Contingency Planning (CP)

Purpose:

The following standards are established to support the policy statement 10.8 that "CSCU will establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for CSCU information systems to ensure the availability of critical information resources and continuity of operations in emergency situations."

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. Information System Backup [NIST 800-53r4 CP9]

1.1 For all information systems:

a.) The Information System Owner and Data Owners will identify and document both Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for the Information System.

b.) The Information System Owner must backup data residing on information systems including, but not limited to, the following:

- Backups of user-level information contained in the information system.
- Backups of system-level information contained in the information system. System-level information includes, for example, system state information, operating system and application software, and licenses.
- Backups of information system documentation including security-related documentation.
- The frequency of information system backups shall be consistent with the information systems' RTOs and RPOs.

c.) The Information System Owner must protect the confidentiality, integrity, and availability of the system backup information at the storage location.

Document Number:	Document Status:	Effective Date:	Approval Date:	Last Rev. Date:	Review Date	Next Review:
ISST 10.800	Approved	2/6/2020	2/6/2020	June 6, 2019	2/6/2020	

1.2 For moderate risk information systems, the Information System Owner:

a.) Tests backup information at least once per year to verify media reliability and information integrity. [NIST 800-53r4 CP9 (1)]

b.) Protect the confidentiality and integrity of the system backup information at the storage location using CSCU approved encryption and cryptographic hashing methods.

1.3 For high risk information systems, the Information System Owner:

a.) Stores backup copies in a separate, CSCU approved facility or in a fire-rated container that is not collocated with the operational system. [NIST 800-53r4 CP9 (3)]

2. Information System Recovery and Reconstitution [NIST 800-53r4 CP10]

2.1 For all information systems, the Information System Owner

a.) Ensures the information system can be recovered and reconstituted to a known state after a disruption, compromise, or failure.

b.) Documents recovery and reconstitution mechanisms and procedures.

c.) Ensure the information system's recovery and reconstitution procedures:

- Are based on organizational priorities, established RPO, RTO, and reconstitution objectives, and appropriate metrics.
- Include the deactivation of any interim information system capability that may have been needed during recovery operations.
- Include an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure.

2.2 For all moderate risk information systems, the Information System Owner:

a.) Ensure the information system's recovery and reconstitution procedures also include the following during disruptions and during recovery and reconstitution:

- Essential operations shall be continued; and

- Confidentiality and integrity of the information will be protected.

b.) Ensures the information system implements transaction recovery for systems that are transaction-based. [NIST 800-53r4 CP10 (2)]

2.3 For high risk information systems, the Information System Owner provides the capability to reimage information system components immediately from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components. The restoration time-period of the information system shall be consistent with the information systems' RTOs and RPOs. [NIST 800-53r4 CP10 (4)]

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.