ARIZONA DEPARTMENT OF CHILD SAFETY

TITLE	POLICY NUMBER	
Incident Response Planning Policy	DCS 05-8240	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	May 20, 2025	5

I. POLICY STATEMENT

The purpose of this policy is to increase the ability for DCS to rapidly detect incidents, minimize any loss due to destruction, mitigate the weaknesses that were exploited, and restore Information Systems services. This Policy will be reviewed annually.

II. APPLICABILITY

This policy applies to all DCS information systems, processes, operations, and personnel including employees, contractors, interns, volunteers, external partners and their respective programs and operations.

III. AUTHORITY

A.R.S. § 18-104 Powers and duties of the department; violation; classification

A.R.S. § 41-4282 Statewide information security and privacy office; duties; suspension of budget unit's information infrastructure

HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, November 2022

NIST 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations, September 2020

IV. EXCEPTIONS

Exceptions to this and all DCS IT policies are approved at the sole discretion of the DCS CIO, will be signed and made an attachment to each applicable policy.

Exceptions to the Statewide Policy Framework taken by DCS shall be documented in the following format:

Section Number	Exception	Explanation / Basis

V. ROLES AND RESPONSIBILITIES

A. The DCS Director shall:

1. be responsible for the correct and thorough completion of DCS IT Policies, Standards, and Procedures (PSPs);

2. ensure compliance with DCS PSPs;

3. promote efforts within DCS to establish and maintain effective use of DCS information systems and assets.

B. The DCS Chief Information Officer (CIO) shall:

1. work with the DCS Director to ensure the correct and thorough completion of DCS IT PSPs;

2. ensure DCS PSPs are periodically reviewed and updated to reflect changes in requirements, lessons learned from actual incidents, and advances the industry.

C. The DCS Chief Information Security Officer (CISO) shall:

1. advise the DCS CIO on the completeness and adequacy of DCS activities and documentation provided to ensure compliance with DCS IT PSPs;

2. ensure the development and implementation of adequate controls enforcing the Incident Response Planning Policy for DCS;

3. ensure all DCS personnel understand their responsibilities with respect to planning and responding to security incidents;

D. The DCS Privacy Officer shall:

1. advise the State CISO and the State CPO on the completeness and adequacy of the DCS activities and documentation provided to ensure compliance with privacy laws, regulations, statutes;

2. assist DCS to ensure the privacy of sensitive personal information within DCS's possession.

E. Supervisors of DCS employees and contractors shall:

1. ensure users are appropriately trained and educated on the Incident Response Planning Policy;

2. monitor employee activities to ensure compliance.

F. System Users of DCS information systems shall:

1. become familiar with related DCS IT PSPs;

2. adhere to DCS IT PSPs regarding classification of incidents response planning within DCS information systems.

VI. POLICY

A. Incident Response Training

DCS shall provide incident response training to DCS information system users consistent with assigned roles and responsibilities before authorizing access to the DCS information system or performing assigned duties, when required by DCS information system changes, and annually thereafter. DCS shall review and update incident response training content annually and following a major incident

[NIST 800-53 IR-2].

1. Breach - DCS shall provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach [NIST 800-53 IR-2(3)].

B. Incident Response Testing

DCS shall test the incident response capability for DCS information system annually using checklists, walk-through, tabletop exercises, simulations, or comprehensive exercises to determine the incident response effectiveness and document the results [NIST 800-53 IR-3].

1. Coordinated Testing – DCS shall coordinate incident response testing with DCS elements responsible for related plans [NIST 800-53 IR-3(2)].

2. Incident Response Test Elements – DCS shall include the following elements (at a minimum) in the annual incident response test:

    a. incident response roles and responsibilities, communications, and contact strategies;

    b. specific incident response procedures;

    c. business recovery and continuity procedures;

    d. data back-up processes;

    e. legal requirement and breach notification analysis;

    f. critical system component coverage and responses;

    g. reference or inclusion of incident response procedures from external entities.

C. Incident Handling

1. DCS shall implement an incident handling capability for incidents that is consistent with the incident response plan; and [NIST 800-53 IR-4] [HIPAA 164.308(a)(6)(ii)]:

    a. shall include preparation, detection and analysis, containment, eradication, and recovery;

b. shall coordinate incident handling activities with contingency planning activities; these activities shall address the following at a minimum:

i. unauthorized wireless access point detection;

ii. alerts generated by change detection solutions (e.g., unauthorized modification of critical files, configuration files or content files).

c. the incident response procedures, training, and testing/exercises shall cover industry developments and lessons learned from ongoing incident handling activities that drive the modification and evolution of the incident response plan

d. implement industry development changes where applicable; and

e. DCS shall ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

2. Automated Incident Handling Process – DCS shall employ automated mechanisms to support the incident handling process [NIST 800-53 IR-4(1)].

3. Assign Incident Handling Role – DCS shall assign to an individual or team the information security management responsibility of implementing an incident response plan and to be prepared to respond immediately to a system breach.

4. 24x7 availability – DCS shall assign to specific personnel the information security management responsibility of being available on a 24x7 basis to respond to alerts.

