CONNECTICUT
Policy and Management

Policy Title:	State of Connecticut Information Security Policy
Originator:	Office of Policy and Management ("OPM")
Effective Date:	January 20, 2026
History:	Version 1.0
Applies to:	State Agencies defined in § 4d-1(3)
Relevant Laws or Regulations:	C.G.S. §§ 4-5, 4-8, 4-65a, 4-66, 4d-1(3), 4d-8a, and § 28-5

Purpose

This document establishes the State of Connecticut's baseline Information Security Policy, which defines the framework for protecting the safety, confidentiality, integrity, and availability of the State of Connecticut's Agencies ("Agencies" or "State Agencies"), people, systems, networks, data, and technology resources. This policy serves as the procedural and definitional foundation for related information security policies issued by OPM, which will provide reference back to this document. Specific baseline controls related to particular security topics and domains will also be established in affiliated documents and provide reference to this policy.

Enabling Authority

In accordance with C.G.S. §§ 4-5, 4-8, 4-65a, 4-66, 4d-1(3), and 4d-8a, the Office of Policy and Management ("OPM") is responsible for developing and implementing an integrated set of policies pertaining to information and telecommunications systems for state Agencies.

Pursuant to C.G.S. § 28-5, the Commissioner, Department of Emergency Services and Public Protection ("DESPP"), is required to prepare a comprehensive civil preparedness plan that, when approved by the Governor, defines the duties of state agencies and other covered entities in supporting emergency response. Among other things, the State Response Framework designates the Department of Administrative Services ("DAS") – Bureau of Information Technology Services ("BITS") as the coordinating agency responsible for planning, response and recovery from cyber incidents (Emergency Support Function-17 ("ESF-17")). In executing this role, among other actions, the State Chief Information Security Officer ("CISO") adopts and publishes a biennial State of Connecticut Cybersecurity Strategy, providing a roadmap to implement statewide information security initiatives.

Scope & Applicability

This policy applies to State of Connecticut Agencies defined in General Statutes section 4d-1(3).

This policy applies to all employees, fellows, interns, consultants, contractors, and partners, paid or unpaid, and to all state data, resources, networks, equipment, and/or other information technology

assets. Any agreements with vendors, partners, consultants, intermediaries shall contain language clearly referencing this policy.

Other branches of government, including the Legislature and the Judiciary, are encouraged to adopt similar standards. State Agencies working under an optimization Memorandum of Understanding ("MOU") DAS should engage with DAS-BITS to support the development, maintenance and execution of appropriate Agency-level plans, when needed, in support of this Statewide policy. Such implementations may be specific to an Agency, or common among similar agencies (particularly those under an optimization MOU).

Information Security Governance Overview

The State of Connecticut defines information security governance as the establishment, maintenance, and support of a security framework aligning with and supporting State and Agency objectives with applicable laws and regulations to manage risks. Consistent with the State Response Framework, the State of Connecticut Cybersecurity Strategy and state law, DAS-BITS and the CISO are establishing and implementing a statewide Information Security Program to align the State's processes, standards and procedures with established, widely recognized guidelines to support State employees and systems. This Information Security Program is based on industry leading standards including relevant publications by the National Institute of Technology Standards, Center for Internet Security, SANS Technology Institute, the Internal Revenue Service, the Federal Bureau of Investigation's Criminal Justice Information System, Payment Card Industry Data Security Standard, and the Health Insurance Portability and Accountability Act.

Governance Structure

OPM and the CISO, including DAS-BITS, provide governance of Information Security practices through policies, plans, standards, strategies, methodologies, guidelines, and procedures.

Policies

Policies provide high-level statements relating to the protection of information and systems across our statewide environment and are approved and published by OPM as outlined in the State's IT Policy Governance Process to protect the State's Agencies and organizations against unnecessary risks. Policies outline security roles and responsibilities, define the scope of information to be protected, and provide a high-level description of the baseline controls that must be in place to protect information technology assets. These policies, including this Information Security Policy, provide a baseline for State Agencies in conducting their IT operations.

Plans

Plans are governance documents that define the framework for Agency-specific security programs including the people, processes, and technology necessary to effectuate a policy. An example is the Incident Response Plan template, which provides a model for an Agency's own incident response program that would enable an Agency to identify, contain, and respond to security incidents quickly, collaboratively and effectively.

For State Agencies working under an optimization MOU, DAS-BITS will generally support the development, maintenance and implementation of appropriate Plans, when needed, in support of a Statewide policy. Such plans may be specific to an Agency, or common among similar agencies (particularly those under an optimization MOU). For example, in the incident response context, an optimized agency may rely on a DAS-BITS plan which identifies specific DAS-BITS personnel to intake incident reports from Agency staff and elevate incidents within DAS when required.

Agencies that do not operate under an MOU with DAS may rely on a Statewide policy if it is sufficient for the specific Agency's circumstances, or they may supplement the Statewide policy with an Agency-specific plan. For example, in the incident response context, an Agency-specific plan may specify personnel within that Agency to serve as the response team, and an Agency-specific reporting mechanism.

Standards

Standards provide specific functional mandatory controls that enforce and support an Agency-level Information Security Policy or Plan. These low-level mandatory controls usually relate to the implementation of specific technology, hardware, or software utilized by the Agency. Standards are typically created by technical teams in coordination with technology owners and are approved by the CISO to ensure alignment with Information Security Policies, Agency goals, Federal standards and obligations where applicable, as well as industry best practices.

Methodologies

Methodologies are sets of widely accepted principles, tools, and practices which are used to guide processes to achieve particular goals. An example of a methodology is the commonly employed Software Development Life Cycle Methodology which defines the series of phases that provide a model for the secure creation, development, and management of an application.

Guidelines

Guidelines are recommendations to help support adopted standards and should be viewed as best practices. For example, guidelines may be adopted to help secure an Agency employee's home or telework locations to better protect State's information or data while away from State office locations.

Standard Operating Procedures (SOPs)/Procedures

Procedures provide step-by-step instructions to help with implementing the various policies, standards, and guidelines. All procedures need to have specifics explaining how to implement or use the controls for the stated technology. For example, procedures may be written to explain how to install a specific server by detailing each step needed to install the servers consistent with the applicable policy, standards, and guidelines for securing the system.

Mandatory vs. Recommended Requirements

In all statewide information security policies, the terms **"SHALL"** and **"SHOULD"** carry specific meanings.

"SHALL" designates a **mandatory minimum requirement** with which State Agencies, third-party providers, and covered personnel **must comply** unless a documented, **approved** exception or approved compensating control is in place. Consistent with NIST standards, a compensating control in this context is an alternative management, operational and/or technical safeguard implemented when standard security controls are not practical due to technical, operational or business constraint, ensuring equivalent protection for information systems. **Non-compliance with a "SHALL" requirement constitutes a policy violation and may result in possible disciplinary action, required remediation, trigger reporting requirements or adverse audit findings.**

In contrast, **"SHOULD"** designates a **recommended or best-practice measure** that Agencies are encouraged, but not required, to adopt. Where an Agency elects not to follow a "SHOULD" recommendation, it **must document the rationale and any compensating controls** as part of Statewide risk management process and submit the rationale documentation to BITS (as detailed below). No approval is required (only documentation and submission).

This convention aligns with federal compliance regimes such as IRS Publication 1075, CJIS Security Policy, HIPAA, and NIST standards, ensuring clarity for implementers and auditors.

Exceptions or Deviations from Information Security Policies and Other Required Notices

Any anticipated exception or deviation from this or any related information security policy, or any part of the plans or standards adopted pursuant to thereto, must be submitted in advance as a BITS Service Desk ticket.

An "**exception**" in this context is a practice that falls **below** the minimum requirements established by an information security policy.

A "**deviation**" in this context is a practice that is in **excess** of the minimum requirements established by an information security policy.

Where an **exception** relates to a "**SHALL**" requirement, **approval** must be obtained prior to implementation. The DAS-BITS and/or OPM will assess the risk of a submitted exception and the adequacy of any proposed compensating control and conclude if the risk is acceptable. When approved, DAS-BITS will notify the Agency and catalog the exception.

Where the **exception** relates to a "**SHOULD**" requirement or an Agency specific plan, standard, methodology or procedure in excess of the minimum statewide policy, **notice** must be made to DAS-BITS prior to implementation. DAS-BITS will catalog the exception, including a copy of the Agency-specific document, where applicable.

Notice and associated documentation related any **deviation** from a "**SHALL**" or "**SHOULD**" requirement must be submitted to DAS-BITS prior to implementation.

Roles and Responsibilities

- **Agency Heads** SHALL ensure Agency and constituent department compliance, and designate resources responsible for coordinating and achieving compliance with this and related information security policies.

