone.

   c. **Keep Desk and Workstation Secure** - Use available operating system functions to lock the workstation when away from the desk. At the end of the day, log out of the computer, but leave the equipment powered on.

   d. **Challenge Unauthorized Personnel** - Assist in enforcing physical access controls by challenging unauthorized personnel who may not be following procedures, appropriate badge display and use, escort control, and/or entry.

   e. **Report Security or Privacy Weaknesses or Violations** - Report any weaknesses in computer security or data privacy, suspicious behavior of others and any incidents of possible misuse or violation of this policy to the proper authorities.

   f. **Wear Issued Badges** – All employees and contractors are required to wear their agency-issued ID badges, while in the building, at all times.

6.2.1.2 **Protect Confidential Information** - Confidential information shall be protected in accordance with applicable statutes, rules, policies, standards, and procedures. Those accessing agency information systems...
shall protect confidential information in accordance with the STATEWIDE POLICY FRAMEWORK 8110, Data Classification and Handling. Specifically, the following:

6.2.1.3 Marking of Confidential Information - All non-public data must be marked (labeled) as Confidential. Unlabeled data is assumed to be Public.

6.2.1.4 Unencrypted Confidential Information - Confidential information sent over email or other electronic messaging without adequate encryption shall be prohibited (even to an authorized user).

6.2.1.5 Storage of Confidential Information - Confidential information must be stored in accordance with the STATEWIDE POLICY FRAMEWORK 8250, Media Protection.

6.2.1.6 Electronic Transmission of Confidential Information - Confidential information that is transmitted outside of the agency information system or on any medium that can be accessed by authorized users shall be encrypted through link or end-to-end encryption with an encryption algorithm and key length that meets the Statewide Standard 8350, System and Communication Protection.

6.2.2 Prohibited Behaviors - The following behaviors shall be prohibited:

   a. Computer Tampering - Unauthorized access, interception, modification or destruction of any computer, computer system, agency information system, computer programs or data; [ARS 13-2316.1-2]

   b. Use of Unauthorized Computing Equipment - Installation or connections of any computing equipment not provided or authorized by management to agency information systems;

   c. Use of Unauthorized Software or Services - Installation or use of any unauthorized software, including but not limited to browser applications and extensions, security testing, monitoring, encryption, or “hacking” software on agency computing resources; [NIST 800 53 CM-11]

   d. Unauthorized Use of Software or Services - Use of peer-to-peer file sharing technology used for the unauthorized distribution, display, performance, or reproduction of copyrighted work; [NIST 800 53 CM-10]

   e. Introduction of Malware - Knowingly introducing a computer contaminant into any computer, computer system or agency information system; [ARS 13-2316.3]
f. **System Disruption** - Recklessly disrupting or causing the disruption of a computer, computer system or agency information system; [ARS 13-2316.4]

**g. Circumvention of Security Controls** - Disabling software, modifying configurations, or otherwise circumventing security controls. [ARS 13-2316] Tampering with physical security measures (e.g., locks, cameras) is also prohibited;

**h. False Identity** - Falsifying identification information or routing information so as to obscure the origins or the identity of the sender, or using or assuming any information system or application identification other than your own;

**i. Cryptocurrency Mining** - Malicious software is introduced onto a computer, and power is used to compute math problems to obtain cryptocurrency.

### 6.2.2.1 Unauthorized Inappropriate or Unlawful Material

- The unauthorized storage, transmission, or viewing of any pornography or other offensive, intimidating, hostile or otherwise illegal material is forbidden. Except to the extent required in conjunction with a bona fide agency approved research project or other agency approved undertaking, an employee of an agency shall not knowingly use agency owned or agency leased computer equipment to access, download, print or store any information infrastructure files or services that depict nudity, sexual activity, sexual excitement or ultimate sex acts; [ARS 38-448] [ARS 13-2316.5]

### 6.2.2.2 Unauthorized Use of Electronic Messaging

- **Spam** - Sending of unsolicited commercial emails/electronic messages in bulk (identical content to multiple recipients).

- **Chain Letters** - Creating of forwarding chain letters of pyramid schemes.

- **Unprofessional Communications** - Unprofessional or un-businesslike in appearance or content.

- **Alter Message Content** - Modification or deletion of email/electronic messages originating from another person or computer with the intent to deceive.

- **False Identity** - Falsifying email/electronic message headers or routing information so as to obscure the origins of the email/electronic message or the identity of the sender, also known as spoofing.
f. **Mask Identity** - Unauthorized use of anonymous addresses for sending and receiving email/electronic messages.

g. **Auto-Forward to External Accounts** - Automatically forwarding email/electronic messages sent to an BU account to an external email/electronic messages without authorization.

h. **Non-agency Email Accounts** - Unauthorized use of a non-agency email account for agency business.

i. **Unencrypted Confidential Information** - Confidential information sent over email or other electronic messaging without adequate encryption (even to an authorized user).

j. **Misrepresentation of BU** - Presenting viewpoints or positions not held by the BU as those of the BU or attributing them to the BU.

6.2.2.3 **Personal Use of Agency Information Systems** - Personal use of agency technology assets/information systems shall be limited to occasional use during break periods provided the use does not interfere with agency information systems or services.

6.2.2.4 **Violation of Intellectual Property Laws** - Unauthorized receipt, use or distribution of unlicensed software, copyrighted materials, or communications of proprietary information or trade secrets.

6.2.2.5 **Unauthorized Access of Confidential Information** - Unauthorized access of information that has been classified as Confidential could cause harm to the state and/or the citizens of the state. The Confidentiality of information is protected by law. The unauthorized access of any confidential information is prohibited. [ARS 13-2316.07]

6.2.2.6 **Unauthorized Release of Confidential Information** - Disclosure of information that has been classified as Confidential could cause harm to the state and/or the citizens of the state. The Confidentiality of information is protected by law. The unauthorized release or disclosure of any confidential information is prohibited. [ARS 36-342] [ARS 36-666] [ARS 41-151.12] [ARS 41-1750.01]

6.2.2.7 **Unauthorized Posting of Agency Documents** - Unauthorized posting of agency draft or final agency documents is prohibited.

6.2.3 **Notifications and Acknowledgements** - The following notifications and acknowledgements shall be used to inform those granted access to organizational information and/or agency information systems of steps the BU may take to ensure the security of agency information systems:
6.2.3.1 **User Responsibility Acknowledgement** - All users review and acknowledge their understanding of this policy and other related information security policies on an annual basis; [PCI DSS 12.6.2]

6.2.3.2 **Assets and Intellectual Property** - All agency information system assets remain the sole property of the State of Arizona. Any data or intellectual property created by the user, including voicemail and electronic messages, shall remain the property of the State of Arizona and shall not be removed, copied or shared with any person or entity except as part of the user’s normal job responsibilities;

6.2.3.3 **Monitoring** - The BU shall inform all users that it reserves the right to monitor all activities that occur on its agency information systems or to access any data residing on its systems or assets at any time without further notice. The BU shall retain the right to override an individual’s passwords and/or codes to facilitate access by the BU;

6.2.3.4 **Potential Blocking of Inappropriate Content** - The BU may block access to web content it deems as inappropriate or filter email destined for your mailbox;

6.2.3.5 **Incomplete Blocking of Inappropriate Content** - The BU shall not be responsible for material viewed or downloaded by users from the Internet or messages delivered to a user’s mailbox. Users are cautioned that many Internet pages and emails include offensive, sexually explicit, and inappropriate material. Even though the BU intends to filter and block inappropriate content and messages it is not possible to always avoid contact with offensive content on the Internet or in your email. If such an action occurs users are expected to delete the offensive material, leave the offensive site and contact the BU security department;

6.2.3.6 **Records Retention** - Files, emails, attachments and other records are retained, preserved, and/or disposed of in accordance with BU records retention policies and in full accordance with the Arizona State Library Records Retention Schedule, Electronic Communication Records: [http://apps.azlibrary.gov/records/general_rs/Electronic%20Communications,%20Social%20Networking%20Website.pdf](http://apps.azlibrary.gov/records/general_rs/Electronic%20Communications,%20Social%20Networking%20Website.pdf);

6.2.3.7 **No Expectation of Privacy** - Users shall have no expectation of privacy for any communication or data created, stored, sent, or received on agency information systems and assets; and
6.2.3.8 User Acknowledgement - By using agency information systems, users shall acknowledge that they explicitly consent to the monitoring of such use and the right of the BU to conduct such monitoring.

