	STATEWIDE **POLICY**	**State of Arizona**

STATEWIDE POLICY (8120): INFORMATION SECURITY PROGRAM

DOCUMENT NUMBER:	**P8120**
EFFECTIVE DATE:	**JANUARY 30, 2025**
REVISION:	**5.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Homeland Security, the Agency shall establish a coordinated plan and program for information security and privacy protections implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.) § 41-4254 and § 41-4282.

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. CONTROL SELECTION AND EXCEPTIONS

4.1 The Statewide Policies, Standards, and Procedures (PSPs) implement a control baseline for Standard and Protected state systems. By issuing the BU's own set of PSPs (based on the Statewide PSP Templates) the BU shall select a control baseline for their systems. [NIST 800-53 PL-10].

4.2 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure. This is the process of tailoring the control baseline and may be applied BU-wide or to specific BU-identified systems provided the exceptions are approved. [NIST 800-53 PL-11].

4.2.1 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.

4.2.2 IT Products and Services Procurement

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

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

Section Number	Exception	Rationale

5. ROLES AND RESPONSIBILITIES

5.1 Arizona Department of Homeland Security Director shall:

- **a.** Be ultimately responsible for the correct and thorough completion of information security PSPs throughout all state BUs.
- **b.** Ensure that by July 1 of each year all BUs have submitted the following information for approval:
  - **i.** A state information system inventory with a system classification assignment and system owner for each state information system
  - **ii.** A system security plan and system security assessment plan for each Protected state information system
  - **iii.** 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.
- **d.** Enforce a course of action where security risks are not adequately addressed. Course of action may include, but is not limited to, the following mandates:
  - **i.** Identification of a plan to address the documented risks
  - **ii.** Implementation of recommended security controls
  - **iii.** Independent security assessment on selected state information systems or controls
  - **iv.** Hosting of state system or state information system components in a state approved solution(s)
  - **v.** Adoption of additional security requirements or procedures for the BU or selected by state systems, controls, or control environments

5.2 State Chief Information Security Officer (CISO) shall:

- **a.** Provide a format for the required compliance documents;
- **b.** Advise the Director on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with statewide information security 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 Director 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:

i. Identify a plan to address the documented risks
ii. Implement recommended security controls
iii. Perform independent security assessment on selected state information systems or controls
iv. Hosting of state information system or state information system components in a state approved solution(s)
v. Adopt any additional security requirements or procedures for the BU or selected by state systems, controls, or control environments

5.3 Enterprise Security Program Advisory Council (ESPAC) shall:

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:

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

b. Ensure BU compliance with Information Security Program 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 security 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:

i. A complete list of information systems with a system classification assignment and system owner for each agency information system
ii. A system security plan and system security assessment plan for each protected agency information system

iii. 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 delegate 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:

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. Identify the individuals that fulfill system roles and responsibilities;

e. Identify the information types processed, stored, and transmitted by their system;

f. Provide the security categorization of the information system, including supporting rationale;

g. Describe any specific threats to the system that are of concern to the BU;

h. Provide the results of a privacy risk assessment for systems processing personally identifiable information;

i. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

j. Provide an overview of the security and privacy requirements for the system;

k. Identify any relevant control baselines or overlays, if applicable;

l. Describe the controls in place or planned for meeting the security and privacy requirements including rationale for any tailoring decisions;

m. Include risk determinations for security and privacy architecture and design decisions;

n. Include security and privacy related activities affecting the system that require planning and coordination with the BU CIO, BU ISO, and system owners of affected agency information systems; and [IRS Pub 1075]

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

6.1.2 (P) **Security and Privacy Architecture** – The BU shall: [NIST 800-53 PL-8][IRS Pub 1075]

a. Develop a security and privacy architecture for the agency information system that describes:

i. The requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

ii. How the architectures are integrated into and support the enterprise architecture;

iii. Any assumptions about, and dependencies on external systems and services;

b. Annually, review and update the architectures to reflect updates in the enterprise architecture; and

c. Reflect planned architecture changes in the security and privacy plans and organizational procedures, and procurements and acquisitions.

