CONNECTICUT
Policy and Management

Policy Title:	Connecticut Cyber Incident Response Planning Policy
Originator:	Office of Policy and Management ("OPM")
Effective Date:	January 21, 2026
History:	Version 1.0
Applies to:	State Agencies defined in C.G.S. § 4d-1(3)
Relevant Laws or Regulations:	C.G.S. §§ 4-5, 4-8, 4-65a, 4-66, 4d-1(3), and 4d-8a; § 28-5

Purpose

The purpose of this policy is to provide State Agencies with guidance on agency-level cyber incident response planning, including the development and implementation of an Agency Cyber Disruption Plan consistent with the State of Connecticut Cyber Disruption Plan. Agency-level planning in this regard shall complement broader State and Federal civil preparedness planning and leverage established systems, protocols and response organizations as detailed below.

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 May 2025 adopted 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).

Scope and Reach

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

This policy is governed by the State of Connecticut Information Security Policy and subject to the definitional and functional requirements outlined in the most recent version of that policy. It should be consulted for an overview of mandatory vs. recommended requirements (SHALL vs. SHOULD), roles and responsibilities, and related process requirements for Agency-level policies or exceptions.

Other branches of government, including the Legislature and the Judiciary, are encouraged to adopt similar standards.

Policy Statement/Narrative

The State Cyber Disruption Response Plan describes the framework for cyber incident response coordination among State Agencies, federal/local/tribal governments, and public and private sector entities. This plan establishes the state's Cyber Disruption Task Force ("CDTF"), which is a group of subject matter experts from various disciplines involved in cyber preparedness, detection, alert, response, and recovery planning and implementation activities. Upon detection of an impending threat or significant event within the state or on the state's computer network, the CDTF may be activated to determine appropriate actions to respond to, mitigate, and investigate damage. If an event overwhelms a local community or is widespread, the State Emergency Operations Center may be opened to coordinate a unified response.

While the State Cyber Disruption Plan details the *state-level* coordination and response plans associated with cyber incidents, the integrity and security of our state systems requires adequate awareness, planning and training at the *Agency* level as well to ensure cybersecurity and other security incidents are identified, reported, contained and remediated. In this respect, a cybersecurity incident covered under this policy may also include minor security incidents that could be evidence of, or lead to, a larger-scale cyber disruption. This includes security incidents in which authorized access to systems or data is impaired, such as a denial of service attack, security incidents where unauthorized access is attempted or gained to systems or data (including digital intrusions such as phishing or similar incidents, access to data above the level for which a user is authorized, as well as physical access breaches, or breaches of acceptable use policies). Such security incidents may be purposeful or unintentional.

Agency staff may be the first to become aware of a security incident and providing a defined and well-rehearsed reporting pathway to decisionmakers, as well as clear guidelines for triaging incidents among agency-level IT subject matter experts, are key to a timely and decisive response.

In this respect, Atate Agencies shall have a documented and routinely updated Agency Incident Response Plan consistent with the State Cyber Disruption Plan and accounting for the State Agency's structure (staffing and IT infrastructure/assets) and available resources. Agency-level incident response is a critical component of the State Cyber Disruption Plan. State Agencies working under an optimization Memorandum of Understanding with DAS should seek guidance from DAS-BITS to support the development, maintenance in implementation of their Agency Incident Response Plan, and *all* State Agencies should leverage the published Agency Incident Response Plan template available from DAS-BITS.

Where an Agency Incident Response Plan includes deviation from this policy or the State Cyber Disruption Plan due to the specific needs of the Agency, the Agency shall document the deviation and the reason consistent with the State of Connecticut Information Security Policy. Any exceptions to this policy or the State Cyber Disruption Plan require approval as detailed in the State Information Security Policy.

Elements of a basic Agency Incident Response Plan include the following:

- **Incident Response Team (IRT)**

The Agency Incident Response Plan shall specify a roster of personnel to comprise an Agency Incident Response Team ("IRT"). The IRT is responsible for the intake and evaluation of incidents affecting the

specific Agency's IT infrastructure, digital assets, data and personnel, and escalating those incidents to DAS-BITS if necessary.

The Agency IRT should include, consistent with existing job responsibilities, Agency leadership, members of the Agency IT team (including the Agency Information Security Officer ("ISO") where staffed), an Agency legal representative, the Agency public information officer, the Agency Data Officer (where staffed), a member of the Agency human resources department, and auxiliary functions or resources, as necessary. Where an Agency is working within an optimized IT environment under DAS-BITS, this should also include a member of the DAS-BITS IRT. An IRT Team Lead or Coordinator should be designated from among the IRT members, typically the ISO or relevant IT staff acting in that capacity. The IRT is responsible for:

- Developing and disseminating an appropriate mechanism for staff to report incidents to the IRT;
- Developing and, at regular intervals, conducting staff training;
- Responding to incident reports, including assessing severity and taking appropriate action to validate, prioritize, contain and escalate an incident; and
- Conducting post-incident assessments, documentation, and revising agency-level policies and practices with lessons learned.

The IRT Team Lead or Coordinator is responsible for:

- Coordinating the Agency's response efforts and the actions of the IRT;
- Engaging auxiliary Agencies and resources;
- Escalating incidents to executive management as appropriate;
- Monitoring progress of the response;
- Ensuring evidence gathering, chain of custody, and preservation as appropriate;
- Managing all communications with outside organizations (i.e., law enforcement, media, and regulatory bodies);
- Managing all communications with other State Agencies such as DAS-BITS and the Connecticut Intelligence Center in DESPP; and
- Prepare a written summary of the incident and corrective action taken.

- **Incident Response Training**

As above, the IRT is responsible for developing and conducting training related to the Agency Incident Response Plan. Generally, incident response training should be tailored to the role particular staff may play in identifying, reporting, and/or remediating a security incident. For example, some staff may only need to know how to recognize and report an incident; System Administrators may require additional training on how to handle incidents; and IRT members should receive more specific training on forensics, data collection techniques, reporting, system recovery, and system restoration. Consistent with standard Agency practices, such training should be conducted during standard onboarding training, when taking on a new role or obtaining new system access, and should also be conducted at regular intervals, whether combined with other training or conducted separately. Routine training should include simulated events and tests or exercises of the Agencies' and the State's incident response capabilities.

- **Incident Response Testing**

State Agencies should coordinate with DAS-BITS and DESPP Division of Emergency Management and Homeland Security Training and Exercise Unit to test the effectiveness of the Agency's incident response capabilities at least annually. This may include, depending on the needs of the Agency, creating checklists and playbooks and/or conducting table-top exercises and simulations that include a variety of incidents, including data breaches.

Agencies should develop testing for the Agency's particular information systems so that staff are familiar with their roles and responsibilities with respect to the specific information system and data housed or processed therein.

Additional References

National Institute of Standards and Technology (NIST) Special Publication 800-53 Release 5.2.0, referencing controls:

- IR-01 Policy and Procedures
- IR-02 Incident Response Training
- IR-03 Incident Response Testing
- IR-04 Incident Handling
- IR-08 Incident Response Plan

Version History

Date	Version	Description	Publisher
January 21, 2026	1.0	Initial Policy	Office of Policy and Management