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

STATEWIDE POLICY (8110): DATA CLASSIFICATION

DOCUMENT NUMBER:	**(P8110)**
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 provide a framework for the protection of data that is created, stored, processed or transmitted STATEWIDE. The classification of data is the foundation for the specification of policies, procedures, and controls necessary for the protection of Confidential Data.

3. SCOPE

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

3.2 Application to Systems - This policy shall apply to all BU 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 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

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.

4.1.2 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services BU subject matter experts 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 or disapprove all state BU security and privacy PSPs and exceptions to existing 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 BU PSPs;

b. Ensure compliance with BU PSPs;

c. Promote efforts within the BU to establish and maintain effective use of agency information systems and assets; and

d. Be the data owner for all Confidential Data sets or shall delegate a data owner for each set of Confidential Data.

5.4 BU CIO shall:

a. Work with the BU Director to ensure the correct and thorough completion of BU IT PSPs; and

b. Ensure BU PSPs are 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 BU PSPs;

c. Request changes and/or exceptions to existing PSPs from the State CISO; and

d. Ensure all personnel understand their responsibilities with respect to securing agency information systems, including classification of data and handling.

5.6 Data Owner shall:

a. Assign classification of data;

b. Assign data custodians and ensure data custodian is familiar with the protection requirements for Confidential Data;

c. Participate in establishing, approving and maintaining policies for the protection of data within state agency; and

d. Promote data resource management within the state agency.

5.7 Data Custodian shall:

a. Ensure implementation of controls according to BU PSPs.

5.8 Supervisors of agency employees and contractors shall:

a. Ensure users are appropriately trained and educated on BU PSPs; and

b. Monitor employee activities to ensure compliance.

5.9 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 Data Classification - Data created, stored, processed or transmitted on agency information systems shall be classified according to the impact to the state or citizens resulting from the disclosure, modification, breach or destruction of the data.

6.2 Data Classification Categories - All agency data shall be classified as one of the following categories: [National Institute of Standards and Technology Special Publication (NIST SP) 800-53 RA-2]

6.2.1 Confidential Data - Data that shall be protected from unauthorized disclosure based on laws, regulations, and other legal agreements. Examples of Confidential Data include:

a. System Security Parameters and Vulnerabilities

1. System security vulnerabilities

2. Generated security information

3. Information regarding current deployment, configuration, or operation of security products or controls

b. Health Information

1. Protected Health Information [Health Insurance Portability and Accountability Act (HIPAA) - PL 104-191, Sections 261 - 264, 45 CFR Part 160 and 164]

2. Medical records [A.R.S. 12-2291, A.R.S. § 12-2292, A.R.S 36-445.04, A.R.S. § 36-404, A.R.S. § 36-509, A.R.S. § 36-3805]

3. Child immunization data [A.R.S. § 36-135]
4. Chronic disease information [A.R.S. § 36-133]
5. Communicable disease information [A.R.S. § 36-664, A.R.S. § 36-666]
6. Developmental disabilities service records [A.R.S. § 36-568.01, A.R.S. § 36-568.02]
7. Emergency medical service patient records [A.R.S. § 36-2220]
8. Genetic testing records [A.R.S. § 12-2801, A.R.S. § 12-2802]
9. Home health service records [A.R.S. § 36-160]
10. Midwifery patient records [A.R.S. § 36-756.01]
11. State trauma registry [A.R.S. § 36-2221]
12. Tuberculosis control court hearing information [A.R.S. § 36-727]
13. Vital Records [A.R.S. § 36-342]

c. Financial Account Data (on individuals)
1. Card Holder Data (CHD) including Primary Account Number (PAN), Cardholder Name, Expiration Date, and Service Code [Payment Card Industry Data Security Standard (PCI DSS) v3.2.1]
2. Credit card, charge card or debit card numbers, retirement account numbers, savings, checking or securities entitlement account numbers [A.R.S. § 44-1373]

d. Criminal Justice Information
1. Child Protective Services records [A.R.S. § 41-1959]
2. Criminal history record information [A.R.S. § 41-619.54]
3. Criminal Justice Information [A.R.S. § 41-1750]

e. Critical Infrastructure/Fuel Facility Reports [A.R.S. § 41-4273]

f. Eligible Persons [A.R.S. § 39-123, A.R.S. § 39-124]

g. Risk Assessment and State Audit Records
1. Auditor General Records [A.R.S. § 41-1279.05]
2. Federal risk assessments of infrastructure [A.R.S. § 39-126]

h. Personal Identifying Information (except as determined to be public record) [A.R.S. § 41-4172]
1. Educational records [Family Educational Rights and Privacy Act (FERPA)]
2. Social Security Number [A.R.S. § 44-1373]

i. Taxpayer Information - Federal Tax Information (FTI) [A.R.S. § 42-2001] [Internal Revenue Service Publication 1075 (IRS Pub 1075)]

j. Licensing, Certification, Statistics and Investigation Information (of a sensitive nature)
1. Abortion reports [A.R.S. § 36-2161]
2. Child Death Records [A.R.S. § 36-3503]
3. Controlled substance records [A.R.S. § 36-2523]

4. Emergency medical service investigation records [A.R.S. § 36-2220]
5. Employment discrimination information [A.R.S. § 41-1482]
6. Health Care Cost Containment Records [A.R.S. § 36-2917]
7. Health Care Directives Registry Information [A.R.S. § 36-3295]
8. Health care entity licensing information [A.R.S. § 36-2403, A.R.S. § 36-404]
9. Medical Marijuana Records [A.R.S. § 36-2810]
10. Medical practice review [A.R.S. § 36-445, A.R.S. § 36-445.01]
11. Nursing home certification records [A.R.S. § 36-446.10]
12. Prescription information [A.R.S. § 36-2604]

k. Other State-owned Confidential Data, may include but not limited to:
1. Archaeological discoveries [A.R.S. § 39-125]
2. Attorney General opinions [A.R.S. § 38-507]
3. Tax Examination guidelines [A.R.S. § 42-2001]
4. Unclaimed property reports [A.R.S. § 44-315]
5. Vehicle information [A.R.S. § 41-3452]

l. Other Non-state-owned Confidential Data, may include, but not limited to:
1. Attorney-Client Privileged Information [A.R.S. § 41-361]
2. Bank Records [A.R.S. § 6-129]
3. Trade secrets and proprietary information [Intellectual Property laws]
4. Management and Support Information

m. Other records protected by law

6.2.2 Public Data - In accordance with Arizona public records law, data that may be released to the public and requires no additional levels of protection from unauthorized disclosure.

6.3 Identification - All data shall be identified as one of the following data classifications:

a. Confidential; or

b. Public (data that is not identified is assumed to be Public).

6.4 Collection

a. (C) Limit Collection -
1. Encrypt confidential data
2. Properly dispose, destroy, or delete data
3. Limit access to confidential information
4. Securely store confidential data

6.5 Handling

6.5.1 (C) Need to Know - All Confidential Data shall only be given to those persons that have authorized access and a need to know the information in the performance of their duties. [HIPAA 164.308 (a)(3)(ii)(A) – Addressable] [PCI DSS 7]

6.5.2 (C) Hand Carry - All Confidential Data being hand-carried shall be kept with the individual and protected from unauthorized disclosure.

6.5.3 (C) Accounting - For bulk transfer of Confidential Data containing 500 or more records, the receipt and delivery of all Confidential Data shall be monitored and accounted for to ensure the data is not lost and potentially compromised.

6.5.4 (C) Guardian - When outside of controlled areas all Confidential Data shall not be left unattended, even temporarily. All Confidential Data shall remain either in a controlled environment or in the employee's physical control at all times. Mail, courier, or other mail services are considered controlled areas.

6.5.5 (C) Out-of-sight - All Confidential Data shall be turned over or put out of sight when visitors not authorized to view data are present.

6.5.6 (C) Conversations - Confidential Data shall not be discussed outside of controlled areas when visitors not authorized to hear Confidential Data are present.

6.5.7 (C) Movement - Unauthorized movement of Confidential Data from controlled areas shall be prohibited. [HIPAA 164.310 (d)(1)]

6.6 Transmission

6.6.1 (C) Encryption - Any external transmission of Confidential Data shall be encrypted either through link or end-to-end encryption. [HIPAA 164.308 (e)(2)(ii) – Addressable] [PCI DSS 4]

6.6.2 (C) Encryption Strength - Encryption algorithm and key length shall be compliant with current state agency minimum encryption standards as stated in the System and Communications Protection Standard [S8350].

6.7 Processing

6.7.1 (C) Approved Processing - Confidential Data shall be processed on approved devices.

6.8 Media Protection

6.8.1 (C) Confidential Data Protection - All Confidential Data shall be protected and implemented at minimum controls as stated in the Media Protection Policy P8250 and Media Protection Standard S8250. [HIPAA 164.310 (d)(2)] [PCI DSS 3, 9]

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 P8110 DATA CLASSIFICATION

8.2 Statewide Policy Exception Procedure

8.3 Standard S8350, System and Communications Protections

8.4 Policy P8250, Media Protection Policy

8.5 Standard S8250, Media Protection Standard

8.6 DoD 5220.22-M. National Industrial Security Program Operating Manual (NISPOM) January 1995. U.S. Government Printing Office ISBN0-16-045560-X

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

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

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**