	STATEWIDE **STANDARD**	**State of Arizona**

STATEWIDE STANDARD (8270-1): PERSONNEL SECURITY CONTROLS:

Statewide Security Clearance Standard for Google Workspace Privileged Access

DOCUMENT NUMBER:	**S8270-1**
EFFECTIVE DATE:	**November 1, 2024**
REVISION:	**1.0**

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 standard is to define the screening criteria for personnel with privileged access within Google Workspace.

3. SCOPE

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

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

- **a. (P)** Policy statements preceded by "(P)" are required for agency systems categorized as Protected.
- **b. (P-PCI)** Policy statements preceded by "(P-PCI)" are required for agency systems with payment card industry data (e.g., cardholder data).
- **c. (P-PHI)** Policy statements preceded by "(P-PHI)" are required for agency systems with protected healthcare information..

d. **(P-FTI)** Policy statements preceded by "(P-FTI)" are required for agency systems with federal taxpayer information.

3.3 **Federal Government Information** - Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services - 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 information security 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 Arizona Department of Homeland Security Director shall:

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

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the Director on the completeness and adequacy of all state BU activities and documentation provided to ensure compliance with statewide information security PSPs throughout all state BUs;

b. Review and approve all state BU security and privacy PSPs;

c. Request exceptions from the statewide security and privacy PSPs; and

d. Identify and convey to the Director the risk to state systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 Enterprise Security Program Advisory Council (ESPAC)

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

5.4 Budget Unit (BU) Director shall:

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

c. Ensure compliance with BU PSPs; and

d. Promote efforts within the BU to establish and maintain effective use of agency 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; and

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

5.6 The BU Information Security Officer (ISO) shall:

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

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

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

5.7 Supervisors of agency employees and contractors shall:

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

b. Monitor employee activities to ensure compliance.

5.8 Users of agency systems shall:

a. Familiarize themselves with this and related PSPs; and

b. Adhere to PSPs regarding the protection of agency systems and assets through personnel security controls.

6. STATEWIDE STANDARD

6.1 **Position Categorization** - In alignment with STATEWIDE POLICY (8270): PERSONNEL SECURITY CONTROLS, personnel with privileged access within Google Workspace have been assigned sensitivity designation of SENSITIVE.

6.2 **Personnel Screening** - The State and all BU's shall screen individuals holding sensitive positions with privileged access within Google Workspace.

a. A person who is subject to registration as a sex offender in this state or any other jurisdiction, or who is awaiting trial on or who has been convicted of committing or attempting, soliciting, facilitating or conspiring to commit one or more of the offenses as listed in A.R.S. § 41-1758.07 subsections B and C in this state or the same or similar offenses in another state or jurisdiction is precluded from receiving Privileged Access within Google Workspace.

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.

7.2 Privileged Access given to any state employee or contract worker as a Google Workspace Administrator includes permissions exceeding the scope of their agency's Organizational Unit within the Admin Console. This definition extends to individuals supporting those with such access, regardless of their employment status.

8. REFERENCES

8.1 STATEWIDE POLICY P8270: Personnel Security Controls

8.2 Statewide Policy Exception Procedure

8.3 ARS § 41-1758.07

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
11/1/2024	**Initial release**	**Draft**	
1/14/2025	**Finalized and approved**	**1.0**	**Ryan Murray, Deputy Director, State CISO**