5. Forensic Capability – DCS shall establish processes to provide for timely forensic investigation in the event of a compromise to any hosted service.

D. Incident Monitoring

DCS shall track and document DCS information system security incidents [NIST 800-53 IR-5] [HIPAA 164.308(a)(6)(ii)].

1. Assign Incident Monitoring Role – DCS shall assign to an individual or

team the information security management responsibility of monitoring and analyzing security alerts and information and distributing alerts to appropriate personnel.

2. Incorporate Automated Alerts – DCS shall implement the system to include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.

3. Continuous Monitoring Strategy – DCS shall develop a DCS-wide continuous monitoring strategy and implement continuous monitoring programs that include [NIST 800 53 PM-31]:

   a. establishing the DCS-defined metrics to be monitored;

   b. establishing DCS-defined frequency for monitoring and annual assessment of control effectiveness;

   c. ongoing monitoring of DCS-defined metrics in accordance with the continuous monitoring strategy;

   d. correlation and analysis of information generated by control assessments and monitoring;

   e. response actions to address results of the analysis of control assessment and monitoring information; and

   f. reporting the security and privacy status of DCS systems to the DCS CISO, DCS Privacy Officer, State CISO and State Privacy Officer annually.

E. Incident Reporting

1. DCS shall require personnel to report [NIST 800-53 IR-6] [A.R.S. § 41-4282] [EO 2008-10] [HIPAA 164.308(a)(6)(ii)] [HIPAA 164.308(a)(1)(ii)(D)] [HIPAA 164.314(a)(2)(i)(C)]:

   a. suspected security incidents to the organizational incident response capability within one hour of knowledge of suspected incident as specified in the DCS-05-8240 Incident Response Planning Policy;

   b. (in the event of a security incident) Security incident ~~information~~ to be communicated to the State CISO; and

c. (in the event of a privacy incident) privacy incident information to the State Privacy Officer.

2. Use of Statewide Incident Handling Program – DCS can utilize the statewide incident handling program to meet the requirement for reporting of security and privacy incidents that are visible within the program (e.g., part of the monitored systems and logs). However, DCS must implement a system to integrate with the notification process for security incidents that originate outside of the monitored systems (e.g., employee reported malware, onsite physical threats, reported loss of laptop)

3. Automated Incident Reporting – DCS shall employ automated mechanisms to assist in the reporting of security incidents. [NIST 800-53 IR-6(1)].

4. Supply Chain Coordination - DCS shall provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems of system components related to the incident. [NIST 800-53 IR-6(3)]

5. Incident Response Reporting - DCS shall Respond to information spills by [NIST 800 53 IR-9]:

   a. assigning DCS Privacy Officer with responsibility for responding to information spills;

   b. identifying the specific information involved in the system contamination;

   c. alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill;

   d. isolating the contaminated system or system component;

   e. eradicating the information from the contaminated system or component;

   f. identifying other systems or system components that may have been subsequently contaminated; and

   g. performing the additional DCS-defined actions.

F. Incident Response Plan

DCS shall develop an incident response plan that:

1. provides the organization with a roadmap for implementing its incident response capability;

2. describes the structure and organization of the incident response capability;

3. provides a high-level approach for how the incident response capability fits into the overall organization;

4. meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

5. defines reportable incidents;

6. provides metrics for measuring the incident response capability within the organization;

7. defines the resources and management support needed to effectively maintain and manage an incident response capability;

8. describes the roles, responsibilities, and communication and contact strategies in the event of a compromise including specific incident response procedures, business recovery and continuity procedures, data backup processes, analysis of legal requirements for reporting compromises, and coverage and responses of all critical system components;

    a. is reviewed and approved by the DCS Chief Information Security Officer (CISO);

    b. addresses the sharing of incident information;

    c. explicitly designates the responsibility for incident response;

9. addresses breaches involving personally identifiable information. including: a process to determine if notice to individuals or other organizations, including oversight organizations, is needed; an assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and identification of applicable privacy

requirements [NIST 800-53 IR-8(1)].

DCS shall:

1. distribute copies of the incident response plan to incident response personnel and organizational elements;

2. review the incident response plan annually;

3. revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

4. communicate incident response plan changes to DCS incident response personnel and the State CISO and State Privacy Officer; and

5. protect the incident response plan from unauthorized disclosure and modification.

G. Incident Response Assistance

DCS shall provide an incident response support resource, integral to the DCS incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents [NIST 800-53 IR-7].

1. Automated Support for Availability of Information – DCS shall employ automated mechanisms to increase the availability of incident response-related information and support [NIST 800-53 IR-7(1)].

H. Investigation – DCS shall promptly investigate potential privacy incidents upon awareness of unencrypted Personally Identifiable Information (PII) loss [A.R.S. § 18-552.A].

a. Breach Determination – The investigation shall determine if the security incident resulted in a system security breach. [A.R.S. § 18-552.A].

b. Determination of No Substantial Economic Loss – If an independent third-party forensic auditor or law enforcement agency performed a reasonable investigation and has determined that the system breach has not resulted in or in not reasonably likely to result in substantial economic loss to affected individuals

DCS is not required to make the notification as described below [A.R.S. § 18-552.J].

