CONNECTICUT

Department of Children & Families

Information Security Policy 2-4S

Social Security Administration (SSA) Supplemental Controls

VERSION 1.0

EFFECTIVE DATE: OCTOBER 01, 2025

Policy Statement

The Connecticut Department of Children and Families' (DCF) core values are:

- **Our vision:** That CT's children are safe and sound within loving and supportive families.
- **Our mission**: Partnering with communities and empowering families to raise resilient children who thrive.
- **Our goals**: To focus on six areas: safety, permanency, racial justice, child & family wellbeing, workforce, and prevention.

This policy serves as a statement of DCF's commitment and oversight for safeguarding its data and information systems.

Contents

Policy Statement **1**
Version History **3**
Scope **3**
Next review **3**
Information Security Policy Purpose **3**
Roles and Responsibilities 4
Children and Familiess (DCF) 4
Administrative Services, Bureau of Information Technology Services (DAS-BITS) 4
NIST Defined Key Roles 4
State of Connecticut Policies **6**
Office of Policy and Management (OPM) 6
Administrative Services - Bureau of Information Technology Solutions (DAS-BITS) 6
Security Controls **7**
Access Control 7
Audit and Accountability 9
Awareness and Training 12
Identification and Authentication 13
Incident Response 13
Media Protection 15
Personnel Security 16
Physical and Environmental Protection 16
Planning 17
Risk Assessment 17
Assessment, Authorization, and Monitoring 18
System and Communications Protection 19
System and Information Integrity 19
System and Services Acquisition 21
Definitions **22**
References **23**

Version History

Version	Sections Revised	Description of Revisions	Date
1.0	ALL	New policy and procedures suite	10/01/2025
		Approval Date Issued	
		Communication, dissemination and publication	
1.x			

Scope

Once approved, communication and dissemination of the supplemental policy will be provided via email to inform DCF employees, contractors, service providers, third parties and all other authorized parties to whom it applies.

Internal publication will be made available on the DCF intranet, under the menu policy & procedures.

Next review

3-year cyclical review from date signed or if any significant changes warrant an out-of-cycle review.

Information Security Policy Purpose

The purpose of this information security policy serves to provide the foundational oversight framework of collective compliance requirements, information technology policies and standards brought together to protect the confidentiality, integrity, availability of sensitive information processed, stored or transmitted in DCF's information systems.

Roles and Responsibilities

Children and Families (DCF)

As a state agency serving residents through its programs, information is collected and received to determine eligibility of services. The agency's Information Exchange Agreement (IEA) with the Social Security Administration (SSA) details compliance requirements for the SSA data it receives.

Administrative Services, Bureau of Information Technology Services (DAS-BITS)

A Memorandum of Understanding (MOU) sets forth the agreement for centralized IT services that include procedures and processes necessary for satisfying the information systems' needs.

NIST Defined Key Roles

The National Institute of Standards and Technology (NIST) has defined key roles and responsibilities in its Introduction to Computer Security Handbook, common roles are:

- User
  - The User is an individual, group, or organization granted access to organizational information in order to perform assigned duties.
  - Responsibilities include:
    - Adhering to policies that govern acceptable use of organizational systems.
    - Using the organization-provided IT resources for defined purposes only; and
    - Reporting anomalies or suspicious system behavior.

- System Administrator
  - The System Administrator is an individual, group, or organization responsible for setting up and maintaining a system or specific components of a system.
  - Responsibilities include:
    - Installing, configuring, and updating hardware and software.
    - Establishing and managing user accounts.

- Overseeing backup and recovery tasks; and
- Implementing technical security controls

❖ System Owner
- ➢ The System Owner also referred to as an application owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system.
- ➢ Responsibilities include:
  - Addressing the operational interests of the user community (i.e., users who require access to the system to satisfy mission, business, or operational requirements).
  - Ensuring compliance with information security requirements; and
  - Developing and maintaining the system security plan and ensuring that the system is deployed and operated in accordance with the agreed-upon security controls.

