ARIZONA STATEWIDE SECURITY STANDARD	STATEWIDE STANDARD	State of Arizona

STANDARD 8320: ACCESS CONTROL

DOCUMENT NUMBER:	S8320
EFFECTIVE DATE:	JULY 1, 2015
REV:	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 standard shall apply to all BUs as defined in A.R.S. § 18-101(1).

3.2 **Application to Systems** - This standard shall apply to all state information systems. Standard statements preceded by "(P)" shall be 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

None.

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

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

5.2 State Chief Information Security Officer (CISO) shall:

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

5.3 BU Director shall:

- **a.** Be responsible for the correct and thorough completion of Statewide Information Technology PSPs within the BU;
- **b.** Ensure BU compliance with Access Control Policy; and
- **c.** Promote efforts within the BU to establish and maintain effective use of 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; and
- **b.** Ensure Access Controls Policy is periodically reviewed and updated to reflect changes in requirements.

5.5 BU ISO shall:

- **a.** Advise the BU CIO on the completeness and adequacy of the BU activities and documentation provided to ensure compliance with BU Information Technology PSPs;
- **b.** Ensure the development and implementation of adequate controls enforcing the Access Controls Policy for the BU; and
- **c.** Ensure all personnel understand their responsibilities with respect to the correct use and management of logical access controls for the protection of state information systems and assets.

5.6 Supervisors of state employees and contractors shall:

- **a.** Ensure users are appropriately trained and educated on Access Control PSPs; and
- **b.** Monitor employee activities to ensure compliance.

5.7 System Users of state information systems shall:

a. Become familiar with this and related PSPs; and

b. Adhere to PSPs regarding correct use and management of logical access controls for the protection of state information systems and assets.

6. STATEWIDE POLICY

6.1 Unsuccessful Logon Attempts - The state information system enforces the following parameters for unsuccessful logon attempts [6.9]:

Parameter	Value
Limit of consecutive invalid logon attempts	6
Response to over limit invalid attempts	Automatically lock account/node
Lock-out period	30 minutes or release by administrator

6.2 (P) Session Lock - The state information system prevents further access to the system by enforcing the following parameters for session locks [6.11]:

Parameter	Value
Initiate lock session after defined duration of inactivity or on user request	15 minutes
Retain session lock for defined duration or until user reestablishes access	30 minutes
Result of user not reestablishing session	Session dropped

6.3 Remote Access Controls - The following usage restrictions, configuration/connection requirements, and implementation guidance for remote access types shall be implemented as a minimum security requirement. Where controls requirements have been documented in the *Policy 8320, Access Control Policy* or other policies, the requirement (and policy) reference will be included at the end of the control description below [6.13]:

6.3.1 Architecture - The following architectural controls shall be implemented for remote access to state information systems:

6.3.1.1 **(P) Managed Access Control Points** - The state information system shall route all remote accesses through a limited number of managed network access control points. [P8320 6.13.3]

6.3.1.2 **Restrict Resources Available** - The state information system shall limit the resources available to the remote connection. Resource restriction includes the identification and limitation to hosts to which the remote resource requires access (e.g., web server, directory server, anti-virus update server) and limitation of the protocols used to access these servers (e.g., HTTP/HTTPS, LDAP, FTP).

6.3.1.3 **(P) Privileged Access Commands** - The BU shall authorize the execution of privileged commands and access to security-relevant information via remote access only for BU defined needs, and documents the rationale for such access in the security plan for the state information system. [P8320 6.13.4]

6.3.1.4 **(P) Prevent Split Tunneling for Remote Devices** - The state information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating using some other connection to resources in external networks, as specified in *Policy 8350, System and Communication*. [P8350 6.2.2]

6.3.2 Client Security - The following client security controls shall be implemented for remote access to state information systems:

6.3.2.1 **(Optional) Health Checks** - Remote access shall not be completed until a health check of the remote system has shown that the remote system has updated anti-virus signatures, updated critical security patches, and passed all other BU-defined security parameter.

6.3.2.2 **Virtual Office Agreement** - Equipment used for remote connections shall meet the minimum security requirements as specified in the Virtual Office Access Agreement Contents section of the *Acceptable Use Policy (P8280)*, specifically:

a. (P) Allowable Computing Devices (P8280 6.5.1)

b. (P) Physical Protection of Computing Devices (P8280 6.5.2)

c. (P) Logical Protection of Computing Devices (P8280 6.5.3)

6.3.2.3 **(P) Session Lock** - The state information system shall prevent further access to the system by initiating a session lock after 15 minutes of inactivity or upon receiving a request from a user; and retains the session lock for 30 minutes or until the user reestablishes access using established identification and authentication procedures. If the user does not reestablish access within 30 minutes the session shall be dropped. [6.11]

6.3.3 Implement Appropriate Authentication - The state information system shall implement appropriate controls for authentication of remote access sessions.

