



Arizona Department of Child Safety

TITLE	POLICY NUMBER	
Artificial Intelligence (AI) Policy	DCS 05-2000	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	June 30, 2024	Initial

I. POLICY STATEMENT

The purpose of this policy is to define the security requirements for establishing and maintaining Artificial Intelligence (AI) for DCS information systems. 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. § 18-101](#) Definitions

[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, Recommended Security Controls for Federal Information Systems](#)

[and Organizations, Sept 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 Information Technology Policies, Standards and Procedures (PSPs);
2. ensure compliance with DCS IT PSPs, and;
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; and
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 the DCS

activities and documentation provided to ensure compliance with DCS IT PSPs;

2. ensure the development and implementation of adequate controls enforcing DCS IT PSPs; and
3. ensure all DCS personnel understand their responsibilities with respect to securing agency information systems.

D. Supervisors of DCS employees and contractors shall:

1. ensure users are appropriately trained and educated on this and all DCS IT PSPs; and
2. monitor employee activities to ensure compliance.

E. System users of DCS information systems shall:

1. become familiar with and adhere to all DCS IT PSPs; and
2. adhere to PSPs regarding the establishment and maintenance of user accounts for agency information systems.

VI. POLICY

A. **General:** Generative AI is a powerful tool that can be used to improve government services and operations. When making use of generative AI tools and capabilities, DCS users should consider the following general principles:

1. **Empowerment.** AI should be utilized to support our workforce to deliver enhanced services and products efficiently, safely, and equitably to the public. We rely on the judgment of our professionals to ensure we realize the benefits of these tools.
2. **Transparency and Accountability:** We acknowledge the limits of foresight. But transparency builds trust and enables collective learning. When AI is used, we must disclose that responsibly and share our workflow freely with other public servants and with the public. DCS must be transparent about how the Agency is using generative AI. This shall include full attribution to which GenAI tool is used (see DCS-05-2000-P01 - Use of Generative AI Procedure for resources).
 - a. All copyrightable works owned by the State that are created with the involvement of generative AI must include an accompanying

annotation sufficient to meet the requirements of the U.S. Copyright Office for Works Containing Material Generated by Artificial Intelligence (88 FR 16190). The annotation should include at least the generative AI technology used and a description of how it was used to create the work.

- b. Detail the AI model, prompts, and methods employed. This documentation aids comprehension and safe usage by colleagues and stakeholders. Sample AI-generated content disclosures:

"This content was generated with the aid of ChatGPT and subsequently revised by the staff of DCS."

"This text was summarized for clarity using Google Bard."

- c. DCS users are encouraged to consider whether more specific policy and guidelines regarding disclosure of Generative AI assisted work products will best serve the public's need for transparency.
 - d. DCS is accountable for the decisions that are made and materials created using generative AI.
3. **Fairness:** The use and development of AI should uplift communities, connecting them effectively with resources to thrive, especially those historically marginalized. As public stewards, DCS will use tools respectfully to reflect values of equity and social justice. AI systems can reflect the cultural, economic, and social biases of the source materials used for training, and the algorithms used to parse and process that content can be a source of bias as well. DCS shall make best efforts to ensure that generative AI is used in a fair and equitable manner.
 4. **Security:** DCS embraces responsible experimentation that maintains control and respects privacy and security while developing uses that drive efficiency, dialogue, and better service. DCS shall take steps to protect the security and integrity of generative AI models. Arizona Department of Homeland Security's cybersecurity staff are available to provide technical support in securing AI resources which may include requiring proactive risk assessment.
 5. **Privacy:** DCS must protect the privacy of individuals when using generative AI. This means that any models shall not be used to collect or store personal information without the consent of the individual.
 - a. DCS must comply with all records management, privacy and other applicable laws, rules, and policies to ensure the appropriate and reasonable protection of data and the protection of rights of

persons that may be impacted by information furnished by AI.