❖ System Security Officer (SSO)
- ➢ The System Security Officer is responsible for ensuring that an appropriate operational security posture is maintained for a system and as such, works in close collaboration with the system owner.
- ➢ Responsibilities include:
  - Overseeing the day-to-day security operations of a system; and
  - Assisting in the development of the security policies and procedures and ensuring compliance with those policies and procedures.

❖ Common Control Provider
- ➢ The Common Control Provider is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls also referred to as security controls.
- ➢ Responsibilities include:
  - Documenting the organization-identified common controls in a security plan (or equivalent document prescribed by the organization), and

- Ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization.

State of Connecticut Policies

Office of Policy and Management (OPM)

OPM[1] is responsible for developing and implementing an integrated set of policies governing the use of information and telecommunications systems for state executive branch agencies.

- Acceptable Use Policy
- Accessibility & Inclusivity Policy for Websites and Digital Assets
- Electronic Mail Records Management Policy
- Data Classification Policy
- Information Technology Policy Governance Process
- Personal Wireless Device Policy

Administrative Services - Bureau of Information Technology Solutions (DAS-BITS) [2]

DAS adopts procedures and processes necessary for satisfying the information systems needs of state executive branch agencies as per the Memorandum of Understanding (MOU) by and between the Department of Children and Families and the Department of Administrative Services.

DAS-BITS' role and responsibilities for common controls (security controls) are detailed in part in the next section.

[1] Connecticut General Statutes § 4d-8a Office of Policy and Management

[2] Connecticut General Statutes § 4d-2 Department of Administrative Services – Bureau of Information Technology Services

Security Controls

Security controls are measures implemented to protect information systems. The following list the relevant SSA security controls that require coordination among organizational entities.

Access Control

Access Control (AC) security control is managed by DAS-BITS. DCF approval is required before DAS-BITS can grant access to DCF information systems.

Account Management (AC-2)

a. Define and document the types of accounts allowed and specifically prohibited for use within the system.
b. Assign account managers.
c. DCF has defined prerequisites and criteria for group and role membership.
d. Specify:
    1. Authorized users of the system are approved by DCF in order for DAS-BITS to action access requests.
    2. Group and role membership; and
    3. Access authorizations (i.e., privileges) and DCF-defined attributes (as required) are provided for each account.
e. Approvals by DCF supervisory managers required for requests to create accounts.
f. Create, enable, modify, disable, and remove accounts in accordance with DCF-defined policy, procedures, prerequisites, and criteria.
g. Monitor the use of accounts.
h. Notify DAS-BITS Help Desk within 24 hours when: accounts are no longer needed; users are terminated or transferred; and system usage or need-to-know changes for an individual.
i. DAS-BITS will authorize access to the system based on:
    1. A valid access authorization.
    2. Intended system usage; and
    3. DCF-defined attributes for roles and system permissions.

j. Review accounts for compliance with account management requirements annually for user account and semi-annually for privileged accounts.
k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
l. Align account management processes with personnel termination and transfer processes.

Access Enforcement (AC-3)

Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Separation of Duties (AC-5)

Identify and document the duties of individuals requiring separation.

Least Privilege (AC-6)

Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Least Privilege | Authorize Access to Security Functions (AC-6) (1)

Authorize access to security functions (software) for defined individuals and roles with a security-relevant information requirement.

Least Privilege | Review of User Privileges (AC-6) (7)

Review the privileges assigned to organization-defined roles or classes of users to validate the need for such privileges.

Unsuccessful Logon Attempts (AC-7)

Enforce a limit of three (3) consecutive invalid logon attempts by a user during a 120-minute period.

The account remains locked until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

System Use Notification (AC-8)

Display a warning banner to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

Users are accessing a U.S. Government System.
System usage may be monitored, recorded, and subject to audit.
Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
Use of the system indicates consent to monitoring and recording.

Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

Device Lock (AC-11)

Prevent further access to the system by initiating a device lock after a maximum of 15 minutes of inactivity; requiring the user to initiate a device lock before leaving the system unattended; and

Retain the device lock until the user re-establishes access using established identification and authentication procedures.

Remote Access (AC-17)

Establish and document usage restrictions, configuration/connection requirements and implementation guidance for each type of remote access allowed. Authorize each type of remote access to the system prior to allowing such connections.

