ELIZABETH CITY STATE UNIVERSITY
Human Resources Security Policy

1. PURPOSE
The purpose of this policy is to ensure Elizabeth City State University (ECSU) Human Resources (HR) incorporates information security best practices into personnel management to safeguard the confidentiality, integrity, and availability of ECSU information resources accessed, managed, and/or controlled by ECSU.

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.

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.

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.

4. POLICY
A. WORKFORCE SECURITY PRIOR TO EMPLOYMENT
To ensure ECSU's information resources can be appropriately secured, all prospective employees are properly vetted prior to receiving an offer of employment with ECSU. The degree of scrutiny shall vary depending on the involvement of the role with confidential information.

Potential employees undergo background verification checks commensurate with their job duties or those of the agencies they support. Some of those screening methods may include, but are not limited to:

i. Previous employment history verification
ii. Criminal history record check
iii. Personal/professional reference checks

Questions or issues found during the background verification check are resolved to the satisfaction of the ECSU Human Resources department leadership prior to any offer of employment being extended to the candidate.

Potential employees must understand and agree to the security requirements of the position and ECSU prior to starting employment.

B. WORKFORCE SECURITY DURING EMPLOYMENT

All ECSU employees must read and acknowledge the *Acceptable Use of Information Resources Policy* and other ECSU information security policies upon the start of their employment with ECSU. Training and education on the information security policies is conducted/coordinated periodically by ECSU Information Security Officer (ISO). New employees have the opportunity to attend these training sessions.

ECSU defines and explains security responsibilities for the role played by the employee and makes clear the ramifications of failing to comply with ECSU policies. Employees are provided with sufficient training and supporting reference materials and expected to complete this training and properly protect ECSU information resources.

Employees changing roles may need to receive additional security review and training before beginning a new role with more stringent security requirements. Department management and/or Human Resources staff ensure access rights have been revoked/adjusted appropriately when an employee's role has changed.

C. WORKFORCE SECURITY FOR TERMINATED EMPLOYMENT

When an individual's employment with ECSU terminates, ECSU ensures:

i. All access accounts are disabled within twenty-four (24) hours of the termination action.
ii. Exit interviews are conducted, if possible and appropriate.
iii. All ECSU information resource-related property is recovered.
iv. All ECSU owned information the terminated employee was responsible for is identified and accounted for.
v. All ECSU equipment is collected, such as laptops, mobile devices, physical keys, and identification badges.

When possible, separation activities are to be coordinated with The Division of Information Technology (DIT) in advance. If advance coordination is not possible, then

department management and/or Human Resources staff engages DIT immediately to revoke or adjust access rights.

Upon termination of an individual deemed to be "High Risk" to ECSU, HR immediately notifies the Information Security Officer (ISO), and DIT System Administrators to revoke the individual's IDs, privileges, and authorizations without delay.

D. DISCIPLINARY PROCESS

Individuals found to be in violation of policy will face disciplinary action. ECSU considers the severity, impact, and other relevant factors of the violation(s) in determining the extent of discipline. Where a violation of non-compliance of information security policy has occurred, corrective actions and sanctions available to ECSU include, but are not limited to:

i. Restriction or suspension of computer and Network access privileges.
ii. Disciplinary action by their academic division and/or ECSU up to and including termination/expulsion.
iii. Referral to law enforcement authorities for criminal prosecution.
iv. Other legal action, including action to recover civil damages and penalties.

E. CONFIDENTIALITY AGREEMENT

ECSU employees are required to protect ECSU's confidential information in accordance with this and other ECSU policies at all times.

Employees with access to Personal Identifiable Information (PII) and Protected Health Information (PHI) are required to sign a confidentiality agreement.

Confidentiality agreements are reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending, or employees are leaving the organization.

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 are 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.