



Arizona Department of Child Safety

| | | |
|-------------------------------|----------------|----------|
| TITLE | POLICY NUMBER | |
| Insider Threat Program Policy | DCS 05-8450 | |
| RESPONSIBLE AREA | EFFECTIVE DATE | REVISION |
| DCS Information Technology | June 30, 2024 | 4 |

I. POLICY STATEMENT

This purpose of this policy is to establish the Department of Child Safety (DCS) Insider Threat Program (ITP) and appropriate controls for the protection of DCS information systems and their communications. This Policy will be reviewed annually.

II. APPLICABILITY

This procedure applies to all DCS information systems, processes, operations, and personnel to include all 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 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.

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 DCS PSPs;
3. ensure all DCS personnel understand their responsibilities with respect to

- securing DCS information systems;
 - 4. manage and store all documentation needed to perform the functions of the Insider Threat Program (ITP);
 - 5. provide ITP training to DCS leadership and all DCS personnel as needed to ensure widest dissemination of the program;
 - 6. establish procedures (as needed) to perform the functions of the ITP;
 - 7. establish a system to process and identify patterns of negligence or carelessness in handling confidential information;
 - 8. oversee the collection, analysis, and reporting of information across DCS to support identification and assessment of insider threat;
 - 9. establish and manage all implementation and reporting requirements, to include self-assessments and independent assessments, the results of which shall be reported to senior management.
- D. Supervisors of DCS employees and contractors shall:
- 1. ensure users are appropriately trained and educated on this and all DCS PSPs;
 - 2. monitor employee activities to ensure compliance.
- E. System Users of DCS information systems shall:
- 1. become familiar with and adhere to all DCS PSPs;

VI. POLICY

- A. Insider Threat Program (ITP) - DCS shall establish an ITP to protect personnel, facilities, and automated systems from insider threats within DCS. The goals of the ITP are to:
- 1. prevent destruction and unauthorized disclosure of confidential information;
 - 2. deter employees from becoming insider threats;

3. detect employees who pose a risk to confidential information systems and confidential information;
 4. mitigate the risks to the security of confidential information through administrative, investigative, or other responses;
 5. DCS personnel are not authorized to perform information technology systems insider threat investigations unless specifically authorized in writing by the DCS ISO.
- B. Training - ITP awareness will be included in initial and annual information security training to reinforce and update employees on the information provided in initial training.
- C. Reporting
1. Reporting possible insider threats is the responsibility of all DCS personnel.
 2. All reports of insider threats shall be given directly to the DCS ISO for future investigation.
 3. Insider threat investigations that appear to have the potential to be an illegal or dangerous activity (as deemed by the ISO and DCS senior management) shall be reported to the proper authorities in a timely manner.
 4. Suspicious activity shall be reported to the IT Security DL at ITSecurityDL@azdcs.gov.

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 |
|--------------------|--|----------|---|
| 02 Jul 2018 | Initial Release | 1 | DeAnn Seneff |
| 8 Jul 2020 | Annual Review | 2 | Matt Grant |
| 15 Aug 2023 | Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-21 to DCS 05-8450 Insider Threat Program Policy for better tracking with Arizona Department Homeland Security (AZDoHS) policy numbers. | 3 | Frank Sweeney DCS CIO |
| 30 Jun 2024 | Annual review and updates to mirror AZDoHS | 4 | <p>DocuSigned by:  <small>CDB46EB4E4A6442...</small> 7/8/2024</p> <p>Frank Sweeney Chief Information officer AZDCS</p> |