Audit and Accountability

Audit and Accountability (AU) security control is managed by DAS-BITS for the state network.

Event Logging (AU-2)

Identify the types of events that the system is capable of logging in support of the audit function:

a. Logon activities.
b. Logoff activities.
c. Activities that might modify, bypass, or negate IT security safeguards.
d. Password changes.
e. Creation or modification of groups.
f. Privileged user actions.
g. Access to the system.
h. Creating and deleting files.
i. Change of permissions or privileges.
j. Command line changes and queries.
k. Changes made to an application or database.
l. System and data interactions.
m. Opening and/or closing of files; and
n. Program execution activities.

Content of Audit Records (AU-3)

Audit records contain information that establishes the following:

a. What type of event occurred.
b. When the event occurred.
c. Where the event occurred.
d. Source of the event.
e. Outcome of the event; and
f. Identity of any individuals, subjects, or objects/entities associated with the event.

Audit Storage Capacity (AU-4)

Audit log storage capacity is allocated to accommodate the retention of audit records for the retention period.

Audit Review, Analysis and Reporting (AU-6)

Review and analyze system audit records weekly for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.

Report findings to the individual(s) specified within the agency's incident response procedures.

Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk-based information, intelligence information, or other credible sources of information.

Audit Reduction and Report Generation (AU-7)

Provide and implement an audit record reduction and report generation capability that:

Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

Does not alter the original content or time ordering of audit records.

Time Stamps (AU-8)

Use internal system clocks to generate time stamps for audit records.

Record time stamps for audit records that meet agency-defined granularity and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Protection of Audit (AU-9)

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Alert security officer immediately upon detection of unauthorized access, modification, or deletion of audit information.

Audit Record Retention (AU-11)

Retain audit records seven (7) years to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

Audit Generation (AU-12)

Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 on all systems that receive, process, store, access, protect and/or transmit SSA data.

Allow the system administrator and security officer to select the event types that are to be logged by specific components of the system.

Generate audit records for the event types defined in AU-2 that include the audit record content defined in AU-3.

Awareness and Training

Awareness and Training (AT) is a shared security control with DAS-BITS, DCF and DCF's Academy for Workforce Development that provides the DSS Data Disclosure Training.

Literacy Training and Awareness (AT-2)

Provide security and privacy literacy training to system users (including managers, senior executives, and contractors) as part of initial training for new users and annually thereafter.

Annual DSS Data Disclosure Training (security and privacy) for users of SSA data.

Role-Based Training (AT-3)

a. Provide role-based security and privacy training to personnel with the SSA-related roles and responsibilities:
    1. Before authorizing access to the system, information, or performing assigned duties, and annually thereafter.

The DSS Data Disclosure training includes:

- The sensitivity of SSA data,
- The rules of behavior concerning use and security in systems and/or applications processing SSA data,
- The Privacy Act and other Federal and State laws governing collection, maintenance, use, and dissemination of information about individuals,

- The possible criminal and civil sanctions and penalties for misuse of SSA data,
- The responsibilities of employees, contractors, and agents pertaining to the proper use and protection of SSA data,
- The restrictions on viewing and/or copying SSA data,
- The proper disposal of SSA data,
- The security breach and data loss incident reporting procedures.

Training Records (AT-4)

Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

Retain individual training records for a period of at least five (5) years.

Identification and Authentication

Identification and Authentication (IA) security control is managed by DAS-BITS.

Identification and Authentication - Organizational Users (IA-2)

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Authenticator Management (IA-5) (1)

Password-based authentication

Enforce the following composition and complexity rules: Minimum 10-characters, at least one Uppercase, lowercase, number and special character.

Incident Response

Incident Response (IR) security control is managed by DAS-BITS who coordinates with all state agencies.

SSA Incident Response Procedure:

If your agency experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center (NNSC) toll free at 1-877-697-4889 (select "Security and PII Reporting" from the options list). The Electronic Information Exchange Partner (EIEP) will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.

