FAYETTEVILLE STATE UNIVERSITY

TELECOMMUTING/TELEWORKING SECURITY

Authority:	Issued by the Chancellor. Changes or exceptions to administrative policies issued by the Chancellor may only be made by the Chancellor.
Category:	Information Technology
Applies to:	●Administrators ●Faculty ●Staff
History:	Issued – October 26, 2021
Related Policies/ Regulations/Statutes:	●Information Classification and Handling
Contact for Info:	Deputy Chief Information Officer (910) 672-1958

I. PURPOSE

The purpose of this policy (Policy) is to outline the standards that teleworking/telecommuting employees must adhere to in order to protect the confidentiality, integrity, and availability of Fayetteville State University (University) information resources that are accessed, managed, and/or controlled by the University and its employees. In addition to following the requirements outlined in this Policy, teleworking/telecommuting employees are required to follow all University security, confidentiality, HR, or other policies that are applicable to employees who work in a physical University office/facility.

This policy is applicable to University employees who have been approved for teleworking/telecommuting. Such employees include, but are not limited to the following:

- employees who work either permanently or occasionally outside of a University office environment or facility
- employees on temporary travel;
- employees who work from a remote campus location; or
- employees who connect to the University network from a remote location.

II. DEFINITIONS

The following definitions apply to terms used in this Policy:

- **Availability** shall mean degree to which information and critical University services are accessible for use when required.

- **Confidentiality** shall mean the degree to which confidential University information is protected from unauthorized disclosure.

- **Information Resource** shall mean data, information, and information systems used by

University to conduct University operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

- **Integrity** shall mean the degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of University.

III. UNIVERSITY OWNED EQUIPMENT

In certain circumstances, the University may provide equipment to an employee to allow the employee to remotely conduct University business. Employees shall use such equipment for work activities only and in accordance with this and other University policies related to such usage.

Employees are responsible for ensuring their remote location offers appropriate protection for University owned equipment and such is appropriately isolated and protected from third-parties. Thus, University employees must ensure that laptops are not left unattended in cars or public locations, locked screens are invoked when leaving a computer unattended and cable locks are used when appropriate.

Employees who utilize their personal computer systems must ensure such systems comply with all University policies and security requirements for remote access and data protection.

IV. DATA SECURITY PROTECTIONS

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

Employees should take steps to ensure that their remote wireless networks are properly secured before using those networks for University-related purposes. The wireless networks should be encrypted and only authorized devices should be able to connect to the network.

Employees should use special care when using public wireless networks (airports, hotels, coffee shops, etc.). These networks are usