FAYETTEVILLE STATE UNIVERSITY

INFORMATION SECURITY INCIDENT RESPONSE

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 ●Students

History: First Issued – May 5, 2022

Related Policies:
- Information Classification and Handling
- Information Security

Contact for Info: Vice Chancellor for Information Technology and Chief Information Officer (910) 672-1200

I. PURPOSE

The purpose of this policy (Policy) is to define the process, roles, and responsibilities of Fayetteville State University (University) in the investigation and response to information security incidents that threaten the confidentiality, integrity, and availability of University information resources.

II. DEFINITIONS

The following definitions are used in this Policy:

- **Information Security Incident** shall mean any event that has the potential to negatively impact the confidentiality, integrity, or availability of Fayetteville State University's sensitive information (including physical files such as paper files) or Mission-Critical Resources. Examples of potential incidents include but are not limited to: the loss or theft of a mobile device that has not been encrypted and that stores sensitive, University-owned information, a virus infection of an end-user workstation that works with sensitive, University-owned information or the malicious disabling of a piece of hardware that endangers Mission-Critical Resources.

- **ISO** shall mean the staff of the Information Technology Services, Information Security Office.

- **Incident Handler** shall mean a University employee trained in incident handling techniques.

- **Mission Critical Resource** shall mean any resource that is critical to the mission of the University. Typical Mission-Critical Resources have a maximum downtime of three consecutive hours or less. The owning business unit determines whether a resource is mission critical. Once designated as mission critical, information security policies and standards apply in an effort to assure that the resource remains available. If a business unit

does not designate a resource as mission-critical, that resource may not be a priority for restoration of services in the event of an incident or outage.

- **Sensitive Information:** Sensitive Information shall mean information which contains the following:

    - **Personal Identifying Information (PII),** as defined by the North Carolina Identity Theft Protection Act of 2005. In combination with name, PII includes employer tax ID numbers, drivers' license numbers, passport numbers, SSNs, state identification card numbers, credit/debit card numbers, banking account numbers, PIN codes, digital signatures, biometric data, fingerprints, passwords, and any other numbers or information that can be used to access a person's financial resources.
    - **Protected Health Information** as defined by Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - **Student education records**, as defined by the Family Educational Rights and Privacy Act (FERPA)
    - **Customer record information**, as defined by the Gramm Leach Bliley Act (GLBA)
    - **Card holder data**, as defined by the Payment Card Industry Data Security Standards (PCI DSS)
    - **Confidential personnel information**, as defined by the *Privacy of State Employees Personnel Records Act*.
    - **Information** that is deemed to be confidential in accordance with the North Carolina Public Records Act
    - **Sensitive information** also includes any other information that is protected by the University Information Classification Standard or law from unauthorized access. Sensitive information must be restricted to those with a legitimate business need for access.

III. ROLES AND RESPONSIBILITIES

The following individuals are responsible for managing information security incidents:

A. Users

Users (University employees, students, contractors, and visitors) who have access to University-owned or managed information through computing systems or devices (including physical files containing payment card holder information) must immediately report all suspected incidents that involve risk to sensitive, University-owned information and/or Mission-Critical Resources as per the University Incident Management Procedures outlined in Section IV.

B. ISO

To protect Sensitive Information or Mission-Critical Resources, the ISO shall direct the incident response and investigation, in coordination and collaboration with the affected department(s).

C. Chief Information Security Officer and the Chief Information Officer

The Chief Information Security Officer (CISO) and the Chief Information Officer (CIO) have the authority to take any action appropriate to mitigate the risk posed by any Information Security Incident. Information Technology Services (ITS) is entitled to obtain reimbursement of associated costs from appropriate department(s) relevant to incident investigation and resolutions.

D. Incident Handlers

The Incident Handler shall provide incident management, consulting, and referral services to the Division of Legal, Audit, Risk and Compliance (LARC) and other services as appropriate.

IV. INCIDENT REPORTING/MANAGEMENT PROCEDURES

A. Incident Reporting

Any individual who has been granted access to University-owned or managed information and/or who suspects an Information Security Incident that might endanger any Sensitive, University-owned Information or Mission-Critical Resource must follow these steps:

1. If sensitive information is believed to be in current danger of being acquired remotely from a computing device by an unauthorized party, a User may disable or disconnect the network interface on the system. Doing so will limit the information available to Incident Handlers so Users should only disable a network interface when necessary to protect against an identified, current threat.

2. To preserve potential evidence, the potentially compromised system should remain powered up and no one should use the system in any way until instructed otherwise by an Incident Handler.

3. Immediately report the suspected Incident to the ITS Service Desk, which is available by calling 910-672-HELP (4357). If a phone is not available, the suspected Incident should be reported via a Service Desk ticket for tracking purposes.

4. A request should be made to the Service Desk staff member to "please create a critical ticket for Information Security."

5. A name and a telephone number at which the reporting User can be reached should be provided.

6. If University equipment has been lost or stolen, the primary user of the equipment must notify University Police at 910-672-1775.

Events that do not place sensitive, University-owned information or Mission-Critical Resources at risk need not be reported to the ISO, but the ISO is available to offer counsel at any time and should be informed of any account compromises, sensitive or otherwise.

B. Incident Management

Information Security Incidents shall be managed as follows:

1. ITS Incident Handlers will lead response efforts including preserving evidence and ensuring an audit trail regarding investigation of the incident.

2. The assigned ITS Incident Handler may notify the appropriate departmental campus contacts. but the individual reporting the matter may consult with their departmental staff in addition to ITS at any time.

3. The ISO will coordinate with the University's Department of Police and Public Safety, LARC and others University units as needed.

4. All external communications with the media or the public related to any Information Security Incident must be coordinated through LARC and the Office of the Chief Information Officer or their designee.

5. If the CISO determines that the affected University unit may lead the incident handling activity or a component thereof, the ISO must be regularly and comprehensively updated on the progress of the incident response.