TITLE	POLICY NUMBER	
Supply Chain Risk Management Policy	DCS 05-8347	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	August 15, 2023	

I. POLICY STATEMENT

The purpose of this policy is to establish security controls for the management of supply chain risks associated with secure operations of DCS systems and services.

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 DCS Information Technology Policies, Standards, and Procedures (PSPs) within DCS;

2. ensure DCS compliance with the Supply Chain Risk Management Policy;

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 the Supply Chain Risk Management Policy is periodically reviewed and updated to reflect changes in requirements.

C. The DCS Information Security Officer (ISO) 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 Supply Chain Risk Management Policy for DCS.

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. Supply Chain Risk Management Plan

1. DCS shall develop a plan for managing supply chain risks associated with acquisition, delivery, integration, operations and maintenance, and disposal of the information systems and services.

2. The Supply Chain Risk Management (SCRM) plan should provide the basis for determining whether a technology, service, or information system is fit for purpose and as such the controls need to be tailored accordingly. The SCRM plan shall include the following:

a. an expression of the supply chain risk tolerance for the agency;

b. acceptable supply chain risk mitigation strategies or controls;

c. a process for consistently evaluating and monitoring supply chain risk;

d. approaches for implementing and communicating the plan;

e. a description of and justification for supply chain risk mitigation measures taken; and associated roles and responsibilities.

3. DCS shall review and update the supply chain risk management plan on an annual basis or as required, to address threat, organizational, or environmental changes.

4. DCS shall protect the supply chain risk management plan from unauthorized disclosure and modification.

B. Supply Chain Risk Management (SCRM) Team

The following shall be implemented.

1. Establish a supply chain risk management team that consists of the agency-defined roles and is responsible for identifying, assessing, and managing risks while using coordinated efforts.

2. The SCRM team shall consist of personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executives, information technology, contracting, information security, privacy, mission, or business, legal, supply chain and logistics and acquisition.

3. The SCRM team shall be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

C. Supply Chain Controls and Processes.

The following shall be implemented.

1. Establish processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of information systems in coordination with the identified supply chain personnel.

    a. Supply chain elements include organizations, entities, or tools employed for the acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components.

    b. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components.

2. Employ the following controls to protect against supply chain risks to information assets, systems, system components, or system services and to limit the harm or consequences from supply chain related events (examples):

a. Control Assessments (CA-2);

b. External System Services (SA-9);

c. Acquisition Process (SA-4);

d. Controlled Maintenance (MA-2);

e. Component Authenticity (SR-11);

f. Component Disposal (SR-12).

3. Document the selected and implemented supply chain processes and controls in an agency defined document such as a SCRM plan.

D. Acquisition Strategies, Tools, and Methods

Acquisition strategies, contract tools, and procurement methods shall be employed to protect against, identify, and mitigate supply chain risks. Examples are as follows:

1. including incentive programs to system integrators, suppliers, or external services providers to ensure that they provide verification of integrity as well as traceability.

2. requiring tamper-evident packaging;

3. using trusted or controlled distribution.

E. Supplier Assessments and Reviews

1. Supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide shall be assessed and reviewed annually. An assessment and review of supplier risk should include security and supply chain risk management processes, foreign ownership, and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors.

2. The reviews shall consider documented processes, documented controls, and publicly available information related to the supplier or contractor.

F. Notification Agreements

1. Agreements and procedures with entities involved in the supply chain

shall be established for the notification of supply chain compromises including security incident and a privacy breach and the notification of assessment or audit results.

G. Inspection of Systems or Components

DCS shall develop:

1. a process to inspect information systems annually or upon any indications of the tampering of information systems shall be implemented;

2. indications of a need for inspection including changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

H. Component Authenticity

DCS shall:

1. develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system;

2. report counterfeit system components to the agency-defined personnel. Organizations should include in their anti-counterfeit policy and procedures, a means to help ensure that the components acquired and used are authentic and have not been subject to tampering.

I. Component Authenticity/Anti-Counterfeit Training

The following agency-defined roles shall be trained to detect counterfeit system components (including hardware, software, and firmware):

1. personnel conducting configuration management activities;

2. system administrators;

3. database administrators;

4. network administrators;

5. procurement personnel.

J. Component Authenticity/Configuration Control for Component Service/Repair

Configuration control shall be maintained over system components awaiting service or repair and serviced or repaired components awaiting return to service. Organizations shall manage risks associated with component repair including the repair process and any replacements, updates, and revisions of hardware and software components within the supply chain infrastructure.

K. Component Disposal

DCS-defined data, documentation, tools, or system components shall be disposed of without exposing sensitive or operational information, which may lead to a future supply chain compromise. Examples include the following:

1. monitoring and documenting the chain of custody through the destruction process;

2. training disposal service personnel to ensure accurate delivery of service against disposal policy and procedures;

3. implementing assessment procedures for the verification of disposal processes with a frequency that fits agency needs;

4. using media sanitization techniques—including clearing, purging, cryptographic erase, deidentification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal.

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
15 Aug 2023	Initial Release with compliance to NIST 800-53 Rev 5 and created policy number DCS 05-8347 for better tracking with Arizona Department Homeland Security (AZDoHS) policy numbers.		DocuSigned by: Frank Sweeney CDB46EB4E4A6442... 8/31/2023 Frank Sweeney Chief Information Officer AZDCS