



Office of the University Auditor

INFORMATION TECHNOLOGY DISASTER RECOVERY PLANNING AUDIT GUIDANCE

June 9, 2020

2020.03

Overview

Campuses can be vulnerable to a variety of natural and man-made disasters. Recognizing that not all events can be prevented, and some risks may be deemed acceptable, proper planning is essential to maintain or restore services when an unexpected or unavoidable event disrupts normal operations. Campuses should design, develop and implement a Disaster Recovery Plan (DR Plan) that has essential steps in ensuring the Campus is adequately prepared to recover and continue vital information technology (IT) infrastructure systems.

SUNY plans to adopt the National Institute of Standards and Technology (NIST) standards as a basis to comply with the contingency planning (CP) security controls. The CP controls are used as a base for the development and continuous monitoring of the various types of plans, such as a DR Plan. To date, the most current NIST standards relating to the CP controls are NIST Special Publications (SP) 800-34, 800-53 and 800-84; a link to the standards can be found under the "**Useful Links**" section of this document.

SUNY's Office of the University Auditor (OUA) prepared this document to assist campuses in evaluating the NIST standards and provides best practices for developing a plan. In addition, OUA recently surveyed campuses for DR Plan activities and have identified common improvement opportunities for consideration, included herein. This guidance along with the NIST standards should be considered in conjunction with SUNY Procedure 6608, other security standards, and effective internal controls.

DR Plan Framework

Having a framework ensures a defined structure for the planning process, plan development, plan priorities and dependencies, plan testing, procedures for maintaining and updating the plan, and the responsibilities of individuals and teams before, during, and after the activation of the DR Plan. Below is a framework to be used as the basis for the plan:

- 1) Develop the contingency planning policy;
- 2) Conduct a Business Impact Analysis (BIA);
- 3) Identify preventive controls;
- 4) Create contingency strategies;
- 5) Design and develop the plan;
- 6) Train the disaster recovery staff;
- 7) Perform testing of the plan; and
- 8) Review and revise the plan as needed.

DR Plan Components

OUA identified the following list of components campuses should consider including in their DR Plan:

- Identify individuals who have authority to declare a disaster;
- List assumptions used to develop the plan and which systems and sites are to be included;
- Identify notification procedures in place to: 1) alert a disaster and 2) when systems return to normal operations;

*Contact OUA with
questions, requests for
an audit, or additional
information:*

State University Plaza
Room N120
Albany, NY 12246

518-445-4113

university.audit@suny.edu

Useful Links:

[Department of Homeland Security \(DHS\) Business Continuity Plan Info](#)

[DHS IT Disaster Recovery Plan Info](#)

[NYS Homeland Security & Emergency Services - COOP Planning Tools](#)

[OSC - Local Government Management Guide on IT Contingency Planning](#)

[Disaster Recovery Institute International Website](#)

Below are various NIST Publications which contain guidance relating to Disaster Recovery Planning:

[NIST SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems](#)

[NIST SP 800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities](#)

See Chapter 3, Section 3.6 – Contingency Planning: [Draft NIST SP 800-53 Rev.5 - Security and Privacy Controls for Information Systems and Organizations](#)

Did you know that SUNY has a Security Operations Center (SOC), which provides expertise, software, training tools, and resources to help SUNY campuses improve their information security exposure? Check them out at: [SUNY SOC](#)

- Clearly document the roles and responsibilities of team members during the response and recovery phases;
- List of primary and alternate team members' emergency contact information;
- List of personnel who will receive the plan;
- List of vendor contact information;
- Detailed recovery procedures to restore systems or components to a known state, including the necessary sequence of activities;
- Maintenance and test schedules;
- Awareness, education and training activities;
- Communication processes that clearly define responsibility for communication to relevant stakeholders, service providers, and external parties;
- Identify the locations of alternative sites or backup facilities; and
- Procedures to validate successful recovery and deactivation of the plan.

***Note:** The above list is a summary guide for campuses based on OUA's interpretation of the NIST standards.

Improvement Opportunities

- ☐ Ensure a formal DR Plan is documented and accessible to the appropriate Campus staff.
- ☐ Develop a BIA to help the Campus identify its critical business processes, recovery objectives, allowable downtimes and resource requirements.
- ☐ Ensure the DR Plan approval process is formalized, and such documentation is adequately maintained.
- ☐ Conduct an annual training program to ensure the Campus staff who are involved in and responsible for executing the DR Plan are aware of their roles and responsibilities.
- ☐ Maintain supporting documentation verifying the Campus trained staff on disaster recovery planning.
- ☐ Perform testing and exercises on the DR Plan to ensure the plan is adequate to sustain various disasters, execution of plan is as intended; and identify parts of the plan that need to be changed.
- ☐ Document testing/exercises results and update the DR Plan as needed.
- ☐ Continuously update the DR Plan for significant changes in operations, staffing, and infrastructure (i.e. new systems, networks, IT equipment, hardware, software, etc.).
- ☐ Ensure copies of the DR Plan are protected when distributing the plan to Campus staff.
- ☐ Retrieve and securely destroy outdated copies of the DR Plan after plan updates.
- ☐ Consider incorporating the DR Plan into the Business Continuity Plan.
- ☐ Establish an alternate site to continue operations if the primary site is unavailable.
- ☐ Consider securing a Business Interruption Insurance Policy specific to IT operations.