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

STATEWIDE POLICY (8280): ACCEPTABLE USE

DOCUMENT NUMBER:	**(P8280)**
EFFECTIVE DATE:	**DRAFT SEPTEMBER 17, 2018**
REVISION:	**2.0**

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (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:

Section Number	Exception	Explanation / Basis

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of 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 BU Director shall:

a. Be responsible for the correct and thorough completion of (Agency) 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.

5.4 BU CIO shall:

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

e. Ensure the Acceptable Use Policy is periodically reviewed and updated to reflect changes in requirements.

5.5 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.

5.6 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.

5.7 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 for visitor sign-in, appropriate badge 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** - Installation or use of any unauthorized software, including but not limited to 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** - The following use of electronic messaging shall be prohibited:

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

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

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

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

e. **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%20&%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]

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

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

e. 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]

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

g. 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 website.

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

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

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

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

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

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