ELIZABETH CITY STATE UNIVERSITY
Risk Assessment and Management Policy

1. PURPOSE

The purpose of this policy is to establish a process to assess, manage, and remediate risks to Elizabeth City State University (ECSU) that result from threats to the confidentiality, integrity, and availability of ECSU information resources. It is the responsibility of all employees and students to identify, analyze, evaluate, respond, monitor, and communicate risks associated with any activity, function, or process within their relevant scope of responsibility and authority.

2. SCOPE

This policy applies to all ECSU employees and students, 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. 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.

Control. Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Impact. The consequences, or effects, of a security incident occurring.

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 the ECSU.

Probability. The likelihood, or possibility, of a security incident occurring.

Risk. The probability or threat of damage, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

Security Breach or Security Compromise. An unauthorized intrusion into an ECSU information resource where unauthorized disclosure, modification, or destruction of confidential information may have occurred.

Security Event. A system, service, or network state, condition, or occurrence indicating information security may have been breached or compromised or that an information security policy may have been violated or control may have failed.

Security Incident. An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information system operation; or violation of information security policy.

Threat. A potential event that may cause harm or loss to ECSU, or individuals associated with ECSU.

Vulnerability. A weakness in ECSU's operating environment that could potentially be exploited by one or more threats.

4. POLICY

A. ASSESSING IT SECURITY RISK

To protect ECSU from the negative effects of security events or incidents, ECSU has established a process for analyzing threats and determining the appropriate actions to address or remediate those threats.

In context of this risk assessment process, ECSU uses the following terms:

i. **Threat.** A potential event that may cause harm or loss to ECSU, or individuals associated with ECSU.
ii. **Vulnerability.** A weakness in ECSU's operating environment that could potentially be exploited by one or more threats.
iii. **Control.** Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
iv. **Impact.** The consequences, or effects, of a security incident occurring.
v. **Probability.** The likelihood, or possibility, of a security incident occurring.

vi. **Risk.** The probability or threat of damage, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

The process of evaluating and assessing IT security risks covers the following activities:

Risk Identification:
The ongoing effort to identify events or issues that may lead to the occurrence of an IT security incident. Security risks may be identified as part of a formal security assessment process, or on an ad-hoc basis by the ECSU community as part of their normal work responsibilities.

Risk Analysis:
The process of determining and classifying the likelihood and impact of a given IT security risk. Other considerations in the analysis process may include timeframes of any security incidents, existing risk mitigations, and prioritization of risks relative to each other. In a formal security assessment process, each identified risk should be appropriately analyzed and classified, and this analysis will be documented in the ECSU Security Risk Register maintained by ECSU Information Security Officer (ISO).

Risk Mitigation:
Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve ECSU's response to a security incident. Note that depending on the situation, it may be appropriate for an identified risk to be accepted by ECSU (no mitigation activities undertaken). The ISO will work with the appropriate ECSU department or information resource owner to determine appropriate mitigation actions. In a formal security assessment process, each identified risk will be reviewed to determine appropriate mitigation activities. These activities will be documented in ECSU Security Risk Register maintained by the ISO.

ECSU Security Risk Register:
The ECSU Security Risk Register is a central repository for information related to security risks that have been identified by ECSU. It contains information about the identified security risk (including associated vulnerabilities), the impact and probability of damage or loss associated with the risk, and tracks progress toward addressing the risk or states that the risk has been accepted.

B. MANAGING IT SECURITY RISKS

ECSU has established the IT Risk Review Board (RRB) as a way for ECSU to identify, catalog, and analyze risks facing ECSU. The IT RRB provides a way for the ECSU to thoughtfully analyze threats and determine actions that are appropriate to address those threats.

The IT RRB is comprised of key decision makers from major divisions/units. Decisions about risk mitigation activities are made by business stakeholders, ensuring that actions are appropriate for ECSU and address risk in an effective manner.

The ECSU Security Risk Register is the mechanism utilized to track ECSU's security risks. As new security risks are identified by ECSU, they are evaluated by the RRB, and added to the risk register as appropriate. The risk register is reviewed and updated by the RRB at regular meetings (at least once per quarter) and more frequently as needed by the Information Security Officer (ISO).

The ISO is responsible for determining when a formal security risk assessment is required for a given system or situation. All ECSU employees are responsible for consulting with the ISO for security risk assessment in each of the following situations:

i. Use of an externally hosted system or application (SaaS or Cloud Service Provider) for storing or transmitting ECSU information.
ii. Deployment of any application, system, or service hosted by ECSU accessible remotely via the Internet.
iii. Deployment of any application, system, or service (internal or external) that will house any ECSU confidential data.
iv. Any configuration change to the ECSU firewall.
v. Any change in process or procedure for handling or interacting with confidential data.
vi. Any other scenario that may introduce a new security risk to the organization.

If you are unsure, contact the Information Security Officer (ISO) for assistance.

Security threats are constantly changing and evolving. It is important that ECSU environment be assessed for changes in security risk posture on an ongoing basis. Systems implemented and operated by ECSU are assessed for vulnerabilities on a periodic basis.

Additionally, security assessments must be performed at least annually for ECSU's data centers and external Internet presence. These assessments must be performed by an independent, third-party security assessment organization. The results of these assessments are to be reviewed by the ISO and appropriate Information Technology Services (ITS) staff, and any noted security issues must be remediated appropriately.

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 / SANCTIONS / ENFORCEMENT

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.

7. EXCEPTIONS

No approved exceptions exist at this time.