Incident Response (IR)

Purpose:

The following standards are established to support the policy statement 10.3 that "CSCU will: (i) establish an operational incident handling capability for CSCU information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate CSCU officials and/or authorities."

Scope:

1. Institutional Units of the Connecticut State College and University System including the Connecticut Board of Regents System Office.

2. All Connecticut State College and University institutional units' information systems.

Standard:

1. Incident Response Training [NIST 800-53r4 IR2]

1.1 For all CSCU information systems, ISPO provides incident response training to CSCU employees, business partners and vendors consistent with their incident response roles and responsibilities.

a.) In coordination with Data Owners, training of individuals assuming an incident response role or responsibility, will occur within 4 weeks of that responsibility being assigned;

b.) When required by information system changes; and

c.) Annually thereafter.

1.2 For moderate and high risk information systems, ISPO:

a.) Incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. [NIST 800-53r4 IR2 (1)]

b.) Employ automated mechanisms to provide a more thorough and realistic incident response training environment. [NIST 800-53r4 IR2 (2)]

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.300	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

2. Incident Response Testing [NIST 800-53r4 IR3]

2.1 For all CSCU information systems, ISPO tests the incident response capability for the information system annually using checklists, simulations and tabletop exercises to determine the incident response effectiveness and documents the results.

2.2 For moderate and high risk information systems, ISPO coordinates incident response testing with organizational elements responsible for related plans. [NIST 800-53r4 IR3 (2)]

3. Incident Handling [NIST 800-53r4 IR4]

3.1 For all information systems the CSCU CIO along with ISPO, Campus Information System Security Officers, Data Owners, and Information System Owners:

a.) Implements an incident handling capability for security incidents that includes identification, containment and assessment, eradication and recovery, notification and follow-up and conclusion;

b.) Coordinates incident handling activities with contingency planning activities; and

c.) Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

3.2 For moderate and high risk information systems the CSCU CIO along with ISPO, Campus Information System Security Officers, Data Owners, and Information System Owners:

a.) Employs automated mechanisms to support the incident handling process. [NIST 800-53r4 IR4 (1)]

b.) Correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. [NIST 800-53r4 IR4 (4)]

4. Incident Monitoring [NIST 800-53r4 IR5]

4.1 For all information systems ISPO tracks and documents information system security incidents.

4.2 For moderate and high risk information systems, ISPO employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. [NIST 800-53r4 IR5 (1)]

5. Incident Reporting [NIST 800-53r4 IR6]

5.1 For all information systems, CSCU:

a.) Requires CSCU personnel, including but not limited to, Data Owners, Information System Owners, Information System Administrators and Information Users, to report suspected security incidents to the organizational incident response, CSCU CERT, immediately; and

b.) Requires security incident information to be reported to ServiceDesk@ct.edu

5.2 For moderate and high risk information systems, ISPO employs automated mechanisms to assist in the reporting of security incidents. [NIST 800-53r4 IR6 (1)]

6. Incident Response Assistance [NIST 800-53r4 IR7]

6.1 For all information systems, ISPO coordinates an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

6.2 For moderate and high risk information systems, the organization employs automated mechanisms to increase the availability of incident response-related information and support. [NIST 800-53r4 IR7 (1)]

7. Incident Response Plan [NIST 800-53r4 IR8]

7.1 For all information systems ISPO:

a.) Develops 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; and
- Is reviewed and approved by CSCU CIO.

b.) Distributes copies of the incident response plan to CSCU President/Chancellor, CSCU CIO, Campus Presidents, Campus Information System Security Officers, Data Owners, and Information System Owners.

c.) Reviews the incident response plan annually.

d.) Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

e.) Communicates incident response plan changes to CSCU President, CSCU CIO, Campus Presidents, Campus Information System Security Officers, Data Owners, and Information System Owners, and

f.) Protects the incident response plan from unauthorized disclosure and modification.

Roles & Responsibilities

Refer to the Roles and Responsibilities located on the website.

Definitions

Refer to the Glossary of Terms located on the website.

References

ITS-04 CSCU Information Security Policy

NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

NIST 800-171 Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016.