6.3 Virtual Office Agreement - The BU shall ensure that individuals utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access agency information systems as a trusted user acknowledge and accept appropriate access agreements prior to being granted access and shall review, and if necessary, update agreements annually.

6.3.1 Assign Responsibility to Provide Policy - The BU shall assign responsibility to a department, role, or named individual to provide acceptable use and other related information security policies to employees and contractors.

6.3.2 Assign Responsibility to Keep Records - The BU shall assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

6.4 Virtual Office Access Agreement Contents - The Virtual Office Access agreements shall contain the following additional policy sections and statements:

6.4.1 (P) Allowable Computing Devices - An individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access agency information systems as a trusted user providing and storing Confidential information shall ensure:

a. The computing equipment is issued to the individual by the agency for the purposes of connecting to a agency information system; or

b. The computing equipment is owned or otherwise under the control of the individual such that the individual may ensure minimum physical and logical protections are in place.

6.4.2 (P) Physical Protection of Computing Devices - An individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access agency information systems as a trusted user providing and storing Confidential information shall ensure that computer equipment is:

a. Physically protected from unauthorized use and removal; and

b. Limited to the use of the authorized virtual office user. Use of the computer equipment by anyone else (e.g., family members, roommates) is strictly forbidden.
6.4.3 (P) Logical Protection of Computing Devices - An individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access agency information systems as a trusted user providing and storing Confidential information shall ensure that computer equipment has the following logical security controls:

   a. **Username and Passwords** - Identification and authentication controls consistent with STATEWIDE POLICY FRAMEWORK 8340, Identification and Authentication;

   b. **Anti-Virus** - Malicious code protection consistent with STATEWIDE POLICY FRAMEWORK 8220, System Security Maintenance, with the exception of central management of malicious code protection;

   c. **Personal Firewalls** - Personal firewalls consistent with STATEWIDE POLICY FRAMEWORK 8320, Access Control;

   d. **Device Encryption** - Full Device Encryption consistent with the Access Control Policy; and

   e. **Security Patches** - Install security-relevant software and firmware updates consistent with STATEWIDE POLICY FRAMEWORK 8220, System Security Maintenance.

6.4.4 Remote Access - Virtual office users may access the agency information system only by approved access methods.

6.5 User-Based Technologies - The BU shall ensure that individuals utilizing user-based technologies (e.g., smart phones, tablet computers) to access agency information systems as a trusted user acknowledge and accept appropriate access agreements (prior to being granted access), and shall review, and if necessary, update agreements annually.

6.5.1 Assign Responsibility to Provide Policy - The BU shall assign responsibility to a department, role, or named individual to provide user-technology standards, acceptable use, and other related information security policies to employees and contractors.

6.5.2 Assign Responsibility to Keep Records - The BU shall assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

6.6 User-Based Technology Agreement Contents - The user-based technology access agreements shall be developed by the BU and contains BU-defined security controls. Statewide Standard 8220, System Security Maintenance provides guidance to BU for minimum recommended user-based technology controls. Such agreements shall include the following, at a minimum: [PCI DSS 12.3]
a. Explicit approval by authorized parties [PCI DSS 12.3.1]

b. Authentication for use of the technology [PCI DSS 12.3.2]

c. A list of all such devices and personnel with access [PCI DSS 12.3.3]

d. A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) [PCI DSS 12.3.4]

e. Acceptable uses of the technology [PCI DSS 12.3.5]

f. Acceptable network locations for the technologies [PCI DSS 12.3.6]

h. List of BU-approved products [PCI DSS 12.3.7]

i. Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity [PCI DSS 12.3.8]

j. Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use [PCI DSS 12.3.9]

k. For personnel accessing Confidential data via remote-access technologies, prohibit the copying, moving, and storage of Confidential data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable requirements [PCI DSS 12.3.10]

6.7 Consequences for Non-compliance - Users of agency information systems who fail to comply with established information security and privacy policies and procedures may be subject to sanctions, including referral to a law enforcement agency for appropriate action. [NIST 80053 PS-8] [HIPAA 164.308(a)(1)(ii)(C)] [HIPAA 164.530(e)(1),(2)]

6.7.1 Agency Employees - State Personnel System (SPS) Rule R2-5A-501, Standards of Conduct, requires that all employees comply with federal and state laws and rules, statewide policies and employee handbook and agency policy and directives. As provided by SPS Rule R2-5A-501(C), an employee who fails to comply with standards of conduct requirements may be disciplined or separated from state employment.

6.7.2 Agency Contractors - Agency contractors violating federal and state laws and rules, statewide policies, and agency policy and directives may result in, but not be limited to, immediate credential revocation, terminations of permissions for access to data systems and physical locations, and barring entry or access permanently. Vendors providing services under a contract are subject to vendor performance reports, and any contract terms and warranties, including potential damages.
7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK P8280 Acceptable Use
8.2 STATEWIDE POLICY FRAMEWORK 8120, Information Security Program Policy
8.3 Statewide Policy Exception Procedure
8.4 State Personnel System (SPS) Rule R2-5A-501, Standards of Conduct
8.5 Statewide Standard 8350, System and Communication Protection
8.6 Statewide Standard 8220, System Security Maintenance
8.7 STATEWIDE POLICY FRAMEWORK 8340, Identification and Authentication
8.8 STATEWIDE POLICY FRAMEWORK 8320, Access Control
8.9 STATEWIDE POLICY FRAMEWORK 8250, Media Protection
8.10 STATEWIDE POLICY FRAMEWORK 8110, Data Classification and Handling
8.11 STATEWIDE POLICY FRAMEWORK 8220, System Security Maintenance
8.16 General Records Retention Schedule for All Public Bodies, Electronic Communications, Social Networking and Website Records, Schedule Number 000-12-22, Arizona State Library, Archives and Public Records
9. ATTACHMENTS

None.

10. 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                     |
| 9/17/2018 | Updated for PCI-DSS 3.2.1       | 2.0      | Morgan Reed, State CIO and Deputy Director                     |
| 5/26/21   | Annual Updates                  | 3.0      | Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer |
STATEWIDE POLICY (8310): ACCOUNT MANAGEMENT

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 8310 ACCOUNT MANAGEMENT.

2 PURPOSE

The purpose of this policy is to establish the baseline controls for the administration of agency information system accounts.

3 SCOPE

3.1 Application to Budget Units (BUs) - 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5 ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:
   a. Be ultimately responsible for the correct and thorough completion of Statewide 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 all state BU activities and documentation provided to ensure compliance with statewide IT PSPs throughout all state BUs;
b. Review and approve or disapprove all state BU security and privacy PSPs and exceptions to existing 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 Enterprise Security Program Advisory Council (ESPAC)

a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 BU Director shall:

a. Be responsible for the correct and thorough completion of BU PSPs;

b. Ensure compliance with BU PSPs; and

c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of BU IT PSPs; and

b. Ensure BU PSPs are periodically reviewed and updated to reflect changes in requirements.

5.6 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 BU PSPs;

c. Request changes and/or exceptions to existing PSPs from the State CISO; and

d. Ensure all personnel understand their responsibilities with respect to secure account management.

5.7 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on BU PSPs; and

b. Monitor employee activities to ensure compliance.
5.8 System Users of agency information systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding account management and acceptable use of agency information systems.

