ELIZABETH CITY STATE UNIVERSITY
Information Security Incident Response Policy

1. PURPOSE

The purpose of this policy is to define the process, roles, and responsibilities of Elizabeth City State University (ECSU) in the investigation and response to information security incidents that threaten the confidentiality, integrity, and availability of ECSU information resources. This policy defines the roles and responsibilities for incident response team members, incident severity levels, the incident response lifecycle, and specific incident response activities.

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 to all other members of the ECSU community.

3. ACRONYMS / DEFINITIONS

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

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

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 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.

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

Personally Identifiable Information (PII). Any 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.

Protected Health Information (PHI). Any information in a medical record that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment.

Risk. 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 an ECSU 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.

Vulnerability. A weakness in ECSU's operating environment that could potentially be exploited by one or more threats.

4. POLICY

A. ROLES AND RESPONSIBILITIES

i. Chief Information Officer (CIO)

The Chief Information Officer 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:

a. Serving as the primary point of contact for significant cyber incidents (internally and externally).
b. Providing support or backup for the Information Security Office / Officer (ISO).
c. Coordinating additional resource allocation as required.
d. Assisting with incident investigation if necessary.
e. Collaborating with the ISO in decision-making when ECSU operations are impacted.
f. Declaring a disaster if necessary to trigger disaster recovery activities.
g. Notifying the Chancellor along with internal and external stakeholders.
h. Coordinating communication to other ECSU executives during an information security incident.
i. Notifying ECSU Communications as appropriate for internal and external communication.

ii. **Information Security Office/Officer (ISO)**

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

a. Managing the overall ECSU information security incident response activities, escalating to the CIO as necessary.
b. Accessing and assigning incident severity.
c. Notifying the CIO and General Counsel of a suspected or actual information security incident.
d. Activating the Information Security Incident Response Team (ISIRT).
e. Managing incident resources and task assignments.
f. Identifying external personnel/resources as needed.
g. Assisting in incident containment, investigation, remediation, and recovery.
h. Collecting and documenting incident 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 investigation is finalized.

iii. **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:

a. Chief Information Officer (CIO)
b. Information Security Officer (ISO)
c. Lead Network Engineer
d. Chief Communications Officer (CCO)

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

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

iv. **Division of Information Technology (DIT)**

DIT staff have primary operational responsibility for information systems that receive, create, store, handle, or discard information. During an information security incident, DIT personnel shall be responsible for:

a. Escalating reported information security incidents to the ISO for analysis.
b. Assisting the ISO or ISIRT in incident containment, investigation, remediation, and recovery.
c. Collecting and documenting incident details and response activities as requested by the ISO or ISIRT.
d. 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.
e. Performing system or data recovery to restore normal operations as requested by the ISO or ISIRT.
f. Providing technical support to the ISO or ISIRT as needed.

v. **University Police**

During an information security incident, University Police shall be responsible for:

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

vi. **General Counsel**

During an information security incident, ECSU General Counsel shall be responsible for:

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/ISIRT as appropriate to ensure that any notifications and other legally required responses are made in a timely manner.
c. Advising ECSU regarding involvement of law enforcement and regulatory agencies.
d. Advising ECSU faculty and staff regarding investigations involving employees and/or students.
e. Reviewing incident communications drafted by ECSU Communications & Marketing Department.
f. Liaising with external counsel as required.

vii. **ECSU Communications & Marketing**

During an information security incident, ECSU Communications & Marketing Department shall be responsible for:

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.

viii. Faculty, Staff, and Students

All members of the ECSU 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:

a. Information Security Officer, infosec@ecsu.edu
b. IT Services Help Desk at (252) 335-3532
c. ECSU manager or supervisor.

B. INCIDENT SEVERITY LEVELS

Incident severity will dictate ECSU'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 ECSU 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:

i. Threatens to impact (or does impact) critical ECSU systems, for example:
  a. Email
  b. Courseware
  c. Human Resources
  d. Financials
  e. Internet connectivity
  f. Internal ECSU network connectivity
ii. Threatens serious financial risk or legal liability.
iii. Threatens to compromise (or does compromise) *Confidential* ECSU data
iv. Threatens to spread to or impact other organizations or networks external to the ECSU.
v. Threatens human life or property by terroristic or other threat.

MEDIUM

A MEDIUM severity incident will demonstrate the following characteristics:

i. Threatens to impact (or does impact) a significant number of ECSU systems or faculty, staff, or students. ECSU can continue to operate but a group, department, or building may be unable to perform normally.
ii. Threatens a non-critical system or service.
iii. Systems impacted contain only *Internal Use Only* or *Public* ECSU data.

LOW

A LOW severity incident will demonstrate the following characteristics:

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

ii. Threatens a non-critical system or service.
iii. Systems impacted contain only *Public* ECSU data.
iv. Minimal to no risk of the incident spreading or impacting other organizations or networks external to the ECSU.

INCIDENT RESPONSE

INCIDENT SEVERITY	RESPONSE TIME	INCIDENT MANAGER	NOTIFICATION	INCIDENT REPORT
HIGH	Immediate	ISO and ISIRT	A. ISO and/or ISIRT B. CIO C. University Police D. General Counsel E. Others on a need-to-know basis	Yes
MEDIUM	4 Hours	ISO	A. ISO B. CIO C. University Police D. General Counsel E. Others on a need-to-know basis	If requested by CIO, University Police, General Counsel, or other ECSU administrator.
LOW	Next Business Day	ISO	A. ISO B. CIO C. Others on a need-to-know basis	No

C. INCIDENT RESPONSE LIFECYCLE

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

PREPARATION

i. Establish an incident response capability.
ii. Ensure ECSU systems, networks, and applications are sufficiently secure.
iii. Implement security monitoring of ECSU information resources.
iv. Perform periodic risk assessments of systems and applications.
v. Make faculty, staff, and students aware of policies and procedures regarding appropriate use of ECSU information resources.
vi. Train DIT staff to maintain ECSU information resources in accordance with ECSU security standards.

DETECTION AND ANALYSIS

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

CONTAINMENT, ERADICATION, AND RECOVERY

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

POST-INCIDENT ACTIVITY

i. Conduct a "lessons learned" meeting with all involved parties following incident resolution.
ii. Generate an incident report as required in the Incident Response Chart.
iii. Retain incident evidence following ECSU retention guidelines.

D. INCIDENT REPORTING REQUIREMENTS

All members of the ECSU 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:

i. Information Security Officer at: infosec@ecsu.edu
ii. IT Services Help Desk at (252) 335.3532
iii. ECSU manager or supervisor.

E. 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 ECSU 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.

F. INCIDENT DISCLOSURE / NOTIFICATION

Only authorized ECSU employees are permitted to disclose information about security incidents to individuals or parties outside of ECSU. 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 ECSU Communications to perform any required information disclosures related to the breach.

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

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.