2. Notification – DCS shall notify affected parties upon breach determination within 45 days after the determination [A.R.S. § 18-551.B, 18-551.H] [HIPAA 164.404(a)].

   a. Non-state Owned PII Notification – For PII not owned by the state, DCS shall notify and cooperate with the owner following the discovery of a breach as soon as practicable, including sharing information relevant to the breach [A.R.S. § 18-552.C].

   b. Notification Exceptions – DCS may delay or potentially forgo notification in the following cases.

      i. If law enforcement determines notification will impede the investigation. The required notification shall be implemented within 45 days of being informed by law enforcement that notifications would no longer impede the investigation [A.R.S. § 18-552.D] [HIPAA 164.412];

      ii. Good Faith Exposure – No notification is required in the event the disclosure was unintentional or inadvertent by a workforce member acting in good faith and there is no further disclosure [HIPAA 164.402.1.i-ii].

      iii. No Retention – No notification is required in the event the disclosure is to an unauthorized person, but it is believed that there is no reasonable way for that person to retain the information [HIPAA 164.402.1.iii].

      iv. Low Probability of Compromise – No notification is required in the event the disclosure is demonstrated to have a low probability of compromise based on a risk assessment that considers at least the following factors [HIPAA 164.402.2]:

         (a) the nature and extent of the PHI involved (including identifier types, and likelihood of re-identification);

         (b) the unauthorized person to whom the PHI was exposed;

(c) whether the PHI was actually acquired or viewed; and

(d) the extent to which the risk to the PHI has been mitigated.

If DCS determines a Low Probability of Compromise, the determination must be supported through a documented risk analysis process.

c. Notification Methods – DCS may use written notice via mail, telephone (but not through a prerecorded message), or email as a method of notification [A.R.S. § 18-552.F].

i. If the cost of notification via these methods would exceed $50,000, the notification method may be a written letter to the attorney general that demonstrates the facts necessary for substitute notice, and a conspicuous posting of the notice for at least 435 days on the DCS website [A.R.S. § 18-552.F.4].

ii. If the breach involves account login information (e.g., username and password, or security questions) and not any other personal information, the notification may be an electronic message that directs the user to re-secure the account (and all other accounts using the same password or security question) by changing the password and security question(s) [A.R.S. § 18-551.G].

iii. If the breach involves account login information with an email account, the notification may be directed to the individual using a method other than the suspect email address:

(a) Notification delivered online when the IP address or online location matches a known customary address or location for that account [A.R.S. § 18-551.G].

d. Notification Timing – DCS shall implement notifications without unreasonable delay and in no case later than 45 days after discovery of a breach or suspected breach of PHI [A.R.S. § 18-552.B], [HIPAA 164.404(b), 164.406(b)].

e. Notification Elements – The notification shall include the following elements [A.R.S. § 18-552.E]:

i. approximate date of the breach;

ii. brief description of personal information included in the breach;

iii. toll-free numbers and addresses for the 3 largest nationwide consumer reporting agencies;

iv. toll-free number, address, and website address for the Federal Trade Commission or any federal agency that assists consumers with identity theft matters.

f. Additional Notifications – For a breach of unsecured PHI the following additional notifications must be implemented:

i. Breach Log – For breaches involving less than 500 residents of a State or jurisdiction, DCS shall maintain a log of such breaches [HIPAA 164.408(c)].

ii. Media Notification – For PHI breaches involving more than 500 residents of a State or jurisdiction DCS shall notify prominent media outlets serving the State or jurisdiction [HIPAA 164.406(a)].

iii. (P-PII) Media Notification – For PII breaches involving more than 1,000 individuals, notify the 3 largest nationwide consumer-reporting agencies and the attorney general with a copy of the notification provided to the individuals [A.R.S. § 18-552.B.2].

iv. HHS Secretary Notification – For any PHI breach, DCS shall notify the Secretary of Health and Human Services. In addition, each year DCS shall notify the HHS Secretary of the logged data of PHI breaches in the manner specified on the HHS website [HIPAA 164.408(a), 164.408(b), 164.408(c)].

g. Federal Regulators – DCS is compliant with the notification requirements if they are compliant with the notification requirements established by their primary or functional federal

regulator [A.R.S. § 18-552.I].

VII. DEFINITIONS

Refer to the Policy, Standards and Procedures Glossary located on the Arizona Strategic Enterprise Technology (ASET) website.

VIII. ATTACHMENTS

None.

IX. REVISION HISTORY

Date	Change	Revision	Signature
06 Dec 2017	Initial Release	1	DeAnn Seneff
02 Jul 2018	Annual Review	2	DeAnn Seneff
03 Apr 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-09 to DCS 05-8240 for better tracking with Arizona Department Homeland Security (AZDOHS) policy numbers.	3	

15 Mar 2024	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	4	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 3/16/2024 Frank Sweeney Chief Information Officer AZDCS
20 May 2025	Annual review to align with newest Arizona Department Homeland Security (AZDOHS) policy revisions	5	Signed by: Frank Sweeney CDB46EB4E4A6442... 6/2/2025 Frank Sweeney Chief Information Officer AZDCS