STATEWIDE POLICY

6. The BU shall implement account management through the following activities:

6.1. (P) **Automated Account Management** - The BU shall employ automated mechanisms to support the management of information system accounts. [NIST 800-53 AC-2(1)] [IRS Pub 1075]

6.2. (P) **Develop Account Management Operational Procedures** - The BU shall ensure that security policies and operational procedures for restricting access to Confidential data are documented, in use, and known to all affected parties and cover all system components. [PCI DSS 7.2.1, 7.3]

6.3. **Identify Account Types** - The BU shall identify the types of agency information system accounts to support organizational missions / business functions (e.g., individual, guest, emergency access, developer, maintenance, administration). [NIST 800-53 AC-2a] [HIPAA 164.312 (a)(2)(iii) – Addressable] [PCI DSS 7.2.2]

6.3.1. **Establish Group and Role-based Accounts** - The BU shall establish conditions for group and role membership. [NIST 800-53 AC-2c] [PCI DSS 7.1.1] [PCI DSS 7.2.2]

6.3.2. **Account Specification** - The BU shall specify authorized users of the agency information system, group and role membership, and access authorizations (i.e., privileges) and other attributes for each account. [NIST 800-53 AC-2d] [PCI DSS 7.1.3]

6.3.3. (P) **Privileged Accounts** - The BU shall restrict privileged accounts (e.g., super user accounts) on the agency information system to administrative roles. [NIST 800-53 AC-6(5)] [IRS Pub 1075] [PCI DSS 7.1.2]

6.3.4. (P) **Separation of Duties** - The BU shall separate BU -defined duties; documents separation of duties of individuals; and defines agency information system access authorizations to support separation of duties. [NIST 800-53 AC-5] [IRS Pub 1075] [PCI DSS 6.4.2]
6.4. **Assign Account Managers** - The BU shall assign account managers for agency information system accounts. [NIST 800-53 AC-2b]

6.5. **Account Approval** - The BU shall require documented approvals by authorized BU staff for requests to create, modify, and enable agency information system accounts. [NIST 800-53 AC-2e-f] [PCI DSS 7.1.4]

6.5.1. **(P) Automated Audit Actions** - The BU shall ensure the agency information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies, as required BU-defined personnel or roles. [NIST 800-53 AC-2(4)] [IRS Pub 1075]

6.6. **Account Monitoring** - The BU shall authorize, and monitor the use of agency information system accounts. [NIST 800-53 AC-2g]

6.6.1. **(P) Vendor Account Monitoring** - The BU shall enable accounts used by vendors for remote access only during the time period needed and monitors the vendor remote access accounts when in use. [PCI DSS 8.1.5]

6.7. **Account Creation, Deletion, and Removal** – The BU shall control the addition, deletion, and modification of user IDs, credentials, and other identifier objects. [PCI DSS 8.1.2]

6.7.1. **Account Removal** - The BU shall notify account managers when accounts are no longer required; users are separated or transferred; and individual information system usage or need-to-know changes. [NIST 800-53 AC-2h] [PCI DSS 8.1.3]

6.7.2. **(P) Immediate Removal of Separated Users** - The BU shall immediately revoke access for any separated users. [PCI DSS 8.1.3]

6.7.3. **(P) Automatic Removal of Temporary Accounts** - The agency information system automatically removes or disables temporary and emergency accounts after a BU-defined time. [NIST 800-53 AC-2(2)] [IRS Pub 1075]

6.7.4. **(P) Disable Inactive Accounts** - The BU shall ensure the agency information system automatically disables inactive accounts after BU-defined time period. For agency information systems containing cardholder data (CHD) the time period must be no more than 90 days. [NIST 800-53 AC-2(3)] [IRS Pub 1075] [PCI DSS 8.1.4]

6.8. **Access Authorization** - The BU shall authorize access to the agency information system based on a valid access authorization; intended system usage; and other attributes as required by the organization or associated mission functions. [NIST 800-53 AC-2f,i] [HIPAA 164.308 (4)(ii)(B) – Addressable] [PCI DSS 7.1, 7.2]
6.8.1. (P) **Default “Deny-All” Setting** - The BU shall ensure the agency information system access control system is set to “Deny all” unless specifically allowed. [PCI DSS 7.2.3]

6.8.2. (P) **Restrict Direct Database Access** - The BU shall ensure the agency information system authenticates all access to any database containing Confidential information and restricts direct access or queries to databases to database administrators. [PCI DSS 8.7]

6.9. **Accounts Rights Review** - The BU shall review accounts for compliance with account management requirements annually. [NIST 800-53 AC-2j] [HIPAA 164.308 (4)(ii)(C) – Addressable]

6.10. **Reissues Account Credentials** - The BU shall establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. [NIST 800-53 AC-2k]

7. **DEFINITIONS AND ABBREVIATIONS**

7.1. Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. **REFERENCES**

8.1. STATEWIDE POLICY FRAMEWORK 8310 Account Management

8.2. Statewide Policy Exception Procedure


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


9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Update for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8320): ACCESS CONTROLS

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 8320 ACCESS CONTROLS.

2. PURPOSE

The purpose of this policy is to define the correct use and management of logical access controls for the protection of agency information systems and assets.

3. SCOPE

3.1 Application to Budget Units (BUs) - 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 - 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 - 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 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 Access Control Policy; and
   c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 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 Access Controls Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 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 Access Controls Policy for the BU; and
   c. Ensure all personnel understand their responsibilities with respect to the correct use and management of logical access controls for the protection of agency information systems and assets.

5.7 Supervisors of agency employees and contractors shall:
   a. Ensure users are appropriately trained and educated on Access Control PSPs; and
   b. Monitor employee activities to ensure compliance.

5.8 System Users of agency information systems shall:
   a. Become familiar with this policy and related PSPs; and
   b. Adhere to PSPs regarding correct use and management of logical access controls for the protection of agency information systems and assets.
6. STATEWIDE POLICY

6.1 Access Enforcement - The BU shall ensure the agency information system enforces approved authorizations for logical access to information and system resources in accordance with applicable control policies (e.g., identity-based policies, role-based policies). [NIST 800-53 AC-3] [HIPAA 164.308(a)(3)(ii)(A) - Addressable, 164.308 (a)(4)(ii)(B) & (C) - Addressable]

6.1.1 (P) Assign Responsibility - The BU shall assign to an individual or team the security management responsibility of monitoring and controlling all access to Confidential data. [PCI DSS 12.5.5]

6.2 (P) Develop Access Control Operational Procedures - The BU shall develop daily operational security procedures for restricting access to sensitive data are documented, in use, and known to all affected parties. [PCI DSS 7.3]

6.3 (P) Information Flow Enforcement - The BU shall ensure the agency information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on BU-defined information flow control policies, including STATEWIDE POLICY FRAMEWORK 8350, Systems and Communications Protections. These policies prohibit direct public access between the Internet and any system component in the Protected agency information system. [NIST 800-53 AC-4] [IRS Pub 1075] [PCI DSS 1.3]

6.3.1 (P) Perimeter Firewalls for Wireless Networks - The BU shall install perimeter firewalls between any wireless network and the Protected agency information system, and configures these firewalls to deny, or control (if such traffic is necessary for business purposes), permit only authorized traffic between the wireless environment into the Protected agency information system. [PCI DSS 1.2.3]

6.3.2 (P) Personal Firewalls - The BU shall require personal firewall software or equivalent functionality on any portable computing devices (including agency and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the agency network. [PCI DSS 1.4]

6.4 (P) Least Privilege - The BU shall employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. [NIST 800-53 AC-6] [IRS Pub 1075] [PCI DSS 7.1]