6.3.3.1 **(P) Two Factor Authentication** - The state information system shall implement two-factor authentication (e.g., multifactor authentication) for remote access to accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets statewide cryptographic standards for strength of mechanism. [P8340 6.1.5, 6.1.6]

6.3.3.2 **(Optional) Mutual Authentication** - The state information system shall implement mutual authentication of both the remote device and the server being accessed.

6.3.4 Implement Appropriate Encryption - The state information system shall implement appropriate controls for encryption of remote access sessions.

6.3.4.1 **Cryptographic Protection** - The state information system implements FIPS validated cryptography for the protection of Confidential information during transmission over open public networks and in accordance with applicable federal and state laws, Executive orders, directives, policies, regulations, and standards. [P8350 6.3.2.1]

6.3.4.2 **(P) Security using Encryption** - The state information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. [6.13.2]

6.3.5 Implement Appropriate Logging and Monitoring - The state information system shall implement appropriate controls for logging of remote access sessions.

6.3.5.1 **(P) Automated Monitoring / Control** - The state information system monitors and controls remote access methods (e.g., detection of cyber- attacks such as false logins and denial of service attacks and compliance with remote access policies such as strength of encryption). [6.13.1]

6.3.5.2 **Audit Events** - The BU ensures that the audit events logged for remote access are consistent with those logged for local access according to the *Policy 8330, System Security Audit Policy*.

6.3.6 Server Security - The state information system shall implement appropriate controls for server security in support of remote access sessions.

6.3.6.1 **Logical Placement of VPN Server** - The BU shall logically place the VPN server in the DMZ as described in the Policy 8350, System and Communication Protection. [P8350 6.1.2.1]

6.3.6.2 **Physical Placement of VPN Server** - The BU shall physical place the VPN server in a protected environment as described in the *Policy 8260, Physical Protections*. [P8260 6.6.2]

6.4 Wireless Access - The BU shall implement the following usage restrictions, configuration /connection requirements, and implementation guidance for wireless access shall be implemented as a minimum security requirement. Where controls requirements have been documented in *Policy 8320, Access Control* or other policies, the requirement (and policy) reference will be included at the end of the control description below:

6.4.1 Architecture - The following architectural controls shall be implemented for remote access to state information systems:

6.4.1.1 **(P) Managed Access Points** - The state information system limit the use of Wireless Access Points (APs) to required and authorized uses. [P8280 6.2.2.2]

6.4.2 Client Security - The following client security controls shall be implemented for wireless access to state information systems:

6.4.2.1 **Restrict Dual Connections** - Laptops and other wireless devices (e.g., smart phones) are capable of multiple connections simultaneously. These connections are referred to as dual connections and may allow for the bridging of two networks. Dual connected networks violate the principle of minimum and secure services (P8350 6.2.6). The BU shall consider the required simultaneous connections (e.g., wired access, WLAN, WiMax, Bluetooth) for a wireless device and take steps to limit dual connections.

a. BIOS Setting - Configure the device's BIOS to automatically terminate WLAN connections when a wired connection is detected. This is referred to as "LAN/WAN switching" in the BIOS setting.

b. Software-based Controls - Many operating systems have software-based controls that restrict simultaneous wired and WLAN connections. These controls are typically part of the WLAN driver or management software provided by the laptop manufacturer.

c. Host-based Network Security Tools - Host-based network security tools (e.g., host-based firewalls and host-based intrusion detection and prevention systems) may be configured to prevent multiple network interfaces from being used simultaneously**.**

d. Disable Automatic Connection to WLAN - Laptop wireless network clients may be configured to disable automatic connection to WLANs detected**.**

6.4.3 Implement Appropriate Authentication - The state information system shall implement appropriate controls for authentication of remote access sessions.

6.4.3.1 **WPA2 Enterprise Authentication** - The state information system shall implement WPA2 Enterprise authentication with an IEEE 802.1X authentication server.

