FAYETTEVILLE STATE UNIVERSITY

BUSINESS CONTINUITY AND DISASTER RECOVERY

Authority:	Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Chancellor.
Category:	Information Technology
Applies to:	●Administrators ●Faculty ●Staff
History:	Approved – August 7, 2024 (Technical Corrections) Issued – October 26, 2021
Related Policies/ Regulations/Statutes:	●Adverse Weather and Emergency Events ●Emergency Operations Plan
Contact for Info:	Vice Chancellor for Information Technology & Chief Information Officer (910) 672-1200

I. PURPOSE

The purpose of this policy (Policy) is to ensure adequate plans and procedures are in place to enable Fayetteville State University (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 to ensure the confidentiality, integrity, and availability of information resources accessed, managed, and/or controlled by the University.

This Policy applies to all information collected, stored, or used by or on behalf of any operational University unit or individual. In the event that any particular information at the University is governed by more specific requirements under other University policies or procedures, the more specific requirements shall take precedence over this Policy to the extent there is any conflict.

II. DEFINITIONS

The following definitions apply to terms used in this Policy:

- **Availability** shall mean the degree to which information and critical College services are accessible for use when required.
- **Business Continuity** shall mean the ability of the University to maintain essential functions during, as well as after, a disaster has occurred.
- **Confidentiality** shall mean the degree to which confidential University information is protected from unauthorized disclosure.
- **Disaster Recovery** shall mean 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** shall mean data, information, and information systems used by the University to conduct University operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

- **Information Security** shall mean 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** shall mean 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** shall mean the degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the University.

III. BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN (BCDR)

All University units must develop and document appropriate and resilient BCDR plans to address interruptions to university business activities and to protect critical business processes from the effects of major failures or disasters. The BCDR plan must include the following:

- Information addressing the loss or failure of individuals critical to the workforce, systems, locations, processes, and suppliers.
- Procedures and strategies to successfully restore services in defined timeframes based upon system criticality.
- The identification and definition of roles and responsibilities.

The BCDR shall be tested periodically and reviewed, updated, and approved at least annually.

A. <u>Roles and Responsibilities</u>

1. Chief Information Officer (CIO)

The CIO serves as the delegated authority responsible for university-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:

- Annual review of any substantial changes to this Policy and the University BCDR plans. Recommended changes to this Policy shall be in accordance with the University's policy on policies.
- Making appropriate recommendations to the Chancellor and Board of Trustees regarding BCDR strategies and activities.
- Providing support or backup for the Information Security Office / Chief Information Security Officer (CISO).
- Coordinating additional resource allocation as required.
- Collaborating with the CISO in decision-making when the University's operations are impacted.

- Notifying the Chancellor of a BCDR declaration.
- Coordinating communication with the Chancellor's Cabinet during a BCDR declaration or event.

2. Chief Information Security Office/Officer (CISO)

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

- Annual review and approval of any substantial changes to this policy and College BCDR plans.
- Making appropriate recommendations to the CIO regarding BCDR strategies and activities.
- Managing the overall University BCDR response activities, escalating to the CIO as necessary.
- Managing BCDR resources and task assignments.
- Identifying external personnel/resources as needed.
- Assisting in event containment, investigation, remediation, and recovery.
- Collecting and documenting event details and response activities.
- Notifying and briefing the CIO and University Cabinet members, as appropriate.
- Notifying Police and Public Safety, and General Counsel, as appropriate.
- Leading postmortem discussions to determine root cause, necessary changes/updates, response strengths/weaknesses, and lessons learned.
- Preparing a formal report for distribution to the University's Cabinet members immediately after the event concludes.

3. Information Technology Services (IT Services)

IT Services staff 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:

- Supporting the development and implementation of appropriate strategies to recover infrastructure platforms and to restore critical applications consistent with university continuity and recovery objectives.
- Overseeing the creation, execution, and testing of formal BCDR plans and activities related to the systems and infrastructure it supports.
- Assisting the CIO and/or CISO in event containment, investigation, remediation, and recovery.
- Collecting and documenting event details and response activities as requested by the CIO and/or CISO.
- Performing system or data recovery to restore normal operations as requested by the CIO and/or CISO.
- Providing technical support to the CIO and/or CISO, as needed.

