ELIZABETH CITY STATE UNIVERSITY
Change Management Policy

1. PURPOSE

The purpose of this policy is to define the requirements for managing changes to any Elizabeth City State University's (ECSU) production network and information systems or information resources 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, volunteers, as well as to all other members of the ECSU campus community.

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 the 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.

Change. Any significant modification to production information processing systems and infrastructure that is a result of:

- An upgrade or implementation of new configuration, functionality, features;
- An interruption of service for maintenance;
- A repair of existing configuration, functionality, features; and
- A removal of existing configuration, functionality, features.

Planned or Scheduled Change. A modification to the information processing systems or infrastructure where formal notification is submitted, reviewed, and approved in advance of the change being made.

Emergency Change. A modification to production information processing systems and infrastructure where formal notification was not submitted, reviewed, and approved in advance of the change being made. Emergency changes may be implemented for break/fix situations to maintain system integrity and security in a timely manner.

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.

Principle of Least Privilege. This principle states a process will be granted only those privileges which are essential to perform its intended function.

4. POLICY

A. CHANGE CONTROL

i. Configuration Change Control

ECSU Division of Information Technology (DIT):

a. Determines the types of changes to production information processing systems and infrastructure that are configuration-controlled;
b. Applies configuration-controlled changes to production systems and infrastructure with explicit consideration for risk and security impact analyses;
c. Notifies affected stakeholders, Test, validate and document changes to production information systems and infrastructure prior implementing the changes;
d. Documents configuration-controlled changes to production systems and infrastructure;
e. Retains and review records of configuration-controlled changes to systems;
f. Maintains an audit trail of activities associated with configuration-controlled changes to systems; and
g. Coordinates and provides oversight and approval for configuration change activities through the Change Control Committee that convenes on a routine basis.

B. AUTHORIZATION AND REVIEW

i. **Production Operating System Changes –** All extensions, modifications, or replacements to production operating system software will follow the Change Management Process and changes categorized as “High Risk” will be made only if a written approval is obtained from the Change Control Committee.

ii. **Change Approval** – All changes to ECSU production information systems and network will follow the Change Management Process.

iii. **Change Review - Security Considerations** - Prior to cut-over, every non-emergency change to production systems must be shown to be consistent with the information security architecture, standards and approved by management as part of the formal change control process.

C. CHANGE PROCEDURES

i. **Change Control Procedure** - All non-emergency changes to production Information systems and infrastructure employ a formal change control procedure to authorize all significant changes to software, hardware, communications networks, and related procedures. The procedure supports both scheduled (regular) changes as well as unscheduled (emergency) changes.

ii. **Production Change Personnel** - ECSU production information systems and infrastructure are changed only by authorized staff according to established procedures.

iii. **Change Risk and Impact Assessment** – A Security Risk and Impact assessment is performed for each non-emergency change to determine the severity level of the production environment if the change was not applied correctly or as intended.

iv. **Back-Out Plan** - Adequate back-out plans, which permit information processing activities to revert to conditions quickly and expediently in effect prior to the most recent change in software, is developed for all changes to production systems software, configuration and application software.

v. **Production Information System Change Implementation** - All non-emergency production information systems changes are communicated to affected parties at least two weeks prior to the change. The cut-over for all non-emergency changes is held until the first weekend of each month.

vi. **Vendor-Provided Systems Software Installation** - Prior to being installed, new or different versions of the operating system and related systems software for multi-user production computers go through the established Change Management Process.

vii. **Emergency Changes** – All emergency changes are retrospectively approved and follow the Change Management Process.

D. CHANGE DOCUMENTATION

i. **Production & BCP/DR Systems Change Documentation** - Documentation reflecting all significant changes to production Information Systems at ECSU is prepared within a week from the time that the change took place. This documentation reflects the change, management approval, and the way in which the change was performed, who tested the changes, who cut-over to the changes, and who authorized the changes. The failover environment for BCP/DR (Business Continuity & Disaster Recovery) Procedures is updated to reflect the changes made in the Production environment.

ii. **Change Log on Every Server** - Every ECSU server will have a change log which details changes to both hardware and software. At a minimum, this log indicates the date of the change, the systems administrator making the change, the server component changed, and an explanation and/or justification for each change.

iii. **Change Log Access** - System access controls are additionally defined so that only authorized persons can make changes to production applications and/or change control logs.

E. RECORDING CHANGES

i. **Change Logging** - The details of all changes to ECSU production information systems, software, hardware and network are logged.

ii. **Change Log Contents** –The Change Management Log contains at least the following attributes:

a. Date of submission

b. Date of change

c. Owner and custodian contact information

d. Nature of the change

e. Individual Performing the change

f. Indication of success or failure

F. CHANGE TESTING

i. **Change Testing - Operational Functionality** - Prior to release to production all non-emergency changes are tested for operational functionality and approved following the Change Management Process.

ii. **Change Testing - Security Configuration** - Prior to release to production all changes are tested for information security configurations.

iii. **Post Change Review/Validation** – All Changes require a post-implementation review after each change to validate changes were applied as intended.

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 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.