6.4.1 (P) Organizational Isolation - The BU shall implement policies and procedures that protect Confidential information from unauthorized access by other (e.g., larger BU to which the BU is a part of) organizations. [HIPAA 164.308 (a)(4)(ii)(A)]
6.4.1.1 (P) Shared Host Isolation – For agencies that provide a shared hosting service to other agencies, the Agency BU shall ensure that agency hosts are protected from other users and processes on the same host or environment. Specifically, that BU shall ensure that: [PCI DSS A.1]
   a. each entity only runs processes that have access to that entity’s own environment [PCI DSS A.1.1] and
   b. each entity’s access and privileges shall be restricted to its own environment. [PCI DSS A.1.2]

6.4.2 (P) Privileged Accounts - The BU shall restrict access rights to privileged user accounts to least privileges necessary to perform job responsibilities. [PCI 7.1.1]

6.4.3 (P) Job Classification - The BU shall restrict access rights based on individual personnel’s job classification and function. [PCI DSS 7.1.3]

6.5 (P) Authorize Access to Security Functions - The BU shall explicitly authorize access to the following security functions and security-relevant information: [NIST 800-53 AC-6(1)] [IRS Pub 1075]
   a. Establishing system accounts
   c. Configuring access authorizations
   d. Setting events to be audited
   e. Setting intrusion detection parameters
   f. Filtering rules for routers and firewalls
   g. Cryptographic key management information
   h. Configuration parameters for security services

6.6 (P) Non-Privileged Access for Non-Security Functions - The BU shall require that users of agency information system accounts, or roles, with access to security functions (e.g., privileged users), use non-privileged accounts or roles, when accessing non-security functions. [NIST 800-53 AC-6(2)] [IRS Pub 1075]

6.7 (P) Auditing of Privileged Functions - The BU shall include execution of privileged functions in the events to be audited by the agency information system. [NIST 800-53 AC-6(9)]

6.8 (P) Prohibit Non-Privileged Users From Executing Privileged Functions - The BU shall ensure the agency information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures. [NIST 800-53 AC-6(10)] [IRS Pub 1075]
6.9 Unsuccessful Logon Attempts - The BU shall ensure the agency information system enforces a BU specified limit of consecutive invalid logon attempts by a user; and automatically locks the account/node for a BU specified period of time or locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded, consistent with the Statewide Access Control Standard 8320. [NIST 800-53 AC-7] [PCI DSS 8.1.6]

6.10 System Use Notification - The BU shall ensure the agency information system: [NIST 800-53 AC-8]

6.10.1 Displays to users a BU-defined notification banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance and shall state the following:

a. Users are accessing an agency information system owned by the State of Arizona;

b. Agency information system usage may be monitored, recorded, and subject to audit;

c. Unauthorized use of the agency information system is prohibited and subject to criminal and civil penalties; and

d. Use of the agency information system indicates consents to monitoring and recording.

e. Retains the notification banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the agency information system; and

f. For publicly accessible systems; the agency information system shall also:

g. Display to users the system use agency information before granting further access;

h. Display to users references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

i. Include in the notice given to public users of the agency information system, a description of the authorized uses of the system.

6.11 (P) Session Lock - The BU shall ensure the agency information system prevents further access to the system by initiating a BU specified limit of time inactivity or upon receiving a request from a user; and retains the session lock for a BU specified limit of time or until the user reestablishes access using established identification and authentication.
procedures. If the user does not reestablish access within a BU specified limit of time the session is dropped. [NIST 800-53 AC-11] [IRS Pub 1075] [HIPAA 164.312 (a)(2)(iii)] [PCI DSS 8.1.7, 8.1.8]

6.12 Permitted Actions Without Identification or Authentication - The BU shall identify user actions that can be performed on the agency information system without identification or authentication consistent with BU missions; and documents and provides support rationale in the security plan for the agency information system, user actions not requiring identification or authentication. [NIST 800-53 AC-14]

6.13 Remote Access - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and authorizes remote access to the agency information system prior to allowing such connections. [NIST 800-53 AC-17]

6.14 (P) Automated Monitoring / Control - The BU shall ensure the agency information system monitors and controls remote access methods (e.g., detection of cyber-attacks such as false logins and denial of service-attacks and compliance with remote access policies such as strength of encryption). [NIST 800-53 AC-17(1)] [IRS Pub 1075]

6.14.1 (P) Security Using Encryption - The BU shall ensure the agency information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions, consistent with the Statewide Standard 8350 System and Communication Protection. [NIST 800-53 AC-17(2)] [IRS Pub 1075] [PCI DSS 2.3, 4.1]

6.14.2 (P) Managed Access Control Points - The BU shall ensure the agency information system routes all remote accesses through a limited number of managed network access control points. [NIST 800-53 AC-17(3)] [IRS Pub 1075]

6.14.3 (P) Privileged Access Commands - The BU shall authorize the execution of privileged commands and access to security-relevant information using remote access only for BU-defined needs, and documents the rationale for such access in the security plan for the agency information system. [NIST 800-53 AC-17(4)] [IRS Pub 1075]

6.15 Wireless Access - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and authorizes wireless access to the agency information system prior to allowing such connections that are consistent with the Statewide Standard 8350 System and Communication Protection. [NIST 800-53 AC-18]

6.15.1 (P) Wireless Authentication and Encryption - The BU shall ensure the agency information system protects wireless access to the agency information system using authentication of users and devices and encryption. [NIST 800-53 AC-18(1)] [IRS Pub 1075] [PCI DSS 4.1]
6.15.2 Wireless Encryption Strength – The BU shall ensure wireless networks transmitting Confidential data use industry best practices to implement strong encryption for authentication and transmission. [PCI DSS 4.1.1]

6.16 Access Control for Mobile Devices - The BU shall establish usage restrictions, configuration/connection requirements, and implementation guidance for BU controlled mobile devices; and authorizes connection of mobile devices to agency information systems. [NIST 800-53 AC-19]

6.16.1 (P) Full Device Encryption - The BU shall employ full-device encryption to protect the confidentiality and integrity of information on mobile devices authorized to connect to agency information systems or to create, transmit or process Confidential information. [NIST 800-53 AC-19(5)] [IRS Pub 1075] [HIPAA 164.308 (e)(2)(ii) - Addressable] [PCI DSS 4.1]

6.17 Use of External Information Systems - The BU shall establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems; and process, store, or transmit BU controlled information using external information systems. [NIST 800-53 AC-20]

6.17.1 (P) Limits on Authorized Use - The BU shall permit authorized individuals to use an external information system to access the agency information system to process, store, or transmit BU controlled information only when the BU: [NIST 800-53 AC-20(1)] [IRS Pub 1075]

a. Verifies the implementation of required security controls on the external system as specified in the BUs information security policies and security plan; or

b. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system in accordance with the Arizona State Library Records Retention Schedule, Management Records, Item 6: http://apps.azlibrary.gov/records/general_rs/Management.pdf.

6.17.2 (P) Portable Storage Devices - The BU shall restrict or prohibit the use of BU controlled portable storage devices by authorized individuals on external information systems. [NIST 800-53 AC-20(2)] [IRS Pub 1075]

6.18 (P) Information Sharing - The BU shall facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for BU-defined circumstances;
and shall employ mechanisms or processes to assist users in making information sharing/collaboration decisions. [NIST 800-53 AC-21] [IRS Pub 1075] [PCI DSS 12.8]

**6.18.1 (P) Maintain List of Service Providers** - The BU shall maintain a list of service providers, including a description of the service provided, that have access to Confidential data. [PCI DSS 12.8.1]

**6.18.2 (P) Written Agreements** - The BU shall maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of Confidential data the service providers possess. [PCI DSS 12.8.2]

**6.18.3 (P) Due Diligence** - The BU shall ensure there is an established process for engaging service providers including proper due diligence prior to engagement. [PCI DSS 12.8.3]

**6.18.4 (P) Service Provider Monitoring Program** - The BU shall maintain a program to monitor service provider’s compliance with requirements for the protection of Confidential data. [PCI DSS 12.8.4]

**6.18.5 (P) Service Provider Information** - The BU shall maintain information about which information security requirements are managed by each service provider, and which are managed by the BU. [PCI DSS 12.8.5]

**6.19 Publicly Accessible Content** - The BU shall: [NIST 800-53 AC-22]

a. Designate individuals authorized to post information onto a publicly accessible information system;

b. Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Review the proposed content of information prior to posting onto the publicly accessible agency information system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible agency information system for nonpublic information annually and removes such information, if discovered.

