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

History: Issued – October 26, 2021

Related Policies/ Regulations/Statutes: ●*Information Classification and Handling*

Contact for Info: Deputy Chief Information Officer (910) 672-1958

I. PURPOSE

The purpose of this 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. This policy (Policy) defines the roles and responsibilities for incident response team members, incident severity levels, the incident response lifecycle, and specific incident response activities.

II. DEFINITIONS

The following definitions are used in this Policy:

- **Availability** shall mean degree to which information and critical College services are accessible for use when required.

- **Confidentiality** shall mean the degree to which confidential University information is protected from unauthorized disclosure.

- **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.

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

- **Personally Identifiable Information (PII)** shall mean a*ny information about an individual* maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

- **Risk** shall mean the probability or threat of damage, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

- **Security Breach or Security Compromise.** An unauthorized intrusion into a University information resource where unauthorized disclosure, modification, or destruction of confidential information may have occurred.

- **Security Event.** A system, service, or network state, condition, or occurrence indicating information security may have been breached or compromised or that an information security policy may have been violated or control may have failed.

- **Security Incident.** An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information system operation; or violation of information security policy.

III. ROLES AND RESPONSIBILITIES

The roles, and responsibilities of individuals in the investigation and response to information security incidents is as follows:

A. Chief Information Officer (CIO)

The Chief Information Office serves as the senior executive officer responsible for University-wide planning, management, security, and coordination of information technology resources. During an information security incident, the CIO shall be responsible for the following:

- Serving as the primary point of contact for significant cyber incidents (internally and externally).
- Providing support or backup for the Information Security Office / Officer (ISO).
- Coordinating additional resource allocation as required.
- Assisting with incident investigation if necessary.
- Collaborating with the ISO in decision-making when University operations is impacted.
- Declaring.
- Notifying the Chancellor who shall declare a disaster, if necessary, to trigger disaster recovery activities.
- Coordinating communication to other University leadership team members during an information security incident.
- Notifying University Communications as appropriate for internal and external communication.

B. Information Security Office/Officer (ISO)

The Information Security Office/Officer has authority and responsibility for operation and management of the University's Information Security Program. During an information security incident, the ISO shall be responsible for the following:

- Managing the overall University information security incident response activities, escalating to the CIO as necessary.
- Accessing and assigning incident severity.
- Notifying the CIO and General Counsel of a suspected or actual information security incident.
- Activating the Information Security Incident Response Team (ISIRT).
- Managing incident resources and task assignments.
- Identifying external personnel/resources as needed.
- Assisting in incident containment, investigation, remediation, and recovery.
- Collecting and documenting incident details and response activities.
- Notifying and briefing the CIO and University leadership team, as appropriate.
- Notifying the Chief of Police 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 University leadership team immediately after the investigation is finalized.

C. Information Security Incident Response Team (ISIRT)

The Information Security Incident Response Team (ISIRT) is a cross-functional team assembled to assist during an information security incident. Once activated, this team will remain active until the incident is closed. The core membership of the ISIRT is the CIO and ISO.

During an information security incident, the ISIRT shall be responsible for the following:

- Assembling additional team members as required, e.g. additional members of IT Services, General Counsel, or other University faculty and staff.
- Assisting in incident containment, investigation, remediation, and recovery.
- Collecting and documenting incident details and response activities.
- Performing damage assessment to determine appropriate steps to recover, e.g. restoration from backup, system reinstall.
- Tracking incident task assignments to closure.
- Restoring normal operations.
- Participating in postmortem discussions to determine root cause, necessary changes/updates, response strengths/weaknesses, and lessons learned.

D. Information Technology Services (IT Services)

Information Technology Services staff have primary operational responsibility for information systems that receive, create, store, handle, or discard information. During an information security incident, IT Services shall be responsible for the following:

- Escalating reported information security incidents to the ISO for analysis.
- Assisting the ISO or ISIRT in incident containment, investigation, remediation, and recovery.
- Collecting and documenting incident details and response activities as requested by the ISO or ISIRT.
- Granting and revoking user rights to information resources and privileged user access to information systems as directed by the ISO, ISIRT, or information resource owners.
- Performing system or data recovery to restore normal operations as requested by the ISO or ISIRT.
- Providing technical support to the ISO or ISIRT as needed.

E. Police and Public Safety

During an information security incident, the Police and Public Safety Department shall be responsible for the following:

- Assisting with incident investigation when necessary.
- Coordinating with external law enforcement as required or requested by the CIO, ISO, or General Counsel.

F. General Counsel

During an information security incident, the 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 notification is required under North Carolina law.
- Working with the CIO and ISO/ISIRT as appropriate to ensure that any notifications and other legally required responses are made in a timely manner.
- Advising the University regarding involvement of law enforcement and regulatory agencies.
- Advising the University’s faculty and staff regarding investigations involving employees and/or students.
- Reviewing incident communications drafted by University Communications.
- Liaising with external counsel as required.

G. Communications

During an information security incident, the University’s Communications department shall be responsible for the following:

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

H. Faculty, Staff, and Students

All members of the University community are required to report suspected or actual information security incidents or security breaches. These incidents include thefts of computer devices, viruses, worms, or computer "attacks" that may lead to unauthorized access to confidential information.

Information security incidents should be reported to:

- Information Security Office / Officer, **InfoSec@uncfsu.edu**
- IT Services Help Desk, **910-672-HELP (4357)** or www.uncfsu.edu/help
- University manager or supervisor.

IV. INCIDENT SEVERITY LEVELS

Incident severity will dictate the University's response to and management of a security event, incident, or breach. Factors used to determine severity include, but are not limited to: the sensitivity of impacted data, the number of End Users impacted, and the overall impact to University operations and reputation. During the lifecycle of a security incident, the severity level may raise or lower as a result of further assessment and response activities.