6.2 System Security Policies – The BU shall develop security, privacy, and supply chain management risk policies and procedures to address the associated risk with the operation and use of agency information systems and the authorized processing of personally identifiable information. These policies and procedures shall include the following:

a. Data Classification Policy and Procedures (P8110)

b. Information Security Program Policy and Procedures, including security, privacy, and supply chain risk management (P8120)
[NIST 800-53 CA-1] [NIST 800-53 PL-1] [NIST 800-53 PM-1] [NIST 800-53 RA-1][SR-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]

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

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

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

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

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

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

j. Acceptable Use Policy, including social media, networking restrictions, restrictions on posting on public websites, and use of organizational identifiers (P8280) [NIST 800 53 AC-1] [NIST SP 800 53 PL-4a, PL-4(1)]

k. Account Management Policy and Procedures (P8310)

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

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

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

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

p. System Privacy Policy and Procedures (P8410)

q. System Privacy Notice (S8410)

6.2.1 Policy Development, Maintenance, and Distribution – The BU shall: [HIPAA 164.316 (a), (b)(1), (b)(2)] [PCI DSS 12.1.1]

a. Designate an agency official to develop, document and disseminate , to appropriate personnel and roles, the policies and procedures for each agency information system;

b. Maintain the organizational security policies and procedures;

c. These policies shall be consistent with applicable laws, directives, regulations, policies, standards, and guidelines;

d. 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 https://apps.azlibrary.gov/records/general_rs/GS%201018%20Rev.5.pdf;

e. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains; and

f. Review documentation at least annually, and update as needed, in response to environmental or operational changes affecting the security of the confidential information.

6.3 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:

- **i.** 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;
- **ii.** Result in minor damage to organizational assets;
- **iii.** Result in a minor financial loss; or
- **iv.** 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:

- **i.** 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;
- **ii.** Result in significant damage to organizational assets;
- **iii.** Result in a significant financial loss; or
- **iv.** 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 Categorization – The BU shall categorize agency information systems and the information it processes, stores, and transmits, document the security categorization results (including supporting rationale) in the security plan for the agency information system; and verify 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 its 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 Risk Assessment - The BU shall: [NIST 800-53 RA-3] [HIPAA 164.308 (a)(1)(ii)(A)]

a. Conduct an assessment of security and privacy risk, including identification of threats to the system, vulnerabilities present in the system, the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the agency information system, the information it processes, stores, or transmits, and any related information;

i. Determine the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

ii. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

iii. Perform and document 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];

iv. Review risk assessment results annually;

v. Disseminate risk assessment results to the BU CIO, BU ISO, agency information system owner, and other BU-defined personnel or roles; and

b. Conduct an assessment of supply chain risks associated with BU systems, system components, and system services. The supply chain risk assessment shall be updated annually, when there are significant changes to the supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain. [NIST 800-53 RA-3(1)].

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][SR-1]

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)] [PCI DSS 12.8.3]

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.** Monitor and 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:
  - **i.** Enumerating platforms, software flaws, and improper configurations;
  - **ii.** Formatting checklists and test procedures; and
  - **iii.** Measuring vulnerability impact.
- **e.** Analyze vulnerability scan reports and results from vulnerability monitoring;
- **f.** Remediate legitimate vulnerabilities within 30 days in accordance with an organization assessment of risk;
- **g.** Share information obtained from the vulnerability monitoring process and 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.** Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components; [NIST 800-53 RA-5(11)];
- **i.** (P) Establish a process to identify and assign risk ranking to newly discovered security vulnerabilities; [PCI DSS 11.2]
- **j.** (P) Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved according to vulnerability ranking. [PCI DSS 11.2.1]
  - **i.** (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] [IRS Pub 1075]

ii. (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]

iii. (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]

iv. (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 information security, privacy, and supply chain risk management programs and associated agency information systems are:

i. Developed and maintained

ii. Reported in accordance with reporting requirements

iii. Documented with the remedial information security, privacy, and supply chain management 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 System Inventory - The BU shall develop and annually update 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 Measures of Performance - The BU shall develop, monitor, and report on the results of information security and privacy measures of performance. [NIST 800-53 PM-6]

6.4.6 Enterprise Architecture - The BU shall develop and maintain an enterprise architecture with consideration for information security, privacy, 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 and privacy 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 security risk to organizational operations and assets, individuals, other organizations, and the agency associated with the operation and use of agency information systems; privacy risk to individuals resulting from the authorized processing of personally identifiable information;

b. Implement this strategy consistently across the organization; and

c. Review and update the risk management strategy annually or as required to address organizational changes.[NIST 800-53 PM-9]

6.4.9 Supply Chain Risk Management Strategy - The BU shall: [NIST 800-53 SR-2]

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the systems, system components, or system services;

b. Review and update the supply chain risk management plan annually or as required to address threat, organizational, or environmental changes;

c. Protect the supply chain risk management plan from unauthorized disclosure and modification;

d. Establish a supply chain risk management team to lead and support the supply chain risk management activities. [NIST 800-53 SR-2(1)]

e. Implement supply chain risk management controls and processes, including: [NIST 800-53 SR-3]