**7. DEFINITIONS AND ABBREVIATIONS**

**7.1** Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.
8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8320 Access Controls

8.2 Statewide Policy Exception Procedure

8.3 STATEWIDE POLICY FRAMEWORK 8350, Systems and Communications Protections

8.4 Statewide Standard 8320, Access Control

8.5 Statewide Standard 8350, System Communication and Protection


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


8.10 General Records Retention Schedule Issued to All Public Bodies, Management Records, Schedule Number GS 1005, Arizona State Library, Archives and Public Records, Item Number 6

9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State of Arizona CIO</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State of Arizona CIO</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State of Arizona CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8330): SYSTEM SECURITY AUDIT

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 8330 SYSTEM SECURITY AUDIT.

2. PURPOSE

The purpose of this policy is to protect agency information systems and data by ensuring the Budget Unit (BU) and agency information systems have the appropriate controls and configurations to support audit log generation, protection, and review.

3. SCOPE

3.1 Application to Budget Units (BUs) - 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 - 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 - 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 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 Security Audit Policy; and
   c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 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 Security Audit Policy is periodically reviewed and updated to reflect changes in requirements.

5.6 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 Security Audit Policy for the BU; and
   c. Ensure all personnel understand their responsibilities with respect to the generation, protection and review of audit logs.

5.7 Supervisors of agency employees and contractors shall:
   a. Ensure users are appropriately trained and educated on System Security Audit Policies; and
   b. Monitor employee activities to ensure compliance.

5.8 System Users of agency information systems shall:
   a. Become familiar with this policy and related PSPs; and
b. Adhere to PSPs regarding the generation, protection and review of audit logs.

6. STATEWIDE POLICY

6.1 Audit Events - The BU shall: [NIST 800-53 AU-2]

a. Determine that the agency information system is capable of auditing the events listed in the Statewide System Security Audit Standard S8330.

b. Coordinate the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events;

c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Ensure the events listed in the Statewide System Security Audit Standard S8330 are logged within the agency information system.

e. (P) For agencies that provide a shared hosting service to other agencies, ensure that logging and audit trails are unique to each agencies environment. [PCI DSS A.1.3]

6.1.1 (P) Audit Reviews and Updates - The BU shall review and update the selected audited events annually, or as required. [NIST 800-53 AU-2(3)] [IRS Pub 1075]

6.2 Content of Audit Records - The BU shall ensure the agency information system generates audit records containing information that establishes: [NIST 800-53 AU-3] [PCI DSS 10.3]

a. What type of event occurred; [PCI DSS 10.3.2] [IRS Pub 1075]

b. When the event occurred; [PCI DSS 10.3.3] [IRS Pub 1075]

c. Where the event occurred; [PCI DSS 10.3.5] [IRS Pub 1075]

d. The source of the event (i.e., name of the affected data, system component, or resource); [PCI DSS 10.3.6] [IRS Pub 1075]

e. The outcome of the event; and [PCI DSS 10.3.5]

f. The identity of any individuals or subjects associated with the event. [PCI DSS 10.3.1] [IRS Pub 1075]

6.2.1 (P) Additional Audit Information - The BU shall ensure the state information system generates audit records containing BU-defined additional information. [NIST 800-53 AU-3(1)] [IRS Pub 1075]
6.3 **Audit Storage Capacity** - The BU shall allocate audit record storage capacity in accordance with BU-defined audit record storage requirements. [NIST 800-53 AU-4]

6.4 **Response to Audit Processing Failures** - The BU shall ensure the agency information system alerts BU-defined personnel or roles in the event of an audit processing failure; and shuts down the agency information system, overwrites the oldest audit records, or stops generating audit records. [NIST 800-53 AU-5]

6.5 **Audit Review, Analysis, and Reporting** - The BU shall review and analyze agency information system audit records periodically for indications of inappropriate or unusual activity; and reports findings to BU-defined personnel or roles. Agency information systems with cardholder data (CHD) shall perform this review daily. [NIST 800-53 AU-6] [HIPAA 164.308 (a)(1)(ii)(D)] [HIPAA 164.312 (b)] [PCI DSS 10.6, 10.6.1, 10.6.2, 10.6.3]

6.5.1 (P) **Process Integration** - The BU shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities. [NIST 800-53 AU-6(1)] [IRS Pub 1075]

6.5.2 (P) **Correlate Audit Repositories** - The BU shall analyze and correlate audit records across different repositories to gain BU-wide situational awareness. [NIST 800-53 AU-6(3)] [IRS Pub 1075]

6.6 **Audit Reduction and Report Generation** - The BU shall ensure the agency information system provides an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and does not alter original audit records. [NIST 800-53 AU-7]

6.6.1 (P) **Automatic Processing** - The BU shall ensure the agency information system provides the capability to process audit records for events of interest based on the following audit fields within audit records: [NIST 800-53 AU-7(1)] [IRS Pub 1075]

   a. Individual identities
   b. Event types
   c. Event locations
   d. Event times and time frames
   e. Event dates
   f. System resources involved, IP addresses involved
   g. Information object accessed
6.7 **Time Stamps** - The BU shall ensure the agency information system uses internal system clocks to generate time stamps for audit records; and generates time in the time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and provides a granularity of time to a BU-defined unit of time. [NIST 800-53 AU-8]

6.7.1 (P) **Synchronization with Authoritative Time Source** - The BU shall ensure the agency information system synchronizes internal agency information system clocks a BU-defined frequency with a BU-defined time source when the time difference is greater than a BU-defined time period. [NIST 800-53 AU-8(1)] [IRS Pub 1075] [PCI DSS 10.4, 10.4.1, 10.4.3]

6.7.2 (P) **Protection of Time Data** - The BU shall ensure the agency information system protects time-synchronization settings by restricting access to such settings to authorized personnel and logging, monitoring, and reviewing changes. [PCI DSS 10.4.2]

6.8 **Protection of Audit Information** - The BU shall ensure the agency information system protects audit information and audit tools from unauthorized access, modification, and deletion. [NIST 800-53 AU-9] [PCI DSS 10.5] [IRS Pub 1075]

6.8.1 (P) **Access by Subset of Privileged Users** - The BU shall authorize access and modification to management of audit functionality to only a BU-defined subset of privileged users. [NIST 800-53 AU-9(4)] [IRS Pub 1075] [PCI DSS 10.5.1, 10.5.2]

6.8.2 (P) **Audit Trail Backup** - The BU shall promptly back up audit trail files to a centralized log server or media that is difficult to alter. [PCI DSS 10.5.3]

6.8.3 (P) **Audit Backup on Separate Physical Systems** - The BU shall ensure the agency information system backs up audit records onto a physically different system or system components than the system or component being audited. [PCI DSS 10.5.4]

6.8.4 (P) **File Integrity Monitoring of Audit Logs** - The BU shall ensure the agency information system uses file integrity monitoring or change detection software on audit logs to ensure that existing log data cannot be changed without generating alerts. New audit data being added to audit logs do not cause such alerts. [PCI DSS 10.5.5]

6.9 **Audit Record Retention** - The BU shall retain audit records for a BU-defined time period with a BU-defined time period available for immediate analysis to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. For agency information systems with cardholder data these defined times are at least one year with a minimum of three months immediately available for analysis. [NIST 800-53 AU-11] [PCI DSS 10.7]
6.10 However, all State BUs must comply with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to: http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf Item 16.b.

