CONTINGENGENCY PLANNING STANDARD (NSU-CP)

Standard Title:	**CONTINGENGENCY PLANNING STANDARD (NSU-CP)**
Standard Number:	**38-10.6**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**CONTINGENCY PLANNING (CP)**
Approval Date:	**8/2/2024**
Responsible Office:	**Office of Information Technology**
Responsible Executive:	**Chief Information Officer**

Applies to: All employees, students, visitors, and contractors, in all academic and operational departments and offices at all Norfolk State University locations, and to all university information technology and data, whether owned and operated by the university, or used for university business through contractual arrangements.

STANDARD STATEMENT

All individuals to whom this standard applies shall comply with the Norfolk State University Information Security Standards and protect all IT systems and data to which they have access commensurate with sensitivity and risk. All university information technology and data whether owned and operated by the university, or used for university business through contractual arrangements shall be managed and protected in accordance with the provisions of the Norfolk State University Information Security Standards.

TABLE OF CONTENTS PAGE NUMBER

DEFINITIONS

Authorization: The process of verifying that a requested action or service is approved for a specific entity.

Authorize: A decision to grant access, typically automated by evaluating a subject's attributes.

Authorized: A system entity or actor that has been granted the right, permission, or capability to access a system resource.

Availability: The property that data or information is accessible and usable upon demand by an authorized person and that timely, reliable access to data and information services is provided for authorized users.

Computer Network: Two or more computers that can share information, typically connected by cable, data line, or satellite link.

Confidentiality: Protection of systems and data so that unauthorized parties cannot view the data, the property that sensitive information is not disclosed to unauthorized entities, and the assurance that information is not disclosed to unauthorized individuals or processes.

Controlled Unclassified Information (CUI): Information the Federal government owns or has created that needs to be safeguarded and disseminated using only controls consistent with Federal laws, regulations and policies.

Data Custodian: An individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

Data Owner: An individual, who defines, manages, and controls the use of data and ensures compliance with the Information Security Standards with respect to the data.

Information Security: The policies, standards, guidelines, processes, activities, and actions taken to protect the confidentiality, integrity, and availability of information systems and the data they handle commensurate with sensitivity and risk.

Information Security Incident: means an adverse event or situation, whether intentional or accidental, that poses an enterprise impact or threat to the integrity, availability, or confidentiality of university data or systems or requires reporting based upon regulatory requirements.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control.

Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Intellectual Property: Please refer to the BOV POLICY # 35 (2019) INTELLECTUAL PROPERTY POLICY.

Sensitive System: A system that processes any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

Sensitive Information/Data: Any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

System Administrator: An individual or entity that implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner: An individual or entity responsible for the operation and maintenance of an IT system.

Technological Resources: Technological resources include but are not limited to: computers and terminals, software, printers, networks and equipment, telecommunication equipment and services such as telephones, facsimile machines, modems, basic and long distance calling service, and voicemail; television and radio systems and equipment; computer information systems; and, data files and/or documents managed or maintained by the University which reside on disk, tape or other media. Technology resources also include multimedia equipped classrooms, computer classrooms, computer laboratories, computer offices, and computer furnishings operated or maintained by NSU.

Users: Faculty, staff and students as well as others who have been authorized to use Norfolk State University's technological resources, (e.g., contractors, interns, volunteers, etc.).

CONTACT(S)

The Office of Information Technology (OIT) officially interprets this standard. OIT is responsible for obtaining approval for any revisions as required through the appropriate governance structures. Questions regarding this standard should be directed to OIT Security.

STAKEHOLDER(S)

University Faculty & Staff
Students
Others who have been authorized to use Norfolk State University's technological resources.

CONTINGENCY PLANNING (CP)
NSU-CP-1 CONTINGENCY PLAN

Control:

a. Develop a contingency plan for the system that:
   1. Identifies essential mission and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
   5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
   6. Addresses the sharing of contingency information; and
   7. Is reviewed and approved by the Chief Information Security Officer or designee;

b. Distribute copies of the contingency plan to organization-defined key contingency personnel (identified by name and/or by role) and organizational elements;

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system on an annual basis or more frequently if required to address an environmental change;

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to organization-defined key contingency personnel (identified by name and/or by role) and organizational elements;

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training;

h. Protect the contingency plan from unauthorized disclosure and modification;

i. Coordinate contingency plan development with organizational elements responsible for related plans;

j. Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations;

k. Plan for the resumption of essential mission and business functions within the organization-defined time period of contingency plan activation;

l. Plan for the continuance of essential mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites;

m. Plan for the transfer of essential mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites;

Coordinate its contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied; and

n. Identify critical system assets supporting all mission and business functions.