6.4.3.2 **(P) Two Factor Authentication** - The state information system shall implement two-factor authentication (e.g., multifactor authentication) for access to wireless AP to accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets statewide cryptographic standards for strength of mechanism. [P8340 6.1.5, 6.1.6]

6.4.3.3 **(Optional) Mutual Authentication** - The state information system shall implement mutual authentication of both the remote device and the server being accessed.

6.4.3.4 **(Optional) Disable Broadcast of SSID** - The wireless AP is configured to not broadcast the Service Set Identification (SSID).

6.4.4 Implement Appropriate Encryption - The state information system shall implement appropriate controls for encryption of wireless networks.

6.4.4.1 **Cryptographic Protection** - The state information system implements FIPS validated cryptography for the protection of Confidential information during transmission over open public networks and in accordance with applicable federal and state laws, Executive orders, directives, policies, regulations, and standards. [P8350 6.3.2.1]

6.4.4.2 **(P) Security using Encryption** - The state information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. [6.13.2]

6.4.4.3 **Wi-Fi Certification** - The state information system procures only Wi-Fi Alliance certified devices. Current Wi-Fi certified devices must implement WPA2.

6.4.5 Server Security - The state information system shall implement appropriate controls for server security in support of remote access sessions.

6.4.5.1 **Logical Placement of Wireless Access Point** - The BU shall logically place the wireless AP in the appropriate subnet of the system architecture. If the wireless access point is intended to provide guest access to the Internet and not provide access to the protected network, then the wireless access point shall be placed in the DMZ.

For wireless access points designed to provide access to the protected network the wireless access point should be connected to a firewall and then to the rest of the system. [P8350 6.1.2.1]

6.4.5.2 **Physical Placement of Wireless Access Point** - The BU shall physical place the VPN server in a protected environment as described in the *Policy 8260, Physical Protections*. [P8260 6.6.2]

6.5 Access Control for Mobile Devices - The following usage restrictions, configuration/ connection requirements, and implementation guidance for BU controlled mobile devices; and authorizes connection of mobile devices to state information systems shall be implemented as a minimum security requirement.

6.5.1 (P) Full Device Encryption - The BU employs full-device encryption to protect the confidentiality and integrity of information on mobile devices authorized to connect to state information systems or to create, transmit or process Confidential information. Full Disk Encryption (e.g., whole disk encryption) encrypts all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the Full Disk Encryption product. [6.15.1]

6.6 Use of External Information Systems - The following terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from external information systems; and process, store, or transmit BU controlled information using external information systems shall be implemented as a minimum security requirements. [6.16]

External information systems are outside the BU-established boundary and under no direct supervision or authority of the BU. These include:

a. Personally-owned computing and communication devices;

b. Privately-owned computing and communication devices resident in commercial or public facilities;

c. Information systems owned or controlled by non-BU organizations; and

d. External information system for processing, storage, or transmission of BU information (e.g., cloud services).

6.6.1 Trusted Relationships - For existing trust relationships (e.g., other BUs with pre-existing trust relationships or agreements) no explicitly terms and conditions required. These connections are not considered an external information system**.**

6.6.2 Authorized Individual Restrictions - BUs may choose to impose different security restrictions (e.g., no remote access, read-only access) on categories of individuals such as contractors or temporary workers.

6.6.3 Public Interfaces - The requirement for terms and conditions does not apply to the access of public interfaces of external systems.

6.6.4 Terms and Conditions Contents - Terms and conditions shall address the following as a minimum:

a. Types of applications that can be accessed on BU state information systems;

b. Classification of data (e.g., Public or Confidential) that may be stored, processed, or transmitted on external systems; and

c. Personnel restrictions to access data.

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

8.1 Policy 8330, System Security Audit Policy

8.2 Policy 8340, Identification and Authentication

8.3 Policy 8350, System and Communication

8.4 Policy 8320, Access Control

8.5 Policy 8280, Acceptable Use Policy

8.6 Policy 8260, Physical Protection

8.7 NIST 800-46 Rev. 1, Guide to Enterprise Telework and Remote Access Security, June 2009.

8.8 NIST 800-77, Guide to IPSec VPNs, December 2005.

8.9 NIST 800-113, Guide to SSL VPNs, July 2008.

8.10 NIST 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007.

8.11 NIST 800-153. Guidelines for Securing Wireless Local Area Networks (WLANs), February 2012.

8.12 NIST 800-11, Guide to Storage Encryption Technologies for End User Devices, November 2007.

8.13 NIST 800-124, Rev. 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise, June 2013

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
01/01/2014	Initial Release	DRAFT	Aaron Sandeen, State CIO and Deputy Director