6.11 Audit Generation - The BU shall ensure the agency information system: [NIST 800-53 AU-12]

   a. Provides audit record generation capability for the auditable events, defined in Section 6.1 (Audit Records), at servers, firewalls, workstations, and other BU-defined system components;

   b. (P) Anti-virus programs are generating audit logs; [PCI DSS 5.2]

   c. Allows BU-defined personnel or roles to select which auditable events are to be audited by specific components of the agency information system; and

   d. Generates audit records for the events, defined in Section 6.1 (Audit Events), with the content defined in Section 6.2 (Content of Audit Records).

6.12 (P) Develop Operational Procedures - The BU shall ensure that security policies and operational procedures for monitoring all access to network resources and Confidential data are documented, in use, and known to all affected parties and cover all system components and include the following: [PCI DSS 10.9]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8330 SYSTEM SECURITY AUDIT

8.2 Statewide Policy Exception Procedure


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


8.7 General Records Retention Schedule for All Public Bodies, Information Technology (IT) Records, Schedule Number: 000-12-41, Arizona State Library, Archives and Public Records, Item Number 16b

9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State of Arizona CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
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 8340 IDENTIFICATION AND AUTHENTICATION.

2. PURPOSE

The purpose of this policy is to define the security requirements for establishing and maintaining user accounts for agency information systems.

3. SCOPE

3.1 Application to Budget Units (BUs) - 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.
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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 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 Identification and Authentication Policy; and
   c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets.

5.5 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 Identification and Authentication Policy is periodically reviewed and updated to reflect changes in requirements

5.6 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 Identification and Authentication Policy for the BU; and
   c. Ensure all personnel understand their responsibilities with respect to establishing and maintaining user accounts for agency information systems.

5.7 Supervisors of agency employees and contractors shall:
   a. Ensure users are appropriately trained and educated on Identification and Authentication Policies; and
   b. Monitor employee activities to ensure compliance.

5.8 System Users of agency information systems shall:
   a. Become familiar with this policy and related PSPs; and
6. **STATEWIDE POLICY**

6.1 **Identification and Authentication of Organizational Users** - The BU shall ensure the agency information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). [NIST 800 53 IA-2] [PCI DSS 8.1, 8.1.1] [HIPAA 164.312 (a)(2)(i), (d)]

6.1.1 **Network Access to Privileged Accounts** - The BU shall ensure the agency information system implements multifactor authentication for network access to privileged accounts. [NIST 800 53 IA-2(1)] [IRS Pub 1075]

6.1.2 **(P) Network Access to Non-Privileged Accounts** - The BU shall ensure the agency information system implements multifactor authentication for non-privileged accounts. [NIST 800 53 IA-2(2)] [IRS Pub 1075]

6.1.3 **(P) Local Access to Privileged Accounts** - The BU shall ensure the agency information system implements multifactor authentication for local access to privileged accounts. [NIST 800 53 IA-2(3)]

6.1.4 **(P) Network Access to Privileged Accounts – Replay Resistant** - The BU shall ensure the agency information system implements replay-resistant authentication mechanisms for network access to privileged accounts. [NIST 800 53 IA-2(8)]

6.1.5 **Remote Access to Organizational Accounts (Privileged and Non-Privileged) – Separate Device** - The BU shall ensure the agency information system implements multifactor authentication for remote access to organizational accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets statewide cryptographic standards for strength of mechanism. [NIST 800 53 IA-2(11)] [PCI DSS 8.3, 8.3.1] [IRS Pub 1075]

6.2 **(P) Device Identification and Authentication** - The BU shall ensure the agency information system uniquely identifies and authenticates before establishing a local, remote, or network connection. [NIST 800 53 IA-3] [IRS Pub 1075] [HIPAA 164.312 (d)]

6.3 **Identifier Management** - The BU shall manage the agency information system identifiers by: [NIST 800 53 IA-4] [PCI DSS 8.5]

   a. **(P) Ensuring that group, shared, or generic account identifiers and authentication methods are not used;** [PCI DSS 8.5, 8.6]
b. Receiving authorization from BU-defined personnel or roles to assign individual, role, or device identifier;

c. Selecting an identifier that identifies an individual, role, or device;

d. Assigning the identifier to the intended individual, role, or device;

e. Preventing reuse of identifiers for one year; and

f. Disabling the identifier after 90 days of inactivity. [PCI DSS 8.1.4]

6.4 Authenticator Management - The BU shall manage the agency information system authenticators (e.g., passwords, tokens, certificate, and key cards) by: [NIST 800 53 IA-5] [HIPAA 164.308(a)(5)ii)(D)] [HIPAA 164.308 (d)]

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; [PCI DSS 8.2.2]

b. Establishing initial authenticator content for authenticators defined by the BU (e.g. password policy);

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators prior to agency information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

g. Changing/refreshing authenticators [BU-defined time period by authenticator type (e.g., passwords, tokens, biometrics, PKI certificates, and key cards)];

h. Protecting authenticator content from unauthorized disclosure and modification;

i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; [PCI DSS 8.6]

j. Changing authenticators for role accounts when membership to those accounts changes; and

k. Employing at least one of the following methods to authenticate all users: [PCI DSS 8.2]

1. Password-Based Authentication
STATEWIDE POLICY (8340): IDENTIFICATION AND AUTHENTICATION

2. PKI-based Authentication
3. In Person or Trusted Third Party Registration
4. Hardware Token-based Authentication

6.4.1 Password-Based Authentication - The BU shall ensure the agency information system, for password-based authentication enforces password controls consistent with the Statewide Standard 8340, Identification and Authentication. [NIST 800 53 IA-5(1)] [PCI DSS 8.2.3, 8.2.4, 8.2.5, 8.2.6]
   a. Password Encryption - The BU shall ensure the use of strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. [PCI DSS 8.2.1]

6.4.2 (P) PKI-based Authentication - The BU shall ensure the agency information system, for PKI-based authentication: [NIST 800 53 IA-5(2)] [IRS Pub 1075]
   b. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
   c. Enforces authorized access to the corresponding private key;
   d. Maps the authenticated identity to the account of the individual or group; and
   e. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information using the network.

6.4.3 (P) In Person or Trusted Third-Party Registration - The BU shall require that the registration process to receive authenticators be conducted in person or by a trusted third-party before the registration authority with authorization by BU-defined personnel or roles. [NIST 800 53 IA-5(3)] [IRS Pub 1075]

6.4.4 Hardware Token-based Authentication - The BU shall ensure the agency information system, for hardware token-based authentication, employs mechanisms that satisfy BU-defined token quality requirements (e.g., compliant with a particular PKI). [NIST 800 53 IA-5(11)]

6.5 Authenticator Feedback - The BU shall ensure the agency information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. [NIST 800 53 IA-6]
6.6 **Cryptographic Module Authentication** - The BU shall ensure the agency information system implements mechanisms for authentication to a cryptographic module that meets the requirements of applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. [NIST 800 53 IA-7]

6.7 **Identification and Authentication (Non-Organizational Users)** - The BU shall ensure the agency information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). [NIST 800 53 IA-8] [PCI DSS 8.1, 8.1.1] [HIPAA 164.312 (a)(2)(i), (d)]

6.7.1 **Acceptance of Third-Party Credentials** - The BU shall ensure the agency information system accepts FICAM-approved third-party credentials. [NIST 800 53 IA-8(2)]

6.7.2 **Use of FICAM-Approved Products** - The BU shall employ only FICAM-approved agency information system components in agency information systems to accept third-party credentials. [NIST 800 53 IA-8(3)]

6.7.3 **Use of FICAM-Issued Profiles** - The BU shall ensure the agency information system conforms to FICAM-issued implementation profiles. [NIST 800 53 IA-8(4)]

6.8 **(P) Develop Operational Procedures** - The BU shall ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties and cover all system components and include the following: [PCI DSS 8.4, 8.8]

- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

7. **DEFINITIONS AND ABBREVIATIONS**

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. **REFERENCES**

8.1 STATEWIDE POLICY FRAMEWORK 8340 IDENTIFICATION AND AUTHENTICATION

8.2 Statewide Policy Exception Procedure
8.3 Statewide Standard 8340, Identification and Authentication


9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen Arizona State CIO</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all Statutes</td>
<td>1.0</td>
<td>Morgan Reed Arizona State CIO</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State of Arizona CIO and Deputy Director</td>
</tr>
<tr>
<td>5/25/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
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 COMMUNICATION 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 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.

