ARIZONA STATEWIDE SECURITY STANDARDS	STATEWIDE STANDARD	State of Arizona

STANDARD 8120: INFORMATION SECURITY PROGRAM STANDARD

DOCUMENT NUMBER:	S8120
EFFECTIVE DATE:	JULY 1, 2015
REVISION:	DRAFT

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.

2. PURPOSE

The purpose of this standard is to provide additional specificity to the associated policy requirements.

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 state information systems. Policy statements preceded by "(P)" are required for state information systems categorized as Protected. Categorization of systems is defined within the Information Security Program Policy.

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 ADOA Policy Exception Procedure.

   4.1.1 Existing IT Products and Services

   a. ADOA 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 ADOA Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

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

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.

    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:

        1. Identification of a plan to address the documented risks
        2. Implementation of recommended security controls
        3. 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. Adoption of additional security requirements or procedures for the BU or selected BU state information 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 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 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 BU Director shall:

a. Be responsible for the correct and thorough completion of Statewide Information Technology 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 state information systems and assets.

5.4 BU Chief Information Officer (CIO) shall:

a. Work with the BU Director to ensure the correct and thorough completion of Statewide 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 state information systems 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 information security risks to Protected state information systems, are adequately addressed according to the Protected state information system risk assessment documentation; and

    d. Be system owner for all state information systems or delegates a system owner for BU state information system.

5.5 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 state information systems; and

    c. Ensure the correct execution of the system security assessment plans.

5.6 System Owner shall:

    a. Be responsible for the overall procurement, development, integration, modification, or operation and maintenance of the state information system; [NIST SP 800-18]

    b. Advise BU ISO as to the state 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 STANDARD

6.1 **System Security Plan Template** - The following template may be used to create a state system security plan.

    6.1.1 **State System Name/Title:** Unique identifier and name of the state information system.

6.1.2 **State System Categorization**: [Assign a single system categorization to the identified state information system according to the requirements in the Information Security Program Policy (P8120), requirements 6.3.1 – 6.3.3.]

   a. Standard; or

   b. Protected

6.1.3 **Information System Owner:** [Assign an owner to the identified state information system. An owner must be a state employee and has the overall responsibility for procurement, development, integration, modification, or operation and maintenance of the state information system.]

6.1.4 **Authorizing Official**: [Document the authorizing official for the state information system. An authorizing official has the authority to formally assume responsibility for operating the state information system at an acceptable level of risk to BU operations or assets.]

	State Information System Owner	Authorizing Official
Name		
Title		
Agency		
Address		
Email Address		
Phone Number		

6.1.5 **Other Designated Contacts:** [List the other key personnel associated with the operations and maintenance of the state information system.]

6.1.6 **Assignment of Security Responsibility**: [List the personnel assigned to security responsibilities with the state information system.]

	1	2
Name		
Title		
Agency		
Address		
Email Address		
Phone Number		

6.1.7 **State Information System Operational Status**: [Indicate the current operational status of the state information system. If required, indicate specific parts or subsystems of the state information system if more than one status is selected.]

	System Name	Subsystem Name (use if needed)
☐ Operational		
☐ Under Development		
☐ Major Modification		

6.1.8 **Information System Type***:* [Indicate the type of system: Major Application – An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application; or General Support System – An interconnected set of information resources under the same direct management control that shares common functionality (including hardware, software, information, data, minor applications, communications, and people).]

6.1.9 **General System Description / Purpose***:* [Describe the function or purpose of the system and the information processes.]

6.1.10 **System Environment***:* [Provide a general technical description of the sate information system. Include hardware, software, and communications equipment.]

6.1.11 **System Interconnections / Information Sharing: [List interconnected systems and system identifiers***,* indicate if there is an agreement on file (e.g., Information Sharing Agreement, Memorandum of Understanding, Service Level Agreement, or other agreement), date of agreement, and name of authorizing official.]

