700.2.7
Adopted: 12/15/15
Amended: 06/13/17
Amended: 03/09/22

# ELIZABETH CITY STATE UNIVERSITY
## Information Security Policy

## 1. PURPOSE

This policy defines the framework upon which the information security program operates and gives direction for Information Security-related policies, standards, and procedures to address specific areas of operation. This policy establishes minimum requirements to protect the confidentiality, integrity, and availability of Elizabeth City State University's (ECSU) information resources accessed, managed, and/or controlled by the University.

## 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 campus 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 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.*** 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.

## 4. POLICY

The ECSU information security program shall be designed to involve each person in training, awareness, reporting, protecting sensitive information, and implementing security controls.

ECSU information technology security program shall be based upon the framework outlined in the International Standards Organization (ISO) and International Electrotechnical Commission (IEC) standard 27002. The framework shall be appropriately interpreted by the Information Security Officer (ISO) and Chief Information Officer (CIO) who have determined that this framework conforms to the needs of this higher education institution. The ECSU information technology security program shall also be informed by security principles and best practices provided by a variety of other sources, including those established by industry organizations and professional associations.

A set of policies for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties. The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

The ECSU security program shall also be subject to applicable regulations, such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act (GBLA), North Carolina Identity Theft Statute, North Carolina Security Breach Notification Law, Digital Millennium Copyright Act, and intellectual copyright laws.

The Information Security Officer (ISO) shall recommend appropriate policies in keeping with applicable law and best practices. The ISO shall promulgate standards and procedures for the University to implement policy and support a robust information security program that enables the University to operate securely and effectively.

## 5. PROCEDURES

ECSU shall develop, manage, and review operating procedures to create the proper security posture for protecting the University’s 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 can be subject to criminal and/or civil action.

## 7. EXCLUSIONS / EXCEPTIONS

No approved exceptions exist at this time.