5.5 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.

5.6 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.

5.7 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.

5.8 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.

6.1.3 (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. [NIST 800 53 CM-7] [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

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 confidentiality and integrity of 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 and NIST Computer Security Resource Center websites.

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


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


9. ATTACHMENTS
None

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen, State CIO and Deputy Director</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed, State CIO and Deputy Director</td>
</tr>
<tr>
<td>9/17/18</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State of Arizona CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>
STATEWIDE POLICY (8410): SYSTEM PRIVACY

<table>
<thead>
<tr>
<th>DOCUMENT NUMBER:</th>
<th>(P8410)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFFECTIVE DATE:</td>
<td>May 26, 2021</td>
</tr>
<tr>
<td>REVISION:</td>
<td>3.0</td>
</tr>
</tbody>
</table>

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 8410 SYSTEM PRIVACY.

2. PURPOSE

The purpose of this standard is to provide more detailed guidance for the development of a system privacy notice based on standards, regulations, and best practices.

3. SCOPE

3.1 Application to Budget Units (BUs) - 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:

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Exception</th>
<th>Explanation / Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall: Be ultimately responsible for the correct and thorough completion of Statewide 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 all BU activities and documentation provided to ensure compliance with statewide IT PSPs throughout all state BUs;

b. Review and approve or disapprove all BU security and privacy PSPs and exceptions to existing PSPs; and

c. Identify and convey to the State CIO the risk to Confidential data based on current implementation of privacy controls and mitigation options to improve privacy.
5.3 Enterprise Security Program Advisory Council (ESPAC)
   a. Advise the State CISO on matters related to statewide information security policies and standards.

5.4 State Chief Privacy Officer (CPO) shall:
   a. Advise the State CIO and State CISO on the completeness and adequacy of the BU activities and documentation for data privacy provided to ensure compliance with Statewide Information Technology Privacy PSPs throughout all state BUs;
   b. Review and approve BU privacy PSPs and requested exceptions from the statewide privacy PSPs; and
   c. Identify and convey, to the State CIO and State CISO, the privacy risk to state information systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

5.5 BU Director shall:
   a. Be responsible for the correct and thorough completion of BU PSPs;
   b. Ensure compliance with BU PSPs; and
   c. Promote efforts within the BU to establish and maintain effective privacy controls on BU information systems and premises.

5.6 BU CIO shall:
   a. Work with the BU Director to ensure the correct and thorough completion of BU IT PSPs; and
   b. Ensure BU PSPs are periodically reviewed and updated to reflect changes in requirements.

5.7 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 Privacy Policy for the BU;
   c. Support the agency privacy officers and provide them with adequate information;
   d. Request changes and/or exceptions to existing PSPs from the State CISO; and
e. Ensure all personnel understand their responsibilities with respect to privacy of Confidential data.

5.8 The BU Privacy Officer shall:

a. Advise the State CISO and the State CPO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with privacy laws, regulations, statutes and Statewide IT Privacy PSPs throughout all agency BUs; and

b. Assist the agency to ensure the privacy of sensitive personal information within the agency’s possession.

c. Reviews and approves BU privacy PSPs and requested exceptions from the statewide privacy PSPs; and

d. Identify and convey to the BU CIO the privacy risk to agency information systems and data based on current implementation of privacy controls and mitigation options to improve privacy.

5.9 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on BU PSPs; and

b. Monitor employee activities to ensure compliance.

5.10 System Users of agency information systems shall:

a. Become familiar with this policy and related PSPs; and

b. Adhere to PSPs regarding system privacy.

6. STATEWIDE POLICY

6.1 Authority to Collect - The BU shall determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or agency information system need. For additional specificity on the authority to collect, refer to Standard 8330, System Security Audit. [NIST 800 53 AP-1] [Privacy Acts] [HIPAA 164.520(a)(1)]

6.2 Purpose Specification - The BU shall describe the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. [NIST 800 53 AP-2] [HIPAA 164.520(a)(1)] [ARS 41-4152]

6.3 Access Enforcement - The BU shall ensure the agency information system enforces approved authorizations for logical access to PII in accordance with applicable control policies (e.g., identity-based policies, role-based policies). [NIST 800-53 AC-3]
6.4 **Least Privilege** - The BU shall employ the concept of least privilege, allowing only authorized accesses to PII for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. [NIST 800-53 AC-6]

6.5 **Governance and Privacy Program** - The BU shall: [NIST 800 53 AR-1]

   a. Appoint a Senior BU official for Privacy accountable for developing, implementing, and maintaining an organization wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and agency information systems; [HIPAA 164.530(a)(1)] [EO 2008-10]

   b. Monitor federal and state privacy laws for changes that affect the privacy program;

   c. Allocate resources to implement and operate the organization-wide privacy program;

   d. Develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;

   e. Develop, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for program, agency information systems, or technologies involving PII; and

   f. Update privacy plan, policies, and procedures annually.

6.6 **Privacy Impact and Risk Assessment** - The BU shall: [NIST 800 53 AR-2]

   a. Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII;

   b. Conduct Privacy Impact Assessments (PIAs) for agency information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, policy, or any existing BU policies and procedures; and

   c. Ensure PIAs are conducted prior to any new collection of PII or upon significant changes in the architecture, information flow, or use of PII within existing systems.

6.7 **Privacy Requirements for Contractors and Service Providers** - The BU shall: [NIST 800 53 AR-3]

   a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and
b. Include privacy requirements in contracts and other acquisition-related documents.

6.8 **Privacy Monitoring and Auditing** - The BU shall monitor and audit privacy controls and internal privacy policy annually to ensure effective implementations. [NIST 800 53 AR-4]

6.9 **Privacy Awareness and Training** - The BU shall: [NIST 800 53 AR-5]

   a. Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that agency employees and contractors understand privacy responsibilities and procedures;

   b. Administer basic privacy training annually and targeted, role-based privacy training for agency employees and contractors having responsibility for PII or for activities that involve PII annually;

   c. (P) Privacy Training – All individuals responsible for handling consumer inquiries about the BU’s privacy practices or the BU’s compliance with privacy regulations shall be informed of all the requirements in these regulations and how to direct consumers to exercise their rights under these regulations.

   d. Ensure that agency employees and contractors certify (manually or electronically) acceptance of responsibilities for privacy requirements annually.

6.10 **Privacy Reporting** - The BU shall conduct an initial evaluation, develop, disseminate, and establish and follow a schedule for regularly updating as necessary, but at least every three years, reports to the State Privacy Officer (SPO) and other appropriate oversight bodies to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance. [NIST 800 53 AR-6]

6.11 **Privacy-Enhanced System Design and Development** - The BU shall design agency information systems to support privacy by automating privacy controls. [NIST 800 53 AR-7]

6.12 **Accounting of Disclosures** - The BU, consistent with state privacy acts and subject to any applicable exceptions or exemptions, shall: [NIST 800 53 AR-8] [HIPAA 164.528(a)]

   a. Keep an accurate accounting of disclosures of information held in each system of records under its control, including:

      1. Date, nature, and purpose of each disclosure of a record

      2. Name and address of the person or agency to which the disclosure was made
b. Retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer or as required by law. However, all State BUs must comply with Arizona State Library, Archives and Public Records rules and implement whichever retention period is most rigorous, binding or exacting. Refer to: http://apps.azlibrary.gov/records/general_rs/Information%20Technology%20(IT).pdf Item 10a. and b.

