ELIZABETH CITY STATE UNIVERSITY
Business Continuity and Disaster Recovery Policy

1. PURPOSE

The purpose of this policy is to ensure adequate plans and procedures are in place to enable ECSU (Elizabeth City State University) to avoid or minimize interruption to any critical functions during and after major failures or disasters. This policy establishes the requirements, roles, and responsibilities for preparing and implementing Business Continuity and Disaster Recovery plans (BCDR) to ensure the confidentiality, integrity, and availability of ECSU information resources accessed, managed, and/or controlled by the ECSU.

2. SCOPE

This policy applies to all ECSU employees, whether full-time or part-time, paid or unpaid, temporary or permanent, volunteers, as well as all other members of the ECSU community. This policy applies to all information collected, stored or used by or on behalf of any operational unit, department and person within the community in connection with ECSU operations. If any information at ECSU is governed by more specific requirements under other ECSU policies or procedures the more specific requirements shall take precedence over this policy to the extent there is any conflict.

3. ACRONYMS / DEFINITIONS

Availability. The measures to which information and critical ECSU services are accessible for use when required.

Business Continuity. The ability of an organization to maintain essential functions during, as well as after, a disaster has occurred.

Business Interruption. An event, whether anticipated or unanticipated, which disrupts the normal course of business operations within the ECSU.

Confidentiality. The measures to which confidential ECSU information is protected from unauthorized disclosure.

Disaster Recovery. A set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Information Resource. Data, information, and information systems used by ECSU to conduct ECSU operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security. The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability of data.

Information Systems. A hardware or virtual computing environment that is installed or configured to collect, process, store, or transmit information for multiple users or, that communicates with other systems to transmit data or process transactions.

Integrity. The measures to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the ECSU.

4. POLICY

A. BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

All ECSU schools, administrative offices, and business units must develop and document an appropriate and resilient Business Continuity and Disaster Recovery Plan (BCDR) to address interruptions to ECSU business activities and to protect critical business processes from the effects of major failures or disasters. The BCDR plan must: Address the loss or failure of critical people (workforce), systems, locations, processes, and suppliers.

i. Document procedures and strategies to successfully restore services in defined timeframes based upon system criticality.
ii. Identify and define roles and responsibilities.
iii. Be tested periodically.
iv. Be reviewed, updated, and approved at least annually.

B. ROLES AND RESPONSIBILITIES

i. Chief Information Officer (CIO)

The Chief Information Officer (CIO) serves as the senior executive officer responsible for ECSU-wide planning, management, security, and coordination of information technology resources. Before, during, and after a BCDR event, the CIO shall be responsible for the following:

a. Oversight of ECSU-wide Business Continuity and Disaster Recovery management.
b. Annual review and approval of any substantial changes to this policy and ECSU BCDR plans.
c. Making appropriate recommendations to the Board of Trustees regarding DCDR strategies and activities.
d. Serving as the primary point of contact for significant interruptions to ECSU business activities resulting from major failures or disasters.
e. Declaring a disaster if necessary to trigger BCDR activities.

f. Providing support or backup for the Information Security Officer (ISO).
g. Coordinating additional resource allocation as required.
h. Collaborating with the ISO in decision-making when ECSU operations are impacted.
i. Notifying the ECSU Chancellor and/or Board of Trustees of a BCDR declaration.
j. Coordinating communication with other ECSU executives during a BCDR declaration or event.
k. Notifying ECSU Communications as appropriate for internal and external communication.

ii. Information Security Office/Officer (ISO)

The Information Security Officer (ISO) has authority and responsibility for operation and management of ECSU's Information Security Program. Before, during, and after a BCDR event, the ISO shall be responsible for the following:

a. Oversight of ECSU-wide Business Continuity and Disaster Recovery management.
b. Annual review and approval of any substantial changes to this policy and ECSU BCDR plans.
c. Making appropriate recommendations to the CIO regarding BCDR strategies and activities.
d. Managing the overall ECSU BCDR response activities, escalating to the CIO as necessary.
e. Managing BCDR resources and task assignments.
f. Identifying external personnel/resources as needed.
g. Assisting in event containment, investigation, remediation, and recovery.
h. Collecting and documenting event details and response activities.
i. Notifying and briefing the CIO and ECSU executives as appropriate.
j. Notifying University Police and General Counsel as appropriate.
k. Leading postmortem discussions to determine root cause, necessary changes/updates, response strengths/weaknesses, and lessons learned.
l. Preparing a formal report for distribution to the ECSU Cabinet immediately after the event concludes.

iii. Division of Information Technology (DIT) Personnel

DIT personnel have primary operational responsibility for information systems that receive, create, store, handle, or discard information. Before, during, and after a BCDR event, IT Services shall be responsible for the following:

a. Supporting the development and implementation of appropriate strategies to recover infrastructure platforms and to restore critical applications consistent with ECSU continuity and recovery objectives.
b. Overseeing the creation, execution, and testing of formal BCDR plans and activities related to the systems and infrastructure it supports on behalf of the ECSU.
c. Assisting the CIO and/or ISO in event containment, investigation, remediation, and recovery.

d. Collecting and documenting event details and response activities as requested by the CIO and/or ISO.
e. Performing system or data recovery to restore normal operations as requested by the CIO and/or ISO.
f. Providing technical support to the CIO and/or ISO as needed.

iv. University Police

Before, during, and after a BCDR event, University Police shall be responsible for the following:

a. Assisting with BCDR activities when necessary.
b. Coordinating with external law enforcement as required or requested by the CIO, ISO, or General Counsel.