System Name	Business Unit	Type	Agreement	Date	Official

6.1.12 **Related Laws / Regulations / Policies:** [List any laws or regulations that establish specific security or privacy requirements for the state information system or data residing on the system. State PSPs may be used for guidance but only include relevant and applicable laws and regulations.]

6.1.13 Minimum Security Control Exceptions: *[Minimum Security Controls are based on the categorization of the system and the statewide security and privacy policy set.* List any exceptions with the statewide security and privacy policies below or planned controls (e.g., controls not yet in place but budgeted and planned, together with rationale, compensating controls for the exception, and expected date of implementation for planned controls.]

Policy #	Policy Name	Exceptions	Compensating Controls	Rationale for Exception
P8110	Data Classification	[None / List Exceptions]		
P8120	Information Security Program	[None / List Exceptions]		
P8130	System Security Acquisition	[None / List Exceptions]		
P8210	Security Awareness Training	[None / List Exceptions]		
P8220	System security Maintenance	[None / List Exceptions]		
P8230	Contingency Planning	[None / List Exceptions]		
P8240	Incident Response Planning	[None / List Exceptions]		
P8250	Media Protection Policy	[None / List Exceptions]		
P8260	Physical Protections	[None / List Exceptions]		
P8270	Personnel Security Controls	[None / List Exceptions]		
P8280	Acceptable Use	[None / List Exceptions]		
P8310	Account Management	[None / List Exceptions]		
P8320	Access Control	[None / List Exceptions]		
P8330	System Security Audit	[None / List Exceptions]		
P8340	Identification and Authentication	[None / List Exceptions]		
P8350	System and Communication Protection	[None / List Exceptions]		
P8410	System Privacy	[None / List Exceptions]		

6.1.14 State Information System Security Plan Dates: *[List completion date of plan, approval date of plan, along with* approver.]

	Security Plan Completion	Security Plan Approval
Name		
Title		
Date		

6.2 **Security Risk Assessment Guidance** – The following guidance is provided for the performance of information security risk assessments. This guidance is presented within the context of the phases of an information security risk assessment process. Namely, the preparation, the performance, and the communication of the results for an information security risk assessment.

6.2.1 **Information Security Risk Assessment Preparation**. Preparation for an information security risk assessment helps to ensure that the business unit derives the most value from this exercise and establishes the context of the risk management process. Business units shall consider the following steps in preparing for an information security risk assessment.

a. Identify Purpose. The obvious purpose for an information security risk assessment is to provide information to the system owners regarding the risk to sensitive data and critical systems so that they may make appropriate decisions regarding how to address those risks. However, information security risk assessments are also required periodically based on applicable regulations, provide oversight to the security operations of the system, or could be the direct (and required) action from a recent audit or inspection. It is important that the business unit clearly understand and identify the purpose of the information security risk assessment and convey that to the team performing and overseeing the assessment in order to ensure project success.

b. Define Assessment Boundaries. An information security risk assessment shall be limited to defined physical and logical boundaries. A physical boundary identifies the physical limit of the assessment such as network components (e.g., workstations, servers, routers, switches), security components (e.g., IDS, firewalls), network media (e.g., cabling), peripherals, buildings, and rooms. A logical boundary identifies the logical limit of the assessment such as the functions of the system, services provided, applications, and network segments.

c. Define Level of Rigor. An information security risk assessment shall have a defined level of rigor specifying the depth of analysis to be performed. The level of rigor may be specified by hours (or other resources metrics) to be expended, or by listing the methods of data gathering.

d. Document Scope Limitations and Constraints. An information security risk assessment is generally expected to cover all relevant administrative, technical, and physical controls. When the scope is limited or constraints are placed on the task of assessing the risk to the state information system the budget unit needs to ensure that these constraints are reasonable. If a budget unit chooses to limit the scope of the risk assessment (e.g., physical security controls are out of scope) then there should be some rationale provided on why such a limitation is reasonable (e.g., physical security controls are reviewed under another assessment program).

