ELIZABETH CITY STATE UNIVERSITY
Organization of Information Security Policy

1. PURPOSE

The purpose of this policy is to develop, implement, assess, authorize, and monitor cybersecurity risks and programs. This policy ensures the implementation of management controls to provide oversight over the implementation of security controls, security roles and responsibilities and security program monitoring, reporting and maturity.

2. SCOPE

This policy applies to Elizabeth City State University (ECSU) applicable 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 University in connection with ECSU operations. In the event that any particular information at ECSU is governed by more specific requirements under other university 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

A. INTERNAL ORGANIZATION

Management Responsibility and Accountability – ECSU formally establishes and documents responsibility and accountability for the information security function at the executive level. This accountability includes a definition and documentation of the information security organization responsible for managing and implementing the program.

Clear Assignment of Control Accountability - ECSU assigns and documents accountability for internal controls. This accountability includes sufficient transparency so that management will be kept informed about the effectiveness and efficiency of these same internal controls.

IT Risk Review Board – ECSU has an IT Risk Review Board comprised of Vice Chancellors (or their designees) that meets at least quarterly to review the status of information risk and security at ECSU, approve and later review information security projects, review new or modified information security policies, and provide oversight over IT Governance and information security management activities.

Information Security Resources – ECSU allocates resources and staff to address information systems security.

Clear Management Support – Management provides clear support of information security efforts, including funding, organizational assignments, and senior management sponsorship of information security policies.

Information Security in Project Management - All significant development projects within ECSU that may impact the security of sensitive information include information security requirements as part of the formal planning process.

Centralized Information Security - Guidance, direction, and authority for all information security activities are centralized for the entire organization.

Information Security Liaisons - Every division or department head designates an information security liaison and gives this liaison sufficient training, in collaboration with Division of Information Technology (DIT), supporting materials, and other resources to properly perform their job.

Incident Response Team - Investigations of system intrusions and other information security incidents is the responsibility of Information Security Officer and affected departments.

Internal Audit Team- Compliance checking to ensure that organizational units are operating in a manner consistent with these requirements is the responsibility of ECSU Internal Audit Team.

Human Resources - Disciplinary matters resulting from violations of information security requirements are handled by local managers working in conjunction with the Office of Human Resources.

B. INFORMATION SECURITY ROLES & RESPONSIBILITIES

Defining Specific Security Roles – ECSU defines specific job roles required for the effective implementation of the information security program. Each role includes a specific description of the information security-related duties performed by each team member performing those job functions.

Assigning Specific Security Roles – ECSU defines at least one individual responsible for the duties of the information security specific roles.

Assigning Information Security Officer – ECSU defines at least one individual responsible for the duties of the information security function. This role will be entitled "Information Security Officer (ISO)."

Human Resources (HR) - Personnel managers, in conjunction with the Office of Human Resources, ensure that cybersecurity responsibilities are clearly defined in performance objectives for all relevant personnel.

C. SEGREGATION OF DUTIES

Conflicting duties and areas of responsibility are segregated to reduce opportunities for fraud, unauthorized or unintentional modification or misuse of information assets. Where adequate segregation cannot be achieved, other compensating controls are established and documented.

D. CONTACT WITH AUTHORITIES AND SPECIAL INTEREST GROUPS

Contacting Law Enforcement - Every decision about the involvement of law enforcement with information security incidents or problems are made by the Information Security Officer in conjunction with members of the IT Risk Review Board, Legal Affairs, and University Police.

Cybersecurity Response Capability – Incident Response Procedures are in place that specify when and by whom authorities (e.g., law enforcement, regulatory bodies, supervisory authorities) will be contacted and how identified cybersecurity incidents will be reported.

Special Interest Groups – ECSU maintains appropriate contacts with special interest groups or other specialist security forums and professional associations within the security community to facilitate ongoing security education and training for organizational personnel; maintain currency with recommended security practices, techniques and technologies; and share current security-related information including threats, vulnerabilities and incidents.

E. INFORMATION SECURITY IN PROJECT MANAGEMENT

ECSU assesses the security controls in information system and infrastructure projects to determine the extent to which security controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system.

5. PROCEDURES

ECSU develops, manages, and reviews operating procedures to improve the security maturity in protecting ECSU information resources. Such procedures are periodically reviewed as required.

6. COMPLIANCE / ENFORCEMENT / SANCTIONS

Any ECSU employees 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.