- b. No confidential data, as defined in DCS-05-8110 Data Classification Policy, shall be added to a publicly accessible AI service or training model.
 - c. Material that is inappropriate for public release shall not be entered as input to generative AI tools that have not been explicitly approved for the intended use case.
6. **Training:** DCS shall mandate a minimum level of AI training for users responsible for business processes which are incorporating generative AI.
- a. ADOA will provide training on proper usage of generative AI for users. DCS shall ensure that all users of tools consisting of or incorporating generative AI complete this training before being granted access and annually thereafter.
7. **Procurement:**
- a. New DCS contracts shall prohibit AI Vendors from using State of Arizona materials or data in generative AI queries or for building or training proprietary Generative AI programs unless explicitly approved in advance by the State in writing.
 - b. DCS Procurement shall ensure vendors disclose the utilization of Generative AI when producing works owned by the State and integration of Generative AI in products used by the State.
 - c. DCS Procurement shall perform due diligence to ensure proper licensure of model training data for all generative AI services using non-state data.
8. **Collaboration:** Before deployment of Generative AI into any state production environment, DCS shall collaborate directly with the offices of the State CIO and the State CISO and review the use case, data classification, risk profile and security controls.
9. **Legal:** There are unresolved legal issues surrounding Generative AI and the data inputs used to create Generative AI models. As Generative AI systems can be trained using copyrighted material and/or other intellectual property that has been sourced without regard for copyright or licensing terms, sources of inputs to models must be reviewed and usage risk evaluated by DCS.

B. Requirements

1. All Generative AI software services, even if they are free or part of a pilot or proof-of-concept project, must be reviewed by DCS Security to ensure the AI software meets all necessary security and privacy requirements, including DCS-05-8280 Acceptable Use Policy. This requirement applies to downloadable software, Software as a Service (SaaS), web-based services, browser plug-ins, and smartphone apps. New AI software requests are subject to existing applicable Information Technology, Security and Privacy policies.
2. Use of Generative AI technology that is incorporated into existing services and products, such as internet search engines, does not require permission to use, however this Policy's guidelines and other requirements must be followed.
3. AI outputs must be reviewed by knowledgeable human operators for accuracy, appropriateness, privacy, and IT Security before being acted upon or disseminated. Generative AI outputs should not be assumed to be truthful, credible or accurate.
4. Generative AI outputs shall not be used to impersonate individuals or organizations without their prior written permission.
5. All software code generated through the use of Generative AI shall not be used in production until fully reviewed and tested for proper functionality and security. Any such use shall be properly documented.

VII. DEFINITIONS

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

- A. Any terms not defined in this Policy are defined in statute or rule.
 1. **AI or Artificial Intelligence:** The science and engineering of making machines capable of performing tasks that are typically associated with human intelligence, such as learning and problem-solving. When used in this Policy, AI includes without limitation AI systems, Classic AI, External AI, Generative AI and LLM AI.
 2. **AI or Artificial Intelligence Systems:** Products and services that incorporate AI hardware and software components that support machine learning, expert systems, and robust data sets to be adaptable and

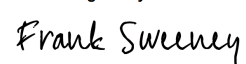
autonomous in providing requested solutions.

3. **AI Supplier or AI Vendor:** Any entity that supplies AI services or components, such as research, development, training, implementation, deployment, maintenance, provision, or sale of AI systems.
4. **Classic (or Non-Generative) AI:** Any system that uses aspects of Artificial Intelligence to apply predefined rules to automate steps in an existing workflow.
5. **External AI Systems:** An AI model or engine that depends on infrastructure or data resources outside the immediate and complete control of the State.
6. **Gen AI:** See ‘Generative AI’ below.
7. **Generative AI:** An AI system that learns the patterns and structures of input training data to generate new content.
8. **Generative AI:** An AI system that learns the patterns and structures of input training data to generate new content.

VIII. ATTACHMENTS

None.

IX. REVISION HISTORY

Date	Change	Revision	Signature
30 Jun 2024	Initial Release	1	DocuSigned by:  CDB46EB4E4A6442... 7/8/2024 Frank Sweeney Chief Information Officer AZDCS