Policy Title:	State of Connecticut Information Technology Policy Governance Process
Originator:	Office of Policy and Management ("OPM")
Effective Date:	July 25, 2025
History:	Version 1.0
Relevant Laws or Regulations:	C.G.S. §§ 4-5, 4-8, 4-65a, 4-66, 4d-1(3), and 4d-8a.

I.   Information Technology Policy Governance

Recognizing that the statutory responsibility for the development and implementation of integrated state information technology (IT) and telecommunications policy lies with the Office of Policy and Management (OPM), pursuant to C.G.S. Secs. 4-5, 4-8, 4-65a, 4-66, 4d-1(3) and C.G.S. Sec. 4d-8a, and the operational role the Department of Administrative Services (DAS) Bureau of Information Technology Solutions (BITS) plays in managing the state's IT infrastructure and in both executing established IT policies and in development of procedures and practices that support OPM's IT policy development, OPM and DAS have developed an IT Policy Governance structure to identify and assist OPM in prioritizing the state's needs in this context.

The primary goals of the governance structure are to ensure that OPM's IT policies are:

1. Well-structured, effective, efficient and aligned with the State's mission, strategic objectives, and financial resources;

2. Routinely reviewed and updated to reflect evolving policies, priorities, objectives, and technological changes; and

3. Effectively communicated and implemented by state agencies.

In addition, the governance structure will help ensure alignment between OPM's IT policies and related strategic plans and processes for IT and data, specifically:

1) The annual "information and telecommunication systems strategic plan" (IT strategic plan), established through C.G.S. Sec. 4d-7, which is required to be developed "in accordance with the policies established by the Office of Policy and Management."

2)   The work of the Information and Telecommunication Systems Executive Steering Committee when convened under C.G.S. Sec. 4d-12;

3) The biennial state data plan, established through C.G.S. Sec. 4-67p, which requires that "information technology-related actions and initiatives of all executive branch agencies, including, but not limited to, the acquisition of hardware and software and the development of software, shall be consistent with the final state data plan."

More specifically, the governance structure aims to provide a mechanism to develop recommendations to OPM for IT policies that support the following objectives:

- **Establish Clear Guidelines**: Develop and maintain policies that provide a clear framework for decision-making and operational consistency across the state's executive agencies.
- **Promote Accountability**: Ensure that policies define roles, responsibilities, and expectations for all stakeholders within the state utilizing stakeholder engagement and appropriate documentation.
- **Enhance Transparency**: Contribute to the creation of policies that foster openness and trust, making expectations clear to both internal and external stakeholders.
- **Encourage Adaptability**: Develop and execute a regular review cadence and recommend updates to policies to reflect changes in legal, regulatory, or operational environments.
- **Manage Risk**: Mitigate potential risks by recommending policies that safeguard state assets, reputation, stakeholders, and state residents against the evolving threat landscape.
- **Support Compliance**: Help ensure that all policies adhere to and advance relevant legal and regulatory requirements and develop a comprehensive plan for dissemination and agency education.
- **Identify Baselines and Promote Operational Synergy**: Develop consistent and uniform baseline security and other standards, and enhance efficiency by identifying common policy and operational needs across subject matter agencies.
- **Standardize and Enhance Accessibility**: Standardize the format and structure of state IT policy documents, institute transparent version control, and establish an organized and centralized public library of adopted policies.
- **Support Agency Policy Development and Implementation**: Respond to agency needs and enable agencies to develop complementary policies and implementation guidance specific to their unique context, based on a set of clear, transparent enterprise policies.

II.   **Group Structure and Composition**

The governance structure shall consist of two constituent groups as follows:

A.   **Steering Group**

The Steering Group shall consist of selected senior policy and operational personnel from OPM and DAS BITS. The OPM Senior Policy Advisor for Information Technology will direct the Steering Group consistent with the role assigned by statute to OPM and as directed by the Secretary.

The Steering Group will engage at a cadence to be determined by OPM to identify any new or revised policy needs, to stand up and oversee ad hoc groups as needed, to assess progress with ongoing policy development projects and establish timelines, and to consider any necessary process reform.

The Steering Group shall include the following individuals or their designee, and may include others as necessary and appropriate:

- OPM Senior Policy Advisor for Information Technology
- Chief Data Officer
- Chief Information Officer (CIO)

- Chief Information Security Officer (CISO)
- OPM Budget and Financial Management Division Designee

B. Ad Hoc Groups

Ad hoc groups may be used by the Steering Group to address particular subject matter policies as needed. Ad hoc group composition will, to the extent practicable, represent a diverse group of agency leadership, legal, compliance experts, technical leaders, executives and subject matter experts consistent with the scope and possible impact of the policy to be developed or reviewed, including those with expertise in public audits or privacy where appropriate. One or more members of the Steering Group shall be designated as the liaison(s) for each ad hoc group, and shall guide and report back on the actions of the ad hoc group to which they are assigned.

III. Identifying IT Policy Needs

The Steering Group may choose to recommend the pursuit of IT policies based on several factors:

a. The Group's own recommendations based on industry research, current technological advances, or emerging threats;
b. Governor, agency or executive branch-identified priorities or recommendations, including through the IT Strategic Plan and State Data Plan;
c. State-to-state consultation;
d. Federal or state regulatory or statutory requirements, guidance or other directives, such as the NIST Cybersecurity Framework; or
e. State legislative initiatives with information technology implications.

IV. Proposed Governance Process for Policy Adoption

The Steering Group will strive to employ the following process to develop, vet and provide advisory recommendations for relevant OPM IT policy documents. Deviation may be undertaken when exigencies warrant.

Step 1.

When appropriate, the Steering Group will assemble an ad hoc group of policy stakeholders to advise on the need for, and context of, the proposed policy. Potential impact and legal exposure should be considered. While statutory responsibility for IT policy is assigned to OPM and final policy decisions are subject to review and approval by the OPM Secretary, the ad hoc group will strive to build consensus among stakeholders in developing policy recommendations. When requested, the ad hoc group will either generate a recommended draft or review a draft/template provided to them by the Steering Group and/or the designated liaison, and develop a recommended strategy for dissemination and education regarding the policy.

The Steering Group shall review, evaluate, and advance the outputs from the ad hoc group and seek to achieve consensus on outcomes, as described below.

Step 2.

Representatives from the Steering Group will review the draft policy with relevant OPM staff to assess consistency with relevant legal guidelines, regulatory requirements, fiscal constraints, and policy objectives. The Chief Data Officer shall review for consistency with the State Data Plan. Human Resources and Labor Relations will be consulted when in OPM's judgment it is necessary to ensure compliance with relevant labor and employment laws and/or collective bargaining requirements.

Step 3.

The Steering Group will circulate draft policies with an identified roster of agency representatives to identify additional content or implementation issues. Circulation may include, but not be limited to, agency customer success managers, security liaisons and agency data officers. Feedback may be time limited.

Step 4.

Representatives of the Steering Group will review the recommended policy with OPM's Secretary or the Secretary's designee(s). When the policy is approved by the OPM Secretary, it is then considered in 'release candidate' status. OPM shall have the responsibility to adopt and publish approved policies to the centralized public Policy Library on OPM's Website.

Step 6.

The Steering Group will develop and implement mechanisms to disseminate the policy, track agency implementation of the policy (and any variances), and address the need for any revisions. Depending on the needs of the policy in question, this may include incorporation into training, attestations, logs or other survey methods.

Step 7.

The Steering Group shall perform regular reviews and recommend updates to policies at regular intervals based on the relative need and risk profile of a given policy.

Date	Version	Description	Publisher
July 25, 2025	1.0	Initial Policy	Office of Policy and Management