ELIZABETH CITY STATE UNIVERSITY
Telecommuting Information Security Policy

1. PURPOSE

The purpose of this policy is to define the requirements and responsibilities of ECSU's employees approved for teleworking/telecommuting. This policy establishes minimum guidelines for faculty and staff to protect the confidentiality, integrity, and availability of ECSU (Elizabeth City State University) 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, 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.

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. GENERAL REQUIREMENTS

With the increased availability of broadband access, distributed information systems, and secure connections, telecommuting has become more viable for many organizations and employees. ECSU considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all faculty and staff who work either permanently or only occasionally outside of the ECSU office environment. It applies to users who work from home full time; to users on temporary travel; to users who work from a remote campus location and to any user who connects to the ECSU network from a remote location.

While there are a number of advantages presented by telecommuting, it also presents some security risks and challenges that need to be properly addressed. Telecommuting workers are required to follow all ECSU, security, confidentiality, Human Resources, or other policies that are applicable to faculty and staff that work in an ECSU office facility.

B. REQUIRED EQUIPMENT

ECSU faculty and staff who telecommute must have the appropriate equipment. Where appropriate, ECSU will provide a desktop or laptop computer to be used for remotely conducting ECSU business. Faculty and staff should use this device for work activities in accordance with other provisions detailed in ECSU information security policy.

Faculty and staff who telecommute full time or frequently must establish an appropriate work environment that provides appropriate protection for ECSU hardware, electronic information, and printed or hard-copy information. Faculty and staff should also have access to a secure portal or location of documents containing confidential information. Telecommuting employees may also be provided with other equipment depending on the circumstance. Faculty and staff must ensure that their telecommuting systems comply with all ECSU policies and security requirements for remote access and data protection.

C. SECURITY PROTECTIONS FOR HARDWARE

Appropriate security protections must be established and implemented for ECSU hardware not residing in an ECSU office location.

Telecommuting faculty and staff must ensure that ECSU computers are appropriately secured. Faculty and staff are responsible for ensuring their home office offers appropriate security protection for ECSU computing assets.

D. DATA SECURITY PROTECTION

ECSU has established procedures to ensure that data is backed up in a secure manner. Telecommuting employees should work with the IT Services group to ensure their data is backed up according to established procedures.

Wireless networks offer many benefits and conveniences, but they can also present risks that must be considered and addressed. Telecommuters must take steps to ensure that their home wireless networks are properly secured before using them for work purposes. These wireless networks must be encrypted and ensure that only authorized devices can connect to the network.

Employees must use special care when using public wireless networks (e.g., airports, hotels, coffee shops). These networks are usually open, and the connections are not encrypted. They often attract hackers that eavesdrop on network communications. Faculty and staff must always connect to the ECSU`s Virtual Private Network when using public wireless networks to ensure that their connection is secure and protected.

Do not leave paper records containing confidential information out in your work area. Lock all confidential paper records in a file cabinet or secure office at night or when you leave your work area.

Take extra precautions performing tasks which require the use of confidential information when you are in a public area (e.g., airports, airplanes, hotel lobbies). Computer screens can easily be viewed from beside or behind you.

E. DISPOSAL OF PAPER AND / OR ELECTRONIC MEDIA

All papers containing confidential information that is no longer needed must be securely shredded before being disposed of. Do not place these papers in a trash container without first securely shredding. Employees that routinely work from home or from other non-ECSU work environments MUST securely dispose of confidential information in accordance with ECSU Policy.

All external media must be sanitized or destroyed in accordance with the ECSU Media Destruction policy.

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.