# ELIZABETH CITY STATE UNIVERSITY
## Information System Acquisition, Development, and Maintenance Policy

## 1. PURPOSE

The purpose of this policy is to ensure information security is an integral part of Elizabeth City State University (ECSU) information systems and resource lifecycle. This policy establishes minimum guidelines for ECSU's Division of Information Technology to protect the confidentiality, integrity, and availability of ECSU's information resources accessed, managed, and/or controlled by ECSU.

## 2. SCOPE

This policy applies to all ECSU employees, whether full-time or part-time, paid or unpaid, temporary or permanent, and volunteers. 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.

***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.

## 4. POLICY

### A. SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

Information security-related requirements must be included in the requirements for any new, or in enhancements to existing, ECSU information systems. Information security requirements must:

i. Be identified through policy and regulation compliance, threat modeling, incident reviews, or vulnerability assessments.
ii. Reflect the business value of the information resources involved.
iii. Consider the potential negative impact to ECSU from lack of adequate security.
iv. Be integrated early in information systems projects for more effective and cost-efficient solutions.
v. Be documented and reviewed by all relevant stakeholders.

Additionally, the following information security requirements must be addressed:
i. Access provisioning and authorization processes (all End Users, including privileged accounts).
ii. End User duties and responsibilities.
iii. Protections for the availability, confidentiality, and integrity of ECSU assets.
iv. Logging and monitoring needs.
v. Criteria for formal testing and acceptance of products into ECSU's environment.

Application services passing over public networks must be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. Considerations include the following:
i. Authentication and authorization processes.
ii. Authorizations for provision or use of the service.
iii. Protection requirements for confidential information.
iv. Safeguards, such as encryption, to protect the availability, confidentiality, and integrity of services and transactions.

Protected data involved in application service transactions must be secured to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

**B. SECURE DEVELOPMENT POLICY**

Rules for the development of software and systems must be established and applied within ECSU to ensure services, architecture, software, and systems are built securely, thereby reducing risk, vulnerabilities, and cost. These rules apply to internal development practice as well as any outsourced development contracted by ECSU. Aspects of secure development must be considered:
i. Security of the development environment.
ii. Secure development methodology and secure coding guidelines.
iii. Security requirements integrated in the design phase.
iv. Security checkpoints within project milestones.
v. Secure code repositories.
vi. Version control.
vii. Application security knowledge.
viii. Capability to detect, fix, and avoid vulnerabilities.

Changes to systems within the development lifecycle must be controlled through formal change control procedures, which at a minimum must include:

i. Documenting agreed authorization levels.
ii. Ensuring changes are submitted by authorized users.
iii. Reviewing controls and integrity procedures to ensure they will not be compromised by the change.
iv. Identifying all software, systems, and information that require change.
v. Reviewing security code to minimize the likelihood of known security weaknesses.
vi. Obtaining formal approval prior to work commencement.
vii. Ensuring authorized user acceptance prior to implementation.
viii. Ensuring system documentation is updated and previous versions are archived.
ix. Maintaining version control of all software updates.
x. Maintaining an audit trail of all change requests.
xi. Updating operating manuals and user procedures, as necessary.
xii. Scheduling implementation to minimize disruption.

When operating platforms (operating systems, databases, and middleware platforms) are changed, critical applications must be reviewed and tested to ensure no adverse impact on ECSU's operations or security. Notification of operating platform changes must be provided in time to allow appropriate testing and review of information systems and applications prior to implementation.

Modifications to vendor software packages must be discouraged, limited to necessary changes only. All changes must be strictly controlled, tested, and documented. If changes are required, the original software must be retained, and updates made to a designated copy.

Principles and procedures for engineering secure systems must be established, documented, and applied to information system engineering activities and must be designed into all architecture layers (business, data, applications, and technology) to ensure the availability, confidentially, and integrity of ECSU's information resources. These principles and procedures must be regularly reviewed to ensure they remain up to date in combating new threats and applicable to advances in technologies and solutions applied.

A secure development environment includes people, processes, and technology associated with system development and integration. ECSU must assess risks associated with individual system development efforts and establish secure development environments, considering:

i. Sensitivity of data to be processed, stored, and transmitted by the system.
ii. Applicable external and internal requirements, e.g., from regulations or policies.
iii. Security controls already implemented by ECSU that support system development.
iv. Trustworthiness of personnel working in the environment.
v. The degree of outsourcing associated with system development.
vi. The need for segregation between different development environments.

vii. Control of access to the development environment.
viii. Monitoring of change to the environment and the code within.
ix. Storage of backups at secure offsite locations.
x. Control over movement of data to and from the environment.

ECSU must supervise and monitor the activity of outsourced system development, to include:

i. Licensing arrangements, code ownership, and intellectual property rights related to the outsourced content.
ii. Contractual requirements for secure design, coding, and testing practices.
iii. Agreement of an approved approach for analyzing the security of the application.
iv. Acceptance testing for quality and accuracy of deliverables.
v. Agreement on minimum acceptable levels of security and privacy quality.
vi. Evidence sufficient testing has been applied to ensure the absence of intentional and unintentional malicious content upon delivery.
vii. Evidence sufficient testing has been applied to guard against the presence of known vulnerabilities.
viii. Right to audit development processes and controls.
ix. Effective documentation of the build environment used to create deliverables.

Testing of security functionality must be performed throughout the development process and must include a detailed schedule of activities and expected results under a range of conditions. Testing must ensure the system works as expected and only as expected. The extent of testing must be in proportion to the importance and purpose of the system.

Acceptance testing programs and criteria must be established for new information systems, upgrades, and new versions to include:

i. Testing of information security requirements.
ii. Testing of adherence to secure system development practices.
iii. Testing of received components and integrated systems.
iv. Use of code analysis tools and vulnerability scans to verify remediation of security-related defects.
v. Testing in a realistic test environment to ensure the tests are reliable and the system will not introduce vulnerabilities to the ECSU's environment.

**C. TEST DATA**

Test data will be selected carefully, protected, and controlled. The use of production data containing personally identifiable information or confidential/sensitive data for testing must be avoided. If use of confidential/restricted data is required, access controls and other safeguards implemented in production systems must be replicated in the test systems. Additionally:

i. Authorization is required each time production information is copied to a test environment.
ii. Production information must be erased from the test environment immediately after testing is complete.

iii. Copying and the use of production information must be logged to provide an audit trail.

**5. PROCEDURES**

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

**7. EXCLUSIONS / EXCEPTIONS**

No approved exceptions exist at this time.