Incident Response Training (IR-2)

Provide incident response training to system users consistent with assigned roles and responsibilities:

1. Within 30 days of assuming an incident response role or responsibility or acquiring system access.
2. When required by system changes; and
3. Annually thereafter.
4. Review and update incident response training content every three (3) years and following major business and system change impacting the environment.

Incident Handling (IR-4)

Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery. Coordinate incident handling activities with contingency planning activities.

Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.

Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Incident Response Plan (IR-8)

Develop an incident response plan that:

Provides the organization with a roadmap for implementing its incident response capability.

Describes the structure and organization of the incident response capability.

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

Meets the unique requirements of the organization, which relate to mission, size, structure, and functions.

Defines reportable incidents.

Provides metrics for measuring the incident response capability within the organization.

Defines the resources and management support needed to effectively maintain and mature an incident response capability.

Addresses the sharing of incident information.

The incident response plan is reviewed and approved by designated agency officials at a minimum on an annual basis.

Explicitly designates responsibility for incident response to agency-defined personnel.

Media Protection

Media Protection (MP) security control is managed by DAS-BITS.

Media Access (MP-2)

Restrict access to digital and/or non-digital media.

Media Sanitization (MP-6)

Sanitize media containing SSA data prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies.

Personnel Security

Personnel Security (PS) is a security control shared with DAS-BITS.

Personnel Screening (PS-3)

Screen individuals prior to authorizing access to the system.

Rescreening of individuals as required for non-employees.

Personnel Termination (PS-4)

Upon termination of individual employment:

Disable system access within three (3) business days.

Retrieve all security-related organizational system-related property.

Retain access to organizational information and systems formerly controlled by terminated individuals.

Physical and Environmental Protection

Physical and Environmental Protection (PE) is managed by DAS-BITS.

Physical Access Control (PE-3)

Enforce physical access authorizations at entry/exit points to facilities where the information systems that receive, process, store, access, or transmit SSA data by:

1. Verifying individual access authorizations before granting access to the facility; and

2. Controlling ingress and egress to the facility using organization-defined physical access control systems, devices or guards.

Maintain physical access audit logs for data center entry or exit points.

Escort visitors and control visitor activity in accordance with agency policies (e.g., personnel and physical security).

Monitoring Physical Access (PE-6)

Review physical access logs at a minimum monthly and upon occurrence of a potential indication of an event.

Planning

Planning (PL) is a security control shared with DAS-BITS.

System Security and Privacy Plans (PL-2)

Develop security and privacy plans for the system that detail information specific to safeguarding SSA data:

- Explicitly define the constituent system components.
- Describe the operational context of the system in terms of mission and business processes.
- Identify the individuals that fulfill system roles and responsibilities.
- Describe the operational environment for the system and any dependencies on or connections to other systems or system components.
- Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions.
- Review the plans at a minimum annually (or as a result of a significant change)

Risk Assessment

Risk Assessment (RA) is a security control shared with DAS-BITS.

Vulnerability Scanning and Monitoring (RA-5)

Monitor and scan for vulnerabilities in the system and hosted applications every thirty (30) days, prior to placing a new information system on the agency network, to confirm remediation actions, and when new vulnerabilities potentially affecting the system are identified and reported.

Analyze vulnerability scan reports and results from vulnerability monitoring.

Remediate legitimate vulnerabilities in accordance with an agency assessment of risk.

Share information obtained from the vulnerability monitoring process and control assessments with security personnel to help eliminate similar vulnerabilities in other systems.

Assessment, Authorization, and Monitoring

Assessment, Authorization and Monitoring (CA) is a security control shared with DAS-BITS.

Control Assessments (CA-2)

Select the appropriate assessor or assessment team for the type of assessment to be conducted.

Develop a control assessment plan that describes the scope of the assessment including:

Assess the controls in the system and its environment of operation annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.

Produce a control assessment report that documents the results of the assessment.

Information Exchange (CA-3)

Approve and manage the exchange of information between the system and other systems using Interconnection Security Agreements (ISAs).

Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated.

Review and update the system interconnection on an annual basis.

Document a data flow diagram that shows how SSA data is accessed by DCF.

Continuous Monitoring (CA-7)

Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:

Establish agency-defined metrics to be monitored.

