ELIZABETH CITY STATE UNIVERSITY
Information Security Compliance Policy

1. PURPOSE

The purpose of this policy is to ensure Elizabeth City State University (ECSU) remains in compliance with all applicable legal and regulatory requirements. To ensure appropriate safeguards are in place to comply with applicable statutory, regulatory, legal, and contractual compliance obligations.

2. SCOPE

This policy applies to all ECSU employees, whether full-time or part-time, paid or unpaid, temporary or permanent, volunteers, contractors, consultants, and vendors 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 university community in connection with ECSU's operations. If any 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's 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

A. COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

To avoid breaches of any criminal and civil law, statutory or State regulatory or contractual obligations, and security requirements, the design, operation, use and management of information systems may be subject to statutory, regulatory, and

contractual security requirements. Advice on specific legal or University of North Carolina System requirements shall be provided by Elizabeth City State University's (ECSU) Office of Legal Affairs.

Laws and standards include, but are not limited to, the following: Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), North Carolina Identity Theft Statute, North Carolina Security Breach Notification Law, Digital Millennium Copyright Act, and intellectual copyright laws.

All users of information and information resources of ECSU including employees, contractors, consultants, and vendors shall acknowledge and accept their responsibilities for information security.

B. INFORMATION SECURITY REVIEWS

ECSU supervisors shall ensure that all security processes and procedures within their areas or information systems under their control and responsibility are followed. In addition, all business units shall be subject to regular reviews to ensure compliance with security policies and standards.

C. SECURITY EXCEPTIONS

The Information Security Officer, with the approval of the institution of higher education head or his or her designated representative may issue exceptions to information security requirements or controls subject to a completed risk assessment. The Information Security Officer shall coordinate exceptions, risk assessments and compensating controls with information and service owners. Any such exceptions shall be justified, documented, approved and communicated as part of the risk assessment process.

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, contractor, consultant, and vendor 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.