TITLE	POLICY NUMBER	
Acceptable Use Policy	DCS 05-8280	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	June 30, 2024	3

I. POLICY STATEMENT

The purpose of this policy is to outline the acceptable use of DCS information system assets to reduce the risks to DCS information systems due to disclosure, modification, or disruption, whether intentional or accidental. This {Policy will be reviewed annually.

II. APPLICABILITY

This policy 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 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.

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 agency information systems.

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. Access Agreements - The DCS Director or designee shall ensure that individuals requiring access to organizational information and DCS information systems acknowledge and accept appropriate access agreements (prior to being granted access) and shall review and, if necessary, update the access agreements annually [NIST 800-53 PS-6].

1. Rules of Behavior - DCS shall: [NIST 800-53 PL-4]

a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;

b. Receive a documented acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;

c. Review and update the rules of behavior annually; and

d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules are reviewed or updated.

2. Assigning Responsibility to Provide Policy - The DCS Director or designee shall assign responsibility to a department, role, or named individual to provide acceptable use and other related information security policies to employees and contractors.

3. Assigning Responsibility to Keep Records - The DCS Director or designee shall assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

B. Access Agreement Contents - The access agreements shall contain the following policy sections and statements:

1. Expected Behaviors - The following behaviors shall be required:

a. Practicing Safe Computing - Those accessing DCS information systems shall use caution and exercise good security practices to ensure the protection of DCS information systems and data, including but not limited to:

i. opening attachments or links - using caution when opening email attachments or following hypertext links received from unknown senders.

ii. keep passwords secure - selecting strong passwords, do not writing them down, changing them frequently, and not sharing them with anyone.

iii. keep desks and workstations secure - use available operating system functions to lock the workstation when away from the desk. At the of the day, log out of the computer, but leave the equipment powered on.

iv. challenge unauthorized personnel - assist in enforcing physical access controls by challenging unauthorized personnel who may not be following procedures, appropriate badge display and use, escort control, and/or entry.

v. report security or privacy weaknesses or violations - report

any weaknesses in computer security or data privacy, suspicious behavior of others and any incidents of possible misuse or violation of this policy to the proper authorities.

vi. wear issued badges - all employees and contractors are required to wear their DCS-issued ID badges, while in the building, at all times.

b. Protect Confidential Information - Confidential information shall be protected in accordance with applicable statutes, rules, policies, standards, and procedures. Those accessing DCS information systems shall protect confidential information in accordance with the Data Classification Policy (DCS-05-8110), including:

c. Marking of confidential information - all non-public data must be marked (labeled) as confidential. Unlabeled data is assumed to be public.

d. Unencrypted confidential information - confidential information sent over email or other electronic messaging without adequate encryption shall be prohibited (even to an authorized user);

e. Storing confidential information - confidential information must be stored in accordance with the Media Protection Policy (DCS 05-8250);

f. Electronic transmitting of confidential information - confidential information that is transmitted outside of DCS information system or on any medium that can be accessed by authorized users shall be encrypted through link or end-to-end encryption with an encryption algorithm and key length that meets the System and Communication Protection Policy (DCS 05-8350) policy requirements.

2. Prohibited Behaviors - The following behaviors shall be prohibited:

i. computer tampering - unauthorized access, interception, modification or destruction of any computer, computer system, DCS information system, computer programs or data [A.R.S. § 13-2316.1-2];

ii. use of unauthorized computing equipment - installation or connections of any computing equipment not provided or authorized by management to DCS information systems;

iii. use of unauthorized software - installation or use of any unauthorized software, including but not limited to browser applications and extensions, security testing, monitoring, encryption, or "hacking" software on DCS computing resources; [NIST 800 53 CM-11];

iv. unauthorized use of software or services - use of peer-to-peer file sharing technology used for the unauthorized distribution, display, performance, or reproduction of copyrighted work [NIST 800 53 CM-10] - as well as:

v. violation of Copyright Law - Use of software and associated documentation in violation of contract agreements and copyright laws; [NIST 800-53 CM-10]

vi. use of Open-Source software - The use of open-source software in violation of the BU-defined restrictions on the use of open-source software; [NIST CM-10(1)]

vii. introduction of malware - knowingly introducing a computer contaminant into any computer, computer system, or DCS information systems [A.R.S. § 13-2316.3];

viii. system disruption - recklessly disrupting or causing the disruption of a computer, computer system, or DCS information system [A.R.S. § 13-2316.4];

ix. circumvention of security controls - disabling software, modifying configurations, or otherwise circumventing security controls [A.R.S. § 13-2316]. Tampering with physical security measures (e.g., locks, cameras) is also prohibited;

x. false identity - falsifying identification information or routing information so as to obscure the origins or the

identity of the sender, or using or assuming any information system or application identification other than one's own;

xi. cryptocurrency mining - malicious software introduced onto a computer, and power is used to compute math problems to obtain cryptocurrency.