Reporting the security and privacy status of the system to agency-defined personnel annually, at a minimum.

System and Communications Protection

System and Communications Protection (SC) is managed by DAS-BITS.

Boundary Protection (SC-7)

Monitor and control communications at the external managed interfaces. Provide SSA with a logical network layout as part of the system authorization process.

Transmission Confidentiality and Integrity (SC-8) (1)

Transmission Confidentiality and Integrity | Cryptographic Protection

The organization implements cryptographic mechanisms to DCF information system to prevent unauthorized disclosure of information and detect changes to information during transmission.

Cryptographic Protection (SC-13)

FIPS validated cryptography.

Protection of Information at Rest (SC-28)

Protect the confidentiality and integrity of the DCF information system with SSA data at rest.

System and Information Integrity

System and Information Integrity (SI) is a security control managed by DAS-BITS.

Flaw Remediation (SI-2)

Identify, report and correct system flaws.

Install security-relevant software and firmware updates promptly after the release of the updates.

Incorporate flaw remediation into the organizational configuration management process.

Malicious Code Protection (SI-3)

Implement signature-based and/or non-signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures.

Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system and implement weekly and real-time scans of files from external sources at endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with agency security policy; and

2. Block or quarantine malicious code and send alert to system administrator in response to malicious code detection.

System Monitoring (SI-4)

Monitor the system to detect

attacks and indicators of potential attacks in accordance with the following monitoring objectives as defined by DAS-BITS:

- Unauthorized local, network, and remote connections.
- Identify unauthorized use of the system through a variety of techniques and methods.

- Provide the output from system monitoring to the Chief Information Security Officer (CISO) and security personnel (weekly).

Information System Monitoring | System Generated Alerts (SI-4) (5)

System generated alerts from the information system monitoring are sent to DAS-BITS security personnel when indications of compromise or potential compromise occur.

Information Management and Retention (SI-12)

Dispose of, destroy, and/or erase all data received from SSA to administer benefit programs after the required processing of such data for the applicable benefit programs.

System and Services Acquisition

System and Services Acquisition (SA) is a security control shared with DAS-BITS.

External System Services (SA-9)

a. Require that providers of external information system services comply with organizational information security requirements and employ organization-defined security controls in accordance with the SSA Technical System Security Requirements (TSSR), applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
b. Define and document government oversight and user roles and responsibilities with regards to external information system services.
c. Employ organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. The state organization will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing the Agreement, and thereafter at SSA's request, the state organization will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA data and provide such lists to SSA.

Definitions

- Application Owner
  - An application owner is responsible for overseeing the software development lifecycle (SDLC) including security requirements. The application owner ensures that the application aligns with business goals and stakeholder needs.
- Computer System
  - A computer system is any type of hardware or software component that can process information, store data, and perform calculations.
- Information System
  - A computer system or set of components for collecting, creating, storing, processing, and distributing information, typically including hardware and software, system users, and the data itself.
- Personally Identifiable Information (PII)
  - PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
    - PII includes:
      - a person's name
      - date of birth,
      - Social Security Number
      - bank account information
      - address
      - health records, and
      - Social Security benefit payment data.
- Chief Information Security Officer (CISO)
  - A CISO also referred to as a System Security Officer (SSO) or an Agency Information Security Officer (AISO) is a professional responsible for overseeing and implementing an organization's information security strategy to protect against cybersecurity threats and ensure compliance with regulations and standards
- Social Security Administration (SSA)
  - Federal standards require the Social Security Administration (SSA) to maintain oversight of the information it provides to its Electronic Information Exchange Partners (EIEPs).
  - EIEPs must protect the information with efficient and effective security controls. DCF is the recipient of information in the form of data received from the SSA.

References

Social Security Administration

- Computer Matching and Privacy Protection Act (CMPPA) of 1988
- Information Exchange Agreement (IEA)

State of Connecticut Policies

- Office of Policy and Management (OPM)
- Department of Administrative Services – Bureau of Information Technology Services (DAS-BITS)

National Institute of Standards and Technology

Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook

Security and Privacy Controls for Information Systems and Organizations Special Publication (SP) 800-53 Revision 5