- **Agency Business Owners** are the executive stakeholders who have ownership of specific types of information, applications, and business systems within their Agencies. Business owners SHALL be responsible for authorizing access to systems, applications, and data and making good decisions to keep them secure. Business owners are responsible for communicating business initiatives and information security practices that may have security implications, as well as requesting exceptions from mandatory requirements notifying BITS of other deviations before proceeding with any commitment or change that would otherwise be against policy. Business owners SHALL annually review their Agency's exceptions and deviations and communicate with BITS regarding any changes related to these or necessitated by changes to Agency's practices or systems/IT assets, or its regulatory, legal or other obligations. Business owners SHALL be identified in the Agency's annual high-value data inventory.

- **System, Application, Asset and Data Owners (within DAS-BITS and Agencies)** ensure IT systems are built, configured, and managed in a manner meeting or exceeding state and Agency security policies, plans and procedures; engage with leadership on technology objectives; and deliver systems for executing the Agency's services. System, Application, Asset or Data Owners are also responsible for keeping an accurate inventory of systems and remediating known vulnerabilities, risks, and threats.

- **Software Developers** develop secure Agency applications and system components. Developers' responsibilities include, but are not limited to, developing software in accordance with State of Connecticut and Agency policies, plans standards, methodologies, and procedures.

- **CISO** is accountable for the State of Connecticut Information Security Program including developing the biannual State of Connecticut Cybersecurity Strategy; compliance with security policies as well as development and compliance with standards, guidelines, plans, and procedures; orchestration of security programs, projects, and initiatives; approval of technology initiatives; and incorporation of security language in contracts.

BITS Information Security Personnel serve as the escalation point for security and risk matters, direction of fraud and information security investigations, and coordination/remediation of incident response efforts. They engage in the support, creation, maintenance, and/or distribution of Agency Incident Response Plans, and training of incident response personnel.

- **Administrators and/or Privileged Users** have privileged access to systems and information; such access is only to be used when appropriate per articulated job functions. Administrator or

privileged accounts shall be used when required for approved modifications and/or changes, and not for everyday user account activity.

- **Third-party vendors and service providers** perform functions for the State of Connecticut and/or its Agencies, including software development, while remaining a separate business entity. Because the State does not have direct oversight and monitoring of such entity, it must rely on the inclusion of contractual provisions in third-party contracts regarding security, ownership, risk acceptance, and adherence to applicable State policies and boilerplate. Accountability of third-party vendors and service providers shall include at minimum contractual provisions requiring:
    - Adherence to the State of Connecticut's policy requirements, standards, and guidelines for accessing systems, services, and data.
    - Due diligence for evaluating security risks of third-party providers' services.
    - Lawful purging or destruction of State of Connecticut data upon completion of services consistent with applicable records retention laws or regulations.
    - Notification to the Agency or BITS of any suspected harm or security breach, consistent with the Agency Incident Response Plan.
    - Sub-contractors adhere to the same level of policy, standards or related compliance to which the third-party vendor or service provider is subject.
    - Allowance of State audits and inspections.

  Third-party vendors and service providers accessing or processing regulatory controlled data must maintain compliance with relevant regulatory standards to protect Agencies' data and systems.

Agency Users include employees, fellows, interns, consultants, contractors, and partners, paid or unpaid, that perform work using the State of Connecticut's systems or third-party service providers' systems and applications. Users shall:

- Adhere to all information security policy requirements, standards, and guidelines and timely complete required information security training.
- Create, maintain, and communicate procedures for their roles and responsibilities in accordance with approved policies, plans and standards.
- Report any security concerns to BITS Security and/or Agency Information Security Personnel consistent with State and Agency Incident Response Plans.

Violations

Violations of this policy or related Information Security Policies, Plans or Standards may result in disciplinary action, including those actions outlined in relevant Standards of Conduct and/or Acceptable Use of State Systems Policies.

Reporting

All security concerns, violations or clarifications regarding State of Connecticut Information Security can be sent to *ITPolicyGovernance@ct.gov*. Emails should contain appropriate details to explain the situation and make further contact for follow-up information.

Revision Schedule and Version History

This policy shall be reviewed annually, or more frequently if significant changes in technology, law, or regulation occur. The review will assess the policy's continued relevance, effectiveness, and alignment with State of Connecticut cybersecurity standards, and applicable federal or state requirements and frameworks.

Date	Version	Description	Publisher
January 20, 2026	1.0	Initial Policy	Office of Policy and Management