INCIDENT RESPONSE
07.300.05

Authority:	Chief Information Officer (CIO)
History:	Approved by CIO July 10, 2021
Sources of Authority:	UNC System Office Policy Manual, Chapter 1400 "Information Technology"; International Organization for Standardization ISO/IEC 27002
Related Links:	07.100.00 Responsible Use of Information Technology Resources 07.200.00 Responsible Management of Information Technology Resources
Responsible Office:	Information Technology Services

I. Purpose

The purpose of this policy is to ensure a consistent and effective approach to the management of information security incidents, including communication on security incidents and weaknesses.

II. Scope

This policy applies to all authentication services that provide access to resources including, but not limited to, the following identities students: faculty, staff, contractors, vendors, business partners, service providers, volunteers, part-time employees, interns, guests, assistants, systems, application program interface tokens, and service accounts.

III. Definitions

A. Event – Any observable occurrence in an information system.

B. Incident – An adverse event that implies harm or attempt to harm. This includes events where an individual or process is not in compliance with UNCW policy.

C. Security Incident – Any incident that negatively impacts the confidentiality, integrity or availability of university data, applications, networks or systems.

IV. Policy

A. Management of Security Events

1. In the case of a suspected security incident or data breach, immediately report it to: itsecurity@uncw.edu. An evaluation of the incident's severity will be conducted at the discretion of ITS Security or relevant authority. If warranted, ITS Security will be charged with

a) pursuing an investigation

b) convening the Cybersecurity Incident Response Team (CSIRT);

c) maintaining appropriate contact with legal representation, law enforcement, compliance personnel, or other appropriate authority;
d) reporting on the details and findings of that investigation;
e) and making recommendations for improvements to minimize the risk of a similar event occurring in the future.

2. It is the responsibility of all campus community members to fully comply with requests for cooperation and resources.

3. The response to a security incident will be assessed and addressed based on the following criteria listed in order of decreasing priority:
a) Security incidents negatively affecting human life or safety
b) Security incidents affecting critical systems or infrastructure
c) Security incidents with the potential for widespread or extensive impact
d) Security incidents that affect the confidentiality, integrity or availability of UNCW data at any level

4. It is the obligation of all investigation team members to appreciate the magnitude of the investigation and to ensure integrity and discretion throughout the investigation process.
a) At any time during the course of an investigation, the CSIRT or ITS Security may request a campus member's participation on the investigation team as a subject matter expert.
b) All individuals who participate in conducting an investigation must report directly to and be approved by management within the ITS Security or relevant authority.
c) Information throughout the investigation will only be shared with individuals on a need-to-know basis.
d) Depending on the significance of the investigation, additional training may be required to provide team members with skills, such as evidence collection, chain of custody, or forensics, sufficient to addressing the needs of the investigation.
e) The investigative team, in coordination with the relevant authority, reserves the right to suspend any account or resources to any user throughout the course of the investigation.
f) All resulting documentation procured during the course of the investigation is to be considered confidential. Relevant materials will be shared with individuals who need to have knowledge of investigation details.
g) Documentation pertaining to the investigation must be stored in a secure location or destroyed upon completion of the investigation.
(1) Documentation and reports are classified as highly sensitive.
(2) Any reports that are retained after the completion of an investigation must be appropriately redacted to protect against unwanted disclosure of private or sensitive information.

B. Reporting

1. Suspected security incidents, including but not limited to accidental exposure of sensitive data or critical business data to unauthorized individuals, should immediately be reported to itsecurity@uncw.edu.

2. Any action taken by persons not trained in incident handling outside of this escalation procedure could put the organization risk due to possible (and likely unintentional) evidence tampering or destruction of network intrusion logs. Therefore, such action by any staff member that is not a member of the CSIRT may be considered a violation of policy and could have serious consequences for the staff member, up to and including termination of employment.

3. Once a user has detected a possible incident or weakness, all information regarding the event must be kept confidential. Disclosure may dramatically increase the impact of an event.

4. External communication regarding an event may only be provided through coordination with the CSIRT or the Office of University Relations.

C. Education / Training

1. Annual incident response training should be provided by IT Security to all with incident response responsibility.

2. This incident response policy should be tested at least annually.