ELIZABETH CITY STATE UNIVERSITY
Information Security Awareness and Training Policy

1. PURPOSE

The purpose of this policy is to establish information security awareness training requirements for all authorized users of ECSU information resources. Employees, students and all other authorized users should gain a broad understanding of information security threats, risks, and best practices to assist ECSU in protecting the confidentiality, integrity, and availability of ECSU information resources accessed, managed, and/or controlled by the ECSU.

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. This policy applies to all information collected, stored or used by or on behalf of any operational unit, department and person within the community in connection with ECSU operations. In the event that any particular information at ECSU is governed by more specific requirements under other ECSU policies or procedures the more specific requirements shall take precedence over this policy to the extent there is any conflict.

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.

Phishing. The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers**.**

4. POLICY

The Information Security Officer (ISO) will develop and implement an information security awareness program to be offered periodically to all ECSU faculty, staff, students, and other authorized users of ECSU information resources. To demonstrate basic competency in information security best practices, faculty and staff must complete this training as part of the onboarding process, annually thereafter, or as required by the ISO. Students will have the option (not required) to complete the information security awareness training program.

INFORMATION SECURITY AWARENESS AND TRAINING PROGRAM

The Information Security Officer (ISO) will:

A. Develop or acquire information security training and test materials.
B. Update and revise training and test materials at least annually to reflect current threats and information security best practices.
C. Provide the ability to collect feedback regarding the content and efficacy of the training program.
D. Track, record, and report training/testing completion rates and other program statistics.
E. Ensure mandatory training compliance across ECSU.

Information security awareness training will include:

A. Information security awareness best practices.
B. Information security roles and responsibilities.
C. Acceptable use of ECSU information resources.
D. Information classification and handling.
E. Causes of unintentional data exposure (e.g. losing a mobile device, emailing the wrong person due to autocomplete)
F. Enabling and utilizing security authentication.
G. How to identify different forms of social engineering attacks (e.g. phishing, phone scams, impersonation calls).
H. Security incident indicators, reporting, and response.
I. Security terms and definitions.

Training in information security threats and safeguards for ECSU Division of Information Technology (DIT) staff is mandatory, with the extent of technical training to reflect the individual's responsibility for configuring and maintaining information security safeguards. Training requirements must be reassessed following any change in job role or responsibilities and new training provided as a priority.

An appropriate summary of the information security policies must be formally delivered to, and accepted by, all temporary staff and any external contractor, prior to starting any work or any supply of services for ECSU.

5. COMPLIANCE

ECSU information resource access privileges may be revoked for faculty and staff, or other authorized users, for whom training is required/mandatory who do not complete required/mandatory training within specified timelines.

6. 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.

7. 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.

8. EXCLUSIONS / EXCEPTIONS

No approved exceptions exist at this time.