NSU-CP-2 CONTINGENCY TRAINING

Control:

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

1. Within 30-days of assuming a contingency role or responsibility;
2. When required by system changes; and
3. Annually thereafter;

b. Review and update contingency training content annually and following environmental change; and

c. Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

NSU-CP-3 CONTINGENCY PLAN TESTING

Control:

a. Test the contingency plan for the system at least on an annual basis and following an environmental change using organization-defined tests to determine the effectiveness of the plan and the readiness to execute the plan;

b. Review the contingency plan test results;

c. Initiate corrective actions, if needed;

d. Coordinate contingency plan testing with organizational elements responsible for related plans;

e. Test the contingency plan at the alternate processing site:

a. To familiarize contingency personnel with the facility and available resources; and

b. To evaluate the capabilities of the alternate processing site to support contingency operations; and

f. Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.

NSU-CP-4 ALTERNATE STORAGE SITE

Control:

a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information;

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site;

c. Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats;

d. Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives; and

e. Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

NSU-CP-5 ALTERNATE PROCESSING SITE

Control:

a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of system operations for essential mission and business functions within the organization-defined time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption;

c. Provide controls at the alternate processing site that are equivalent to those at the primary site;

d. Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats;

e. Identify potential accessibility problems to the alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions;

f. Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives);

g. Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions; and

h. Plan and prepare for circumstances that preclude returning to the primary processing site.

NSU-CP-6 TELECOMMUNICATIONS SERVICES

Control:

a. Establish alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within 24 hours when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites; and

b. Require primary and alternate telecommunications service providers to have contingency plans.

NSU-CP-7 SYSTEM BACKUP

Control:

a. Conduct backups of user-level information contained in the system within the organization-defined frequency consistent with recovery time and recovery point objectives;

b. Conducts backup of system-level information contained in the information system in accordance with organization-defined frequency consistent with recovery time and recovery point objectives;

c. Conduct backups of system documentation including security- and privacy-related documentation in accordance with organization-defined frequency consistent with recovery time and recovery point objectives;

d. Protect the confidentiality, integrity, and availability of backup information;

e. Test backup information to verify reliability and information integrity;

f. Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing;

g. Transfer system backup information to the alternate storage site at least on a daily basis or sooner based on organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives;

h. Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations; and

i. Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of sensitive backup information.

NSU-CP-8

Control: For every IT system identified as sensitive relative to availability, each agency shall or shall require that its service provider implement backup and restoration plans to

support restoration of systems, data and applications in accordance with agency requirements. At a minimum, these plans shall address the following:

a. Secure alternate back-up, storage, and processing site that is geographically separate and distinct from the primary location;

b. Performance of backups only by authorized personnel;

c. Review of backup logs after the completion of each backup job to verify successful completion;

d. Approval of backup schedules of a system by the System Owner;

e. Approval of emergency backup and operations restoration plans by the System Owner;

f. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding;

g. Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present in a usable form; and

h. For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures.

NSU-CP-9 SYSTEM RECOVERY AND RECONSTITUTION

Control: Provide for the recovery and reconstitution of the system to a known state within an organization-defined time period consistent with recovery time and recovery point objectives after a disruption, compromise, or failure.

EDUCATION AND COMPLIANCE

This standard shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

- Communicate the standard in writing, electronic or otherwise, to the University community within 30 days of approval;
- Post the standard on the appropriate website; and
- Educate and train all stakeholders and appropriate audiences on the standard's content, as necessary. Failure to meet the publication requirements does not invalidate this standard.

The Chief Information Security Officer (or designee) is responsible for official interpretation of this standard. Questions regarding the application of this standard should be directed to the Office of Information Technology. The Chief Information Security Officer reserves the right to revise or eliminate this standard.

Violations of this standard, including without limitation any misuse of data or IT resources may result in the limitation or revocation of access to University IT resources. In addition, failure to

comply with requirements of this standard may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies, and may violate federal, state, or local laws.

EXCEPTIONS

Exceptions to this standard must be documented in writing and approved by the Vice President for Operations and Chief Strategist, the Chief Information Officer, and the Chief Information Security Officer.

REVIEW SCHEDULE

- Next Scheduled Review: 8/2/2026
- Approval by, date: OIT Standards Development Group, 8/2/2024
- Revision History: 7/31/2025
- Supersedes: SEC530 CP Controls

RELATED DOCUMENTS

32-01 - Acceptable Use of Technological Resources
https://www.nsu.edu/policy/admin-32-01.aspx
32-02 - Data Classification Policy
https://www.nsu.edu/policy/admin-32-02.aspx
38-10 - Information Security Policy
https://www.nsu.edu/policy/bov-38-10.aspx