v. General Counsel

During and after a BCDR event, ECSU General Counsel shall be responsible for the following:

a. Determining what, if any, actions ECSU is required to take to comply with applicable law, including whether any notification is required under North Carolina law.
b. Working with the CIO and ISO as appropriate to ensure that any notifications and other legally required responses are made in a timely manner.
c. Advising ECSU`s senior leadership regarding involvement of law enforcement and regulatory agencies.
d. Reviewing BCDR event communications drafted by ECSU's Communications & Marketing.
e. Liaising with external counsel as required.

vi. ECSU Communications & Marketing

During and after a BCDR event, ECSU's Communications & Marketing shall be responsible for the following:

a. Preparing internal and external updates or releases at the request of the CIO under guidance from ECSU General Counsel.
b. Responding to external information inquiries.

vii. Vice Chancellors and Deans

Vice Chancellors and Deans (in addition to the Chancellor and other members of the senior leadership team) shall be responsible for protecting all ECSU information resources within their respective offices or departments by:

a. Annually reviewing and approving of any substantial changes to this policy and BCDR plans.
b. Ensuring faculty and staff are familiar with BCDR protocols for emergencies and business disruptions, and compliance with this policy and supporting standards/guidelines.

c. Maintaining an appreciation of the risks associated with the loss of confidentiality, integrity, or availability of information resources used in their office or department.
d. Determining the proper levels of protection, through consultation/coordination with the ISO and Division of Information Technology personnel, for office or department information resources and ensuring necessary safeguards are implemented and recovery procedures defined.
e. Ensuring all information resources used by the office or department are assigned an Information Owner.
f. Promoting BCDR awareness in the office or department and ensuring all staff participate in relevant training.
g. Ensuring office and department staff compliance with the requirements of the Information Security Program.

viii. Administrative Offices and Business Units

Administrative Office and Business Unit management shall be responsible for protecting all ECSU information resources within their respective offices or units by:

a. Annually reviewing and approving of any substantial changes to this policy and ECSU BCDR plans.
b. Ensuring staff are familiar with BCDR protocols for emergencies and business disruptions, and compliance with this policy and supporting standards/guidelines.
c. Maintaining an appreciation of the risks associated with the loss of confidentiality, integrity, or availability of information resources used in their office or department.
d. Determining the proper levels of protection, through consultation/coordination with the ISO and IT Services, for office or department information resources and ensuring necessary safeguards are implemented and recovery procedures defined.
e. Ensuring all information resources used by the office or department are assigned an Information Owner.
f. Promoting BCDR awareness in the office or department and ensuring all staff participate in relevant training.
g. Ensuring office and department staff compliance with the requirements of the Information Security Program.

C. BUSINESS IMPACT ANALYSIS

On an annual basis, all ECSU schools, administrative offices, and business units are required to perform a Business Impact Analysis for each system used in their area of responsibility. This assessment should identify and define the criticality of key systems and the repositories that contain the relevant and necessary data for the system. The criticality ranking establishes recovery targets and the rigor of BCDR activities. The following criteria are used for criticality ranking:

CRITICALITY	CRITERIA
Core Infrastructure	A. Information systems that must be functioning and operational before dependent systems can perform as intended. B. Examples of core systems: electricity, data network, Domain Name System server (DNS), Dynamic Host Configuration Protocol (DHCP), Active Directory C. Immediate recovery is required to prevent major interruption of ECSU operations. D. System maximum downtime of 2 hours or less.
Critical	A. Information systems essential to support ECSU business operations. B. System loss or failure will have an extreme impact on business operations. C. System maximum downtime of 4 hours or less.
High	A. Information systems crucial to support ECSU business operations. B. System loss or failure will have a significant impact on business operations. C. System maximum downtime of 24 hours or less.
Medium	A. Information systems important to support ECSU business operations. B. System loss of failure will have a moderate impact on business operations. C. System maximum downtime of 72 hours or less.
Low	A. Information systems providing improved effectiveness or efficiency of ECSU business operations. B. System loss or failure will have a negligible impact on business operations. C. System downtime greater than 72 hours.

D. TESTING

All BCDR plans will be periodically tested. The frequency of testing will be as defined for the appropriate criticality level and will include tests to verify whether ECSU management and staff are able to put the plan into operation.

E. TRAINING AND AWARENESS

The ISO will communicate BCDR policies and processes to all departments and units and implement appropriate employee awareness and training programs to promote the understanding of all related policies, standards and guidelines.

F. MAINTENANCE

ECSU Vice Chancellors, Deans, Administrative Offices, Business Unit management must review BCDR plans annually or when a major change to critical people, systems, processes, suppliers or locations occurs. All departments and units will have appropriate change management processes in place to ensure the plan is current, credible and practical.

G. APPROVAL

A BCDR plan shall be reviewed by the CIO and ISO, and approved by the responsible ECSU Vice Chancellor, Dean, Administrative Office, or Business Unit manager. Once approved by all levels, any future updates to the specific BCDR plan need only to be approved by the responsible ECSU Vice Chancellor, Dean, Administrative Office, or Business Unit manager. The CIO and ISO will periodically review all plans for being current and update as needed. The CIO will provide periodic reports on BCDR planning efforts ECSU-wide to the Board of Trustees.

5. PROCEDURES

ECSU shall develop, manage, and review operating procedures to create the proper security posture for protecting ECSU information resources. Such procedures shall be periodically reviewed as required.

6. COMPLIANCE / ENFORCEMENT / SANCTIONS

Any ECSU employee or student found to have violated this policy shall be subject to disciplinary action. Sanctions will be proportionate to the severity and/or frequency of offense and can include termination of employment or expulsion. In addition, violators may be subject to criminal and/or civil action.

7. EXCLUSIONS / EXCEPTIONS

No approved exceptions exist at this time.