b. Unauthorized inappropriate or unlawful material - the unauthorized storage, transmission, or viewing of any pornography or other offensive, intimidating, hostile or otherwise illegal material is forbidden. Except to the extent required in conjunction with a bona fide DCS-approved research project or other DCS approved undertaking, an employee of DCS shall not knowingly use DCS-owned or DCS-leased computer equipment to access, download, print, or store any information infrastructure files or services that depict nudity, sexual activity, sexual excitement or ultimate sex acts [A.R.S. § 38-448] [A.R.S. § 13-2316.5].

c. Unauthorized use of electronic messaging - the following use of electronic messaging shall be prohibited:

i. Spam - sending of unsolicited commercial emails/electronic messages in bulk (identical content to multiple recipients);

ii. Chain letters - creating or forwarding chain letters or pyramid schemes;

iii. Unprofessional Communications - unprofessional or un-businesslike communications in appearance or content;

iv. Alter message content - modification or deletion of email/electronic messages originating from another person or computer with the intent to deceive;

v. False Identity - falsifying email/electronic message headers or routing information so as to obscure the origins of the email/electronic message or the identity of the sender, also known as spoofing;

vi. Mask identity - unauthorized use of anonymous addresses for sending and receiving email/electronic messages;

vii. Auto-forwarding to external accounts - automatically forwarding email/electronic messages sent to a DCS account to an external email/electronic messages without authorization;

viii. Non-DCS email accounts - unauthorized use of a non-DCS email account for DCS business;

ix. Unencrypted Confidential Information - confidential information sent over email or other electronic messaging without adequate encryption (even to an authorized user).

x. Misrepresentation of DCS - presenting viewpoints or positions not held by DCS as those of DCS or attributing them to DCS.

d. Personal use of DCS information systems - personal use of DCS technology assets/information systems shall be limited to occasional use during break periods provided the use does not interfere with DCS information systems or services.

e. Social Media and External Site - DCS-defined restrictions on the use of the following: [NIST 800-53 PL-4(1)]

i. social media, social networking sites, and external sites and applications,

ii. unauthorized posting of DCS information on public websites, and

iii. the use of DCS identifiers (e.g., email address) and authentication secrets for creating accounts on external sites or applications.

f. Violation of intellectual property laws - unauthorized receipt, use or distribution of unlicensed software, copyrighted materials, or communications of proprietary information or trade secrets;

g. Unauthorized access of confidential information - unauthorized access of information that has been classified as Confidential could cause harm to the state and/or the citizens of the state. The confidentiality of information is protected by law. The unauthorized access of any confidential information is prohibited [A.R.S. § 13-2316.07].

h. Unauthorized release of confidential information - disclosure of information that has been classified as Confidential could cause harm to the state and/or the citizens of the state. The confidentiality of information is protected by law. The unauthorized release or disclosure of any confidential information is prohibited [A.R.S. § 36-342] [A.R.S. § 36-666] [A.R.S. § 41-151.12] [A.R.S. § 41-1750.01].

i. Unauthorized posting of DCS documents - unauthorized posting of DCS draft or final DCS documents is prohibited.

3. Notifications and Acknowledgements - The following notifications and acknowledgements shall be used to inform those granted access to organizational information and/or DCS information systems of steps DCS may take to ensure the security of DCS information systems.

a. User responsibility acknowledgement - all users review and acknowledge their understanding of this policy and other related information security policies on an annual basis;

b. Assets and intellectual property - all DCS information system assets remain the sole property of the State of Arizona. Any data or intellectual property created by the user, including voicemail and electronic messages, shall remain the property of the State of Arizona and shall not be removed, copied, or shared with any person or entity except as part of the user's normal job responsibilities;

c. Monitoring - DCS shall inform all users that it reserves the right to monitor all activities that occur on its DCS information systems or to access any data residing on its systems or assets at any time without further notice. DCS shall retain the right to override an

individual's passwords and/or codes to facilitate access by DCS;

d. Potential blocking of inappropriate content - DCS may block access to web content it deems as inappropriate or filter email destined for your mailbox;

e. Incomplete blocking of inappropriate content - DCS shall not be responsible for material viewed or downloaded by users from the internet or messages delivered to a user's mailbox. Users are cautioned that many internet pages and emails include offensive, sexually explicit, and inappropriate material. Even though DCS intends to filter and block inappropriate content and messages, it is not always possible to avoid contact with offensive content on the internet or in one's email. If such an action occurs, users are expected to delete the offensive material, leave the offensive site, and contact DCS IT Security Team;

f. Records retention - files, emails, attachments, and other records are retained, preserved, and/or disposed of in accordance with Arizona State Library Records Retention Schedule, General Records Retention Schedule issued to: All State and Local Agencies Electronic Communications, Social Media, and Website Records Schedule Number GS 1026: azlibrary.gov/sites/default/files/electronic_communications_social_media_website.pdf;

g. No expectation of privacy - users shall have no expectation of privacy for any communication or data created, stored, sent, or received on DCS information systems and assets; and

h. User acknowledgement - by using DCS information systems, users shall acknowledge that they explicitly consent to the monitoring of such use and the right of DCS to conduct such monitoring.

C. Virtual Office Agreement - DCS shall ensure that individuals utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access DCS information systems as a trusted user acknowledge and accept appropriate access agreements prior to being granted access and shall review, and if necessary, update agreements annually.

1. Assigning Responsibility to Provide Policy - DCS shall assign responsibility to a department, role, or named individual to provide acceptable use and other related information security policies to employees and contractors.

2. Assigning Responsibility to Keep Records - DCS shall assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

D. Virtual Office Access Agreement Contents - The Virtual Office Access agreements shall contain the following additional policy sections and statements:

1. Allowable Computing Devices - an individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access DCS information systems as a trusted user providing and storing Confidential information shall ensure:

   a. the computing equipment is issued to the individual by DCS for the purposes of connecting to a DCS information system; or

   b. the computing equipment is owned or otherwise under the control of the individual such that the individual may ensure minimum physical and logical protections are in place.

2. Physical Protection of Computing Devices - an individual utilizing computing equipment outside of designated work environments (e.g., virtual offices, working from home, telework centers) to access DCS information systems as a trusted user providing and storing Confidential information shall ensure that computer equipment is:

   a. physically protected from unauthorized use and removal; and

   b. limited to the use of the authorized virtual office user. Use of the computer equipment by anyone else (e.g., family members, roommates) is strictly forbidden.

3. Logical Protection of Computing Devices - an individual utilizing computing equipment outside of designated work environments (e.g.,

virtual offices, working from home, telework centers) to access DCS information systems as a trusted user providing and storing Confidential information shall ensure that computer equipment has the following logical security controls:

a. username and passwords - identification and authentication controls consistent with the DCS Identification and Authentication Policy (DCS 05-8340);

b. anti-virus - malicious code protection consistent with the DCS System Security Maintenance Policy (DCS-05-8220), with the exception of central management of malicious code protection;

c. personal firewalls consistent with the DCS Access Control Policy (DCS-05-8320);

d. full device encryption consistent with the DCS Access Control Policy (DCS 05-8320); and

e. security patches – installing security-relevant software and firmware updates consistent with the DCS System Security Maintenance Policy (DCS-05-8220).

4. Remote Access – virtual office users may access DCS information system only by approved access methods.

E. User-Based Technologies - DCS shall ensure that individuals utilizing user-based technologies (e.g., smart phones, tablet computers) to access DCS information systems as a trusted user acknowledge and accept appropriate access agreements (prior to being granted access), and shall review, and if necessary, update agreements annually.

1. Assigning Responsibility to Provide Policy - DCS shall assign responsibility to a department, role, or named individual to provide user-technology standards, acceptable use, and other related information security policies to employees and contractors.

2. Assigning Responsibility to Keep Records - DCS shall assign responsibility to a department, role, or named individual to keep records of distributed, acknowledged, and accepted acceptable use policies for employees and contractors.

F. User-Based Technology Agreement Contents - The user-based technology access agreements shall be developed by DCS and contain DCS-defined security controls. The DCS System Security Maintenance Policy (DCS 05-8220) provides guidance to DCS for minimum recommended user-based technology controls. Such agreements shall include the following, at a minimum:

1. explicit approval by authorized parties;

2. authentication for use of the technology;

3. a list of all such devices and personnel with access;

4. a method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices);

5. acceptable uses of the technology;

6. acceptable network locations for the technologies;

7. list of DCS-approved products;

8. automatic disconnect of sessions for remote-access technologies after a specific period of inactivity;

9. activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use;

10. for personnel accessing Confidential data via remote-access technologies, prohibit the copying, moving, and storage of Confidential data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable requirements.

G. Consequences for Non-Compliance - Users of DCS information systems who fail to comply with established information security and privacy policies and procedures may be subject to sanctions, including referral to law enforcement

agency for appropriate action [NIST 800 53 PS-8] [HIPAA 164.308(a)(1)(ii)(C)] [HIPAA 164.530(e)(1),(2)].

1. DCS Employees - State Personnel System (SPS) Rule R2-5A-501, Standards of Conduct, requires that all State employees comply with federal and state laws and rules, statewide policies, and employee handbook and DCS policy and directives. As provided by SPS Rule R2-5A-501(C), an employee who fails to comply with standards of conduct requirements may be disciplined or separated from state employment.

2. DCS Contractors - DCS contractors violating federal and state laws and rules, statewide policies, and DCS policy and directives may result in, but not be limited to, immediate credential revocation, terminations of permissions for access to data systems and physical locations, and barring entry or access permanently. Vendors providing services under a contract are subject to vendor performance reports, and any contract terms and warranties, including potential damages.

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
15 Aug 2023	Updated to NIST 800-53 Rev 5 and change policy number from DCS 05-013 to DCS 05-8280 Acceptable Use Policy	2	Frank Sweeney DCS CIO

	for better tracking with Arizona Department Homeland Security (AZDoHS) policy numbers.		
30 Jun 2024	Annual updates to meet AZDoHS updated Policy	3	DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 7/8/2024 Frank Sweeney Chief Information Officer AZDCS