Data Quality - The BU shall: [NIST 800 53 DL-1]

1. Confirm to the greatest extent possible upon collection or creation of PII, the accuracy, relevance, timeliness, and completeness of that information;
2. Collect PII directly from the individual to the greatest extent practicable;
3. Check for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems annually; and
4. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

6.13 Data Integrity - The BU shall: [NIST 800 53 DI-2]

a. Document processes to ensure the integrity of PII through existing security controls.

6.14 Minimization of Personally Identifiable Information - The BU shall: [NIST 800 53 DM-1]

a. Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

b. Limit the collections and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

c. Conduct an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings at least every three years and update as necessary to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

6.15 Data Retention and Disposal - The BU shall: [NIST 800 53 DM-2]

a. Retain each collection of PII for BU-defined time period to fulfill the purposes identified in the notice or as required by law, refer to Policy DRAFT, Document Retention;
b. Dispose of, destroy, erases, and/or anonymize the PII, regardless of the method of storage, in accordance with an Arizona State Library-approved record retention schedules and in a manner that prevents loss, theft, misuse, or unauthorized access; and [ARS 44-7601] [ARS 41-151.12]

c. Use techniques, documented in the Policy 8250, Media Protection, to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

6.16 Consent - For collection, use, and disclosures of PII not already authorized by law the BU shall: [NIST 800 53 IP-1]

   a. Provide means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to its collection; [HIPAA 164.522(a)(1)]

   b. Provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

   c. Obtain consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII;

   d. Ensure that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

6.17 Individual Access - The BU, consistent with the laws and regulations, and subject to any applicable exceptions or exemptions, shall: [NIST 800 53 IP-2] HIPAA 164.524(a)]

   a. Provide individuals the ability to have access to their PII maintained in its system(s) of records;

   b. Publish rules and regulations governing how individuals may request access to records maintained in a system of records; and [HIPAA 164.524(b),(c),(d)]

   c. Adhere to requirements and policies and guidance for the proper processing of PII requests.

6.18 Redress - For collection, use, and disclosures of PII not already authorized by law the BU shall: [NIST 800 53 IP-3] [HIPAA 164.526(a)-(f)]

   a. Provide a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate; and

   b. Establish a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information sharing partners and, where feasible and appropriate, notifies affected individuals.
6.19 **Complaint Management** - For collection, use, and disclosures of PII not already authorized by law the BU shall implement a process for receiving and responding to complaints, concerns, or questions from individuals about the BU privacy practices. [NIST 800 53 IP-4] [HIPAA 164.530(d)]

6.20 **Inventory of PII** - The BU Privacy Officer shall: [NIST 800 53 SE-1]

   a. Establish, maintain, and update at least every three years an inventory that contains a listing of all programs and BU information systems identified as collecting, using, maintaining, or sharing PII; and

   b. Provide each update of the PII use to the BU CIO or BU ISO at least every three years to support the establishment of information security requirements for all new or modified BU information systems containing PII.

6.21 **Privacy Incident Response** - The BU shall: [NIST 800 53 SE-2]

   a. Develop and implement a Privacy Incident Response Plan consistent with requirements in STATEWIDE POLICY FRAMEWORK 8240 Incident Response Planning; and

   b. Provide an organized and effective response to privacy incidents in accordance with the BU Privacy Incident Response Plan.

6.22 **Privacy Notice** - The following guidance is offered for the development of a Privacy Notice: [NIST 800 53 TR-1] [HIPAA 164.520(c)] [ARS 41-4152]

   a. Provides effective notice to the public and to individuals regarding:

   b. Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of PII;

   c. Authority for collection PII;

   d. The choices, if any, individuals may have regarding how the BU uses PII and the consequences of exercising or not exercising those choices;

   e. The ability to access and have PII amended or corrected if necessary;

   f. Describes the following:

      How the PII the BU collects and the purpose(s) for which it collects that information;

      How the BU uses PII internally;

      1. Whether the BU shares PII with external entities, the categories of those entities, and the purposes for such sharing;

      2. Whether individuals have the ability to consent to specific uses of sharing of PII and how to exercise any such consent;
3. How individuals may obtain access to PII; and
4. How the PII will be protected.

g. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change; and

h. Provides notice in clear and conspicuous language when individuals are first asked to provide PII to the BU.

6.23 Dissemination of Privacy Program Information - The BU shall: [NIST 800 53 TR-3]

a. Ensure the public has access to information about its privacy notice and is able to communicate with its Privacy Officer; and

b. Ensure that its privacy notice are publicly available through BU websites or publicly facing email addresses and/or phone lines that enable the public to provide feedback and/or direct questions to privacy offices regarding privacy notice.

6.24 Internal Use - The BU shall use PII internally only as authorized by law or for the authorized purpose(s) described in privacy notice. [NIST 800 53 UL-1]

6.25 Information Sharing with Third Parties - The BU shall: [NIST 800 53 UL-2] [HIPAA 164.508(a)]

a. Share PII externally, only as authorized by law or for the authorized purposes identified and described in privacy notice or in a manner compatible with those purposes;

b. Where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, Service Level Agreements, Business Associate Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used and offers the same level of protection as documented in this policy; [HIPAA 164.514(e)(4)]

c. Monitor, audit, and train its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use of sharing of PII; and

d. Evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new privacy notice is required.
7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET and NIST Computer Security Resource Center websites.

8. REFERENCES

8.1 STATEWIDE POLICY FRAMEWORK 8410 SYSTEM PRIVACY
8.2 Statewide Policy Exception Procedure
8.3 STATEWIDE POLICY FRAMEWORK 8250, Media Protection
8.4 STATEWIDE POLICY FRAMEWORK 8240, Incident Response Planning
8.5 Policy (DRAFT), Document Retention
8.6 Statewide Standard 8330, System Security Audit
8.8 Executive Order 2008-10: Mitigating Cyber Security Threats
8.9 Arizona Revised Statue; Title 12: Courts and Civil Proceedings; Article 7.1 Medical Records; Section 12-2297: Retention of records
8.10 Arizona Revised Statutes; Title 41: State Government; Chapter 1: Executive Officers; Article 2.1: Arizona State Library, Archives and Public Records Established in the Office of the Secretary of State; Section 41-151.12; Records; records management; powers and duties of director; fees; records services fund
8.11 Arizona Revised Statutes; Title 41: State Government; Chapter 39: Information Obtained or Disseminated by State and Local Governments; Article 1: Access to State Agency Web Site Records and Privacy; Section 41-4152.
8.12 Arizona Revised Statutes; Title 41: State Government; Chapter 41: Arizona Department of Homeland Security; Article 1: General Provisions; Section 41-4172: Anti-identification procedures.
8.13 Arizona Revised Statutes; Title 44: Trade and Commerce; Chapter 33: Record Discard and Disposal; Article 1: Discard and Disposal of Personal Identifying Information Records;
Section 44-7601: Discarding and disposing of records containing personal identifying information; civil penalty; enforcement; definition.

8.14 General Records Retention Schedule for All Public Bodies, Information Technology (IT) Records, Schedule Number 000-12-41, Arizona State Library, Archives and Public Records, Item Numbers 10 a and b

9. ATTACHMENTS

None.

10. REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Revision</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/01/2014</td>
<td>Initial Release</td>
<td>Draft</td>
<td>Aaron Sandeen Arizona State CIO</td>
</tr>
<tr>
<td>10/11/2016</td>
<td>Updated all the Security Statutes</td>
<td>1.0</td>
<td>Morgan Reed Arizona State CIO</td>
</tr>
<tr>
<td>9/17/2018</td>
<td>Updated for PCI-DSS 3.2.1</td>
<td>2.0</td>
<td>Morgan Reed, State of Arizona CIO and Deputy Director</td>
</tr>
<tr>
<td>5/26/21</td>
<td>Annual Updates</td>
<td>3.0</td>
<td>Tim Roemer, Director of Arizona Department of Homeland Security &amp; State Chief Information Security Officer</td>
</tr>
</tbody>
</table>