e. Document Risk Model. There are a variety of reasonable security risk models that may be used in the performance of an information security risk assessment (e.g., NIST 800-30). The budget unit (or the contractor for the budget unit) may use any reasonable security risk model provided the model accounts for the following aspects of a baseline information security risk assessment:

f. Document Risk Elements. The information security risk model shall identify and document the elements to be reviewed, assessed, and analyzed in order to determine the risk to the state information system. These elements typically include: threats, assets, vulnerabilities, likelihood, and impact.

g. Document Risk Calculation. The information security risk model shall identify the process by which risk is determined. This is typically in the form of a risk calculation, estimate based on parameters, or a risk determination table based on the risk elements listed above.

6.2.2 **Information Security Risk Assessment Performance**. The effective performance of an information security risk assessment is critical to the accuracy and usefulness of the assessment. Business units shall consider the following steps in the performance of an information security risk assessment.

a. Objectivity. Consistent with requirement 6.5.1.1 of P8120 (Information Security Program Policy), an information security risk assessment shall be performed by impartial assessors or assessment teams. Impartiality requires that the assessment team have no conflict of interest between the development, selection, and/or operation of the security controls under assessment.

b. Adequate Data Gathering. An information security risk assessment shall have adequate data gathered on the controls within the physical and logical boundaries of the assessment. Adequacy of the data gathering is largely subjective but BUs shall be hesitant to rely on information security risk assessments that have too few data points to

draw an accurate conclusion or assessments that rely on interviews of surveys alone from those in charge of the assessed controls. To the extent possible the BU should ensure that effective data gathering approaches from reviewing documents, interviewing personnel, observing behavior, inspecting controls, and testing controls are utilized.

c. Defendable Analysis. An information security risk assessment shall include a documented and defendable analysis of the data gathered to support findings. Information security risk assessments typically provide such analysis in the form of tables or charts. Each finding / recommendation shall be traceable to sufficient evidence of the vulnerability that is being addressed.

6.2.3 **Information Security Risk Assessment Documentation**. The effective and accurate communication of results from of an information security risk assessment is critical to the usefulness of the assessment. Business units shall consider the following steps in the documentation of an information security risk assessment.

a. Communication with Key Staff. The results of an information security risk assessment provide pertinent information and guidance to system owners, information security officers, and chief information officers within the budget unit. The results of the assessment shall be shared with budget unit director, CIO, information security officer, and system owners at a minimum. The state CISO may also be included in the dissemination of the assessment results.

b. Communication with Custodians and Others. The results of the information security risk assessment includes recommendations for improvements (e.g., patch systems, develop procedures, implement additional controls) that will need to be conveyed to those in charge of implementing these changes. When relevant, all available evidence of the associated vulnerabilities and details of the recommended solutions shall be made available to the system custodians, staff members, or contractors tasked with confirming the vulnerability and/or implementing the recommended solution. Keep in mind that the principle of least privilege shall be applied here and there may be some details deemed irrelevant and sensitive and therefore not conveyed to others.

c. Clear Recommendations. An information security risk assessment shall provide a report with clear recommendations that identify the control gap or risk and the recommended solution or solution set to address the control gap or risk. Business units may want to require that the

information security risk assessment recommendations provide information on the cost of the recommendation as well.

6.2.4 Vulnerability Scanning – Vulnerability scanning should be performed continuously using an industry standard automated tool. Results should be documented. Vulnerabilities should be remediated timely and retested to insure that potential risks have been mitigated.

6.3 Plan of Actions and Milestones Guidance - The following guidance is provided for the implementation and management of the state information system plan of actions and milestones (POAM) document.

6.3.1 POAM Overview. The POAM (aka POA&M) is a document designed to assist in the management of identified weaknesses in the state information system. The POAM document identifies known weaknesses (or compliance gaps) and lists the tasks necessary to mitigate these weaknesses. The documentation of these tasks together with an assignment of dates and resources provides system owners and other key personnel with the necessary information to manage the risk to the state information system.

6.3.2 Use of POAM for System Funding. The information regarding system weaknesses and mitigation tasks contained in the POAM is useful in the justification for system funding. The following guidance is provided to assist in making the POAM most useful for system funding assistance.

    a. Link POAM with Investment Planning. Any requests or analysis for funding to support the state information system should be consistent with the POAM and the identified tasks within.

    b. Include Resources Required. The POAM should include information and estimations for resources required to complete the tasks associated with identified weaknesses. These resource estimates should include staff levels and / or funding required and include an indication as to the frequency by which such funding will be required (e.g., quarterly, full-time, every other year).

    c. Integrate Security Assessment Efforts. The POAM is typically the result of a system security plan, however, many other assessment effort may identify weaknesses in the state information system and should integrate with the POAM. Assessments such as IG audits, self-assessments, information security risk assessments, and penetration testing may result in the identification of system weaknesses. The POAM process should be utilized as a single source to track and manage system weaknesses. It is important to include a reference for the source of the weakness identification in an integrated POAM.

d. Prioritize Mitigation Efforts. The POAM may list may system weaknesses which may be beyond the current funding initiatives. It is important to carefully consider the prioritization of the weaknesses and their associated mitigation tasks to ensure state resources are properly utilized. Prioritization of these tasks should consider relevant criteria when prioritizing such as current integrated tasks, system development lifecycles, cost considerations, effectiveness of the proposed tasks, the perceived impact of the weakness, and the effort / time required to implement the mitigation tasks.

e. Assign Dates and Responsible Parties. Each mitigation task should have an assigned date of estimated completion and a responsible party (or point of contact) for the implementation of the task.

f. Monitor and Report POAM Activity. The weaknesses, mitigation tasks, and progress made should be maintained quarterly in the POAM and reported to appropriate BU staff members such as the BU CIO and BU Information Security Officer. The following metrics are useful in monitoring and reporting POAM activity:

g. Total number of weaknesses identified at the start of the quarter;

h. Number of weaknesses for which corrective action was completed on time by end of the quarter;

i. Number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled;

j. Number of weaknesses for which corrective action has been delayed, including explanation for delay; and

k. Number of new weaknesses discovered following the last POAM update and brief description of how they were identified.

l. Validate and Age Completed Weaknesses. When a mitigation task has been completed the weakness associated with the mitigation task should be tested and marked as "completed" if the test demonstrates the weakness has been adequately addressed. Once a weakness has been marked as "completed" for 12 months, the weakness may be "aged off' or removed from the POAM.

m. POAM Template. The following template may be used to complete a POAM for a state information system:

| System Name | | | | | System Owner | | | | | |
| POAM Last Updated | | | | | | | | | | |
Weakness Identifier	Weakness Description	POC	Resources Required	Scheduled Date of Completion	Description of Milestone	Date Changes (if necessary)	Reporting Source	Status	Comments	Severity

6.4 **Continuous Monitoring** – Each BU should implement continuous monitoring that includes:

    a. Security metrics identified through the risk assessment or industry standards

    b. Continuous logging

    c. Real-time reporting with escalation procedures

6.5 **Penetration Testing Guidance** – Penetration testing should be performed by a qualified third-party at least annually. Results from each test should be documented. Vulnerabilities should be remediated timely and retested to insure that potential risks have been mitigated.

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

8.1 CMS Information Security Program, CMS Plan of Action & Milestones (POA&M) Guidelines, Version 1.0, July 6, 2007

8.2 Guide for Developing Security Plans for Federal Information Systems, NIST Special Publication 800-18 Revision 1, February 2006.

8.3 Guide for Conducting Risk Assessments, NIST Special Publication 800-30, Revision 1, September 2012.

8.4 The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments, 2nd Edition, Douglas J. Landoll, 2010.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
		DRAFT	