- **i.** Establishing a process(es) to identify and address weaknesses or deficiencies in the key supply chain elements and processes in coordination with supply chain personnel;
- **ii.** Employing adequate controls to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related event; and
- **iii.** Documenting the selected and implemented supply chain processes and controls in the supply chain risk management plan;

f. Employ appropriate acquisition strategies, contract tool, and procurement methods to protect against, identify, and mitigate supply chain risks; [NIST 800-53 SR-5];

g. Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide; [NIST 800-53 SR-6]

h. Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises and results of assessments or audits; [NIST 800-53 SR-8]

i. Inspect the appropriate systems or system components randomly but at sufficient frequency to adequately detect tampering [NIST 800-53 SR-10];

j. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and report counterfeit system components to the source of the counterfeit component and the State CISO. The BU shall: [NIST 800-53 SR-11]

- **i.** Train appropriate personnel to detect counterfeit system components (including hardware, software, and firmware); [NIST 800-53 SR-11(1)]
- **ii.** Maintain configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service. [NIST 800-53 SR-11(2)]

k. Dispose of system components using the approved techniques and methods that ensure the sanitization of sensitive data. [NIST 800-53 SR-12]

6.4.10 Risk Response - The BU shall respond to findings from security and privacy assessments, monitoring, and audits in accordance with BU-defined risk tolerance. [NIST 800-53 RA-7]

6.4.11 Privacy Impact Assessments - The BU shall conduct privacy impact assessments for systems, programs, or other activities before developing or procuring information technology that processes personally identifiable information and before initiating a new collection of personally identifiable information that will be processed using information technology and includes personally identifiable information permitting the physical or virtual (online) contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more individuals, other than BUs or state employees. [NIST 800-53 RA-8]

6.4.12 Criticality Analysis - The BU shall identify critical system components and functions by performing a criticality analysis for BU systems, system components, and system services when the system is being designed, modified, or upgraded. [NIST 800-53 RA-9]

6.4.13 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 integrate the security authorization processes into an BU-wide risk management program.

6.4.14 Mission/Business Process Definition - The BU shall: [NIST 800-53 PM-11]

a. Define mission/business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the agency; and

b. Determine information protection needs and personally identifiable information processing needs arising from the defined mission/business processes; and

c. Revise the process as necessary, until achievable protection needs are obtained.

6.4.15 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]

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

6.4.17 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.

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

6.5.1 Control Assessments – The BU shall: [NIST 800-53 CA-2] [HIPAA 164.308 (a)(8)] [PCI DSS 12.4.2] [PCI DSS 12.4.2.1] Develop a control (e.g., security and privacy controls) 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;

a. Assess the controls in the information system and its environment of operation quarterly 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;

b. Produce a control assessment report that documents the results of the assessment; and

c. Provide the results of the control assessment to the BU CIO, BU CSO, BU Privacy Officer, State Privacy Officer, and the State CSO.

6.5.2 (P) Independent Assessors - The BU shall employ impartial assessors or assessment teams to conduct 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; information exchange agreements; memorandum of understanding or agreement; service level agreement; user agreements; or nondisclosure agreements;

b. Document, for each interconnection, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update agreements annually:

i. (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 at managed interfaces. [NIST 800-53 SC-7(5)] [IRS Pub 1075]

ii. (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)][PCI DSS 12.9.1, 12.9.2]

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

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

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]

Assign a senior official the authorizing official for the information system and accepting common controls inherited by Statewide or other organizational systems;

Ensure the authorizing official authorizes the agency information system for processing and accepts the inherited common controls before commencing operations; and

Update the security authorization every three years.

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

- **a.** Establishment of system-level 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 system-level 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;
- **h.** Employs independent assessors or assessment teams to monitor the controls in the system on an ongoing basis; [NIST 800-53 CA-7(1)]; and
- **i.** Ensures risk monitoring is an integral part of the continuous monitoring strategy that includes effectiveness, compliance, and change monitoring. [NIST 800-53 CM-7(4)].

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, facsimile machines, sensors, and servers) to the agency information system and, for each internal connection, shall document the interface characteristics, security and privacy requirements and the nature of the information communicated. The BU shall terminate internal system connections after the need for such connections is no longer required and shall review these connections annually. [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, known to all affected parties, and any remediation actions taken are documented. [PCI DSS 11.6] [PCI DSS 12.4.2] [PCI DSS 12.4.2.1]

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 National Institute of Standards and Technology, Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, September 2020.

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

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

8.6 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2021.

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

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 of Arizona CIO and Deputy Director**
5/26/2021	**Annual Updates**	**3.0**	**Tim Roemer, Director of Arizona Department of Homeland Security & State Chief Information Security Officer**

1/16/2024	**Annual Updates**	**4.0**	**Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**
1/30/2025 **2/11/2025**	**Annual Updates**	**5.0**	**Errika Celsy, Chief Privacy and Compliance Officer;** **Ryan Murray, Deputy Director Department of Homeland Security & State Chief Information Security Officer**