ELIZABETH CITY STATE UNIVERSITY
Information Security Incident Response Policy

Preamble

This policy outlines the procedures for decision-making regarding emergency actions taken for the protection of Elizabeth City State University (ECSU) information resources from accidental or intentional unauthorized access, disclosure or damage.

1. Applicability

This policy is applicable to all University students, faculty and staff and to all others granted use of Elizabeth City State University information resources who become aware of an information security incident concerning a Network, Academic or Administrative Computing System. Every user of any of ECSU’s information resources has responsibility toward the protection of the University’s information assets; certain offices and individuals have very specific responsibilities.

2. Purpose

ECSU recognizes the need to follow established procedures to address situations that may indicate that the security of the University’s information assets may have been compromised. The purpose of information security incident response is to mitigate the effects caused by such an incident and to protect the information resources of the University from future unauthorized access, use or damage. Such procedures include ensuring that the appropriate level of University management becomes involved in the determination of actions implemented in response to an information technology security incident.

A standard University wide approach to information security events is important because of the following factors:

A. The need to promptly and effectively address any improper access of University information systems or the data they contain
B. Legal and regulatory requirements regarding the safeguarding of University information assets
C. The University’s implementation and reliance on University-wide applications, like Banner and Oracle, which impact the entire campus
D. Intellectual capital that ECSU both produces and owns needs to be protected against premature disclosure or unauthorized tampering
E. Damage to the University’s SACS accreditation status can have both direct and indirect negative effects
F. A general worldwide increase in the number and severity of computer security incidents
G. The need to protect the privacy of persons whose information is stored on information systems owned by the University
3. Definitions

A. Information Security Incident — An information security incident is defined as any real or suspected adverse event in relation to the security of computer systems or computer networks. Examples of incidents include activities such as:

I. Attempts (either failed or successful) to gain unauthorized access to a system or its data
II. Unscheduled system down time or service interruption
III. Unwanted disruption or denial of service
IV. The unauthorized use of a system for the processing or storage of data
V. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

B. Administrative Computing System — Any application, or information system, that directly or indirectly deals with or supports financial, administrative, or other information that is an integral part of running the business of the University

C. Academic Computing System — Any application, or information system, that directly or indirectly deals with or supports the University’s primary mission of teaching, learning and research.

D. Resources – Hardware, firmware, or software

4. Notification

A member of the University community who becomes aware of an information security incident involving an Academic or Administrative Computing System must immediately:

A. Submit a security ticket to helpdesk@mail.ecsu.edu or directly to the IT Security Incidence Response Team at itsirt@mail.ecsu.edu or
B. Contact the University’s Administrative Computing Office that handles Information Security at 252-335-3319 or itsecurity@mail.ecsu.edu.
C. Upon recommendation of the Chief Information Officer, the University’s IT Security Incident Response Team may convene a fact-finding working group comprised of cognizant business and technical personnel and, where appropriate (such as instances where legal requirements are implicated, e.g., where private data of individuals is compromised), consult with the University Attorney, and communicate the incident to the Internal Auditor and the Vice Chancellor for Business and Finance or designate(s).
5. IT Security Incident Response Team

When warranted by information obtained during preliminary fact-finding, the University’s Information Security Officer will promptly convene a meeting with the Information Technology Security Incident Response Team (ITSIRT). Depending on the circumstances of each situation, the Information Security Officer shall include in the ITSIRT representation of some or all of the office/department affected in resolving the incident.

6. Escalation of Decision-Making

The ITSIRT will plan and coordinate the activities of all the offices involved, keeping other concerned offices advised as appropriate. In carrying out this responsibility, the ITSIRT will ensure that important operational decisions are elevated to the appropriate Vice Chancellor to protect the fundamental interests of the University and others impacted by the incident. Such decisions include, but are not limited to:

A. Restricting information system access or operations to protect against unauthorized information disclosures
B. Reporting and/or publicizing unauthorized information disclosures, as required by law
C. Involving law enforcement agencies in cases where applicable statutes appear to have been violated
D. The Information Security Office will also be responsible for documenting the deliberations and decisions of the ITSIRT as well as all actions taken pursuant to ITSIRT deliberations.

7. Report Preparation

The Information Technology Security Incident Response Team, jointly with the Internal Audit office, will be responsible for writing a final report(s) to the appropriate University office(s) which summarizes findings regarding the information security incident and, if appropriate, makes recommendations for improvement of related information security practices and controls.

COGNIZANT OFFICE — Information Technology, Information Security, Administrative Computing department, Internal Auditor, Network Services Department

8. Information Technology Security Incident Response Team

Consist of Information Technology staff responsible for the daily security of the University Administrative and Academic Systems.

Members include:
Director of Administrative Computing, Information Security
Director of Network Services, Network Security
Director of IT Client Services
Banner Security Coordinator
Internal Auditor
Network Engineer
Network Analyst
Network Analyst, Email Administrator
Datacenter Coordinator and Backup Administrator
Database Administrator
Administrative Computing, Secretary