HIGH

A HIGH severity incident will demonstrate the following characteristics:

- Threatens to impact (or does impact) critical University systems, e.g.:
  - Email
  - Courseware
  - Human Resources
  - Financials
  - Internet connectivity
  - Internal University network connectivity
- Threatens serious financial risk or legal liability.
- Threatens to compromise (or does compromise) *Confidential* University data (see policy on *Information Classification and Handling*).
- Threatens to spread to or impact other organizations or networks external to the University.
- Threatens human life or property by terroristic or other threat.

MEDIUM

A MEDIUM severity incident will demonstrate the following characteristics:

- Threatens to impact (or does impact) a significant number of University systems or faculty, staff, or students. The University can continue to operate but a group, department, or building may be unable to perform normally.
- Threatens a non-critical system or service.
- Systems impacted contain only *Internal Use Only* or *Public* University data (see policy on *Information Classification and Handling).*

LOW

A LOW severity incident will demonstrate the following characteristics:

- Threatens to impact (or does impact) a small number of University systems or faculty, staff, or students.

- Threatens a non-critical system or service.
- Systems impacted contain only *Public* University data (see policy on *Information Classification and Handling).*
- Minimal to no risk of the incident spreading or impacting other organizations or networks external to the University.

V. INCIDENT RESPONSE

A. Response Table

The following table represents how an incident should be responded to response to an based upon severity level.

INCIDENT SEVERITY	**RESPONSE TIME**	**INCIDENT MANAGER**	**NOTIFICATION**	**INCIDENT REPORT**
HIGH	Immediate	ISO and ISIRT	• ISO and/or ISIRT • CIO • Campus Safety • General Counsel • Others on a need-to-know basis	Yes
MEDIUM	4 Hours	ISO	• ISO • CIO • Campus Safety • General Counsel • Others on a need-to-know basis	If requested by CIO, Campus Safety, General Counsel, or other University administrator.
LOW	Next Business Day	ISO	• ISO • CIO • Others on a need-to-know basis	No

B. Incident Response Lifecycle

The following elements represent phases of the incident response lifecycle and provide tasks that may be performed during each.

1. Preparation

- Establish an incident response capability.
- Ensure University systems, networks, and applications are sufficiently secure.
- Implement security monitoring of University information resources.
- Perform periodic risk assessments of systems and applications.

- Ensure faculty, staff, and students are aware of policies and procedures regarding appropriate use of University information resources.
- Train IT staff to maintain University information resources in accordance with University security standards.

2. Detection and Analysis

- Discover an incident through security monitoring or notification by internal or external party.
- Perform an initial analysis to determine the incident's scope, severity level, and risk of continued operations.
- Follow response time and notification requirements defined in Section V.A.
- Document all facts regarding the incident:
    - Incident status (New, In Progress, Resolved, etc.)
    - A summary of the incident.
    - Indicators and other incidents related to the incident.
    - All actions taken by the incident response team.
    - Chain of custody, if applicable.
    - Impact assessments related to the incident.
    - Contact information for other involved parties.
    - A list of evidence gathered during the incident investigation.
    - Next steps to be taken.
- Notify impacted parties or regulatory agencies as required by contracts or regulations.

3. Containment, Eradication, and Recovery

- Determine the technical plan of action.
- Identify and isolate affected systems (e.g. shut down a system, disconnect if from a network, disable certain functions).
- Collect, preserve, and secure evidence.
- Eradicate the incident:
    - Identify and mitigate all vulnerabilities that were exploited.
    - Remove malware, inappropriate materials, and other malicious components.
- Revert any unauthorized changes, restore from clean backups, or rebuild affected systems as necessary.
- Install service packs, Hotfixes, or security patches as necessary and recommended by the vendor.

4. Post-Incident Activity

- Conduct a "lessons learned" meeting with all involved parties following incident resolution.
- Generate an incident report as required in Section 4.3.
- Retain incident evidence following University retention guidelines.

VI. INCIDENT REPORTING REQUIREMENTS

All members of the University community are required to report suspected or actual information security incidents or security breaches. These incidents include thefts of computer devices, viruses, worms, or computer "attacks" that may lead to unauthorized access to confidential information.

Information security incidents should be reported to the following:

- Information Security Office / Officer, **InfoSec@uncfsu.edu**
- IT Services Help Desk, **910-672-HELP (4357)** or www.uncfsu.edu/help
- University manager or supervisor.

VII. BREACH OF PII OR PHI

A security incident involving a breach or inappropriate disclosure of PHI (Personal Health Information) or PII (Personally Identifiable Information) may require the University to perform specific response actions as required by data protection laws and regulations (such as HIPAA or various state Data Privacy laws). If a security incident involves the breach (or potential breach) of PHI or PII, the ISO must immediately engage the General Counsel to ensure that all activities required by law, regulation, or contractual obligation are performed appropriately.

VIII. INCIDENT DISCLOSURE / NOTIFICATION

Only authorized University employees are permitted to disclose information about security incidents to individuals or parties outside of the University. IT Services staff may provide informational updates to faculty, staff, and students as is necessary in the course of addressing a security incident. The ISO will work to provide timely updates to these employees so they have current information to share. Employees who do not normally interface with faculty, staff, or students as part of their job duties should refer requests for information about security incidents to the ISO or to the IT Services Help Desk.

If the security incident involves a breach of PHI or PII, the ISO will work with the CIO, General Counsel, and University Communications to perform any required information disclosures related to the breach.

Any request for information about a security incident from parties other than affected University faculty, staff, or students (e.g. media, law enforcement, other government agency, etc.) must be referred to the ISO, CIO, or General Counsel.