4. Police and Public Safety

Before, during, and after a BCDR event, Police and Public Safety shall be responsible for assisting with BCDR activities when necessary and coordinating with external law enforcement as required or requested by the CIO, CISO, or General Counsel.

5. General Counsel

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

- Determining what, if any, actions the University is required to take to comply with applicable law, including whether any specific notification is required under applicable laws or policies.
- Working with the CIO and CISO to ensure that any legally required notifications or responses are made in a timely manner.
- Reviewing BCDR event communications, if necessary.
- If necessary, liaising with external counsel.

6. Public Relations

During and after a BCDR event, College communications shall be responsible for preparing internal and external updates or releases at the request of the CIO under guidance from the General Counsel and responding to external information inquiries.

7. Senior Leadership

The Senior Leadership will be responsible for protecting all University information resources within their respective units as follows:

- Annually reviewing and approving any substantial changes to this Policy as outlined in the University's policy on policies and their respective BCDR plans.
- With assistance from the CIO, CISO, and IT Services, ensuring faculty and staff are familiar with BCDR protocols for emergencies, business disruptions, and compliance with this Policy and supporting standards/guidelines.
- Maintaining an appreciation of the risks associated with the loss of confidentiality, integrity, or availability of information resources used in their units.
- Determining the proper levels of protection, through consultation/coordination with the ISO and IT Services, for unit information resources and ensuring necessary safeguards are implemented and recovery procedures defined.
- Ensuring all information resources used by the respective units are assigned an Information Owner.
- With assistance from the CIO, C ISO, and IT Services, promoting BCDR awareness in their units and ensuring all staff participate in relevant training.

- Ensuring staff compliance with the requirements of the Information Security Program.

8. Academic and Administrative Units

Academic and Administrative Unit managers/supervisors shall be responsible for protecting all University information resources within their respective offices or units as follows:

- With assistance from the CIO, CISO, and IT Services, ensuring faculty and staff are familiar with BCDR protocols for emergencies, business disruptions, and compliance with this Policy and supporting standards/guidelines.
- Maintaining an appreciation of the risks associated with the loss of confidentiality, integrity, or availability of information resources used in their office or department.
- Determining the proper levels of protection, through consultation/coordination with the CISO and IT Services, for unit information resources and ensuring necessary safeguards are implemented and recovery procedures defined.
- Ensuring all information resources used by their respective units are assigned an Information Owner.
- With assistance from the CIO, C ISO, and IT Services, promoting BCDR awareness in their units and ensuring all staff participate in relevant training.
- Ensuring staff compliance with the requirements of the Information Security Program.

B. Business Impact Analysis

On an annual basis, all University 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	• Information systems that must be functioning and operational before dependent systems can perform as intended. • Immediate recovery is required to prevent major interruption of University operations. • System maximum downtime of 2 hours or less.
Critical	• Information systems essential to support University business operations. • System loss or failure will have an extreme impact on business operations. • System maximum downtime of 4 hours or less.

High	• Information systems crucial to support University business operations. • System loss or failure will have a significant impact on business operations. • System maximum downtime of 24 hours or less.
Medium	• Information systems important to support University business operations. • System loss of failure will have a moderate impact on business operations. • System maximum downtime of 72 hours or less.
Low	• Information systems providing improved effectiveness or efficiency of University business operations. • System loss or failure will have a negligible impact on business operations. • System downtime greater than 72 hours.

C. **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 the University's management and staff are able to put the plan into operation.

D. **Training and Awareness**

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

E. **Maintenance**

University Senior Leadership must ensure that their BCDR plans are reviewed 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.

F. **Approval**

A BCDR unit plan shall be reviewed by the CIO and CISO and approved by the appropriate University Division Leader(s). Once approved by all levels, any future updates to the specific BCDR plan need only to be approved by the appropriate unit head. The CIO and CISO will periodically review all plans for accuracy and updates as needed. The CIO will provide periodic reports on University-wide BCDR planning efforts to the Chancellor and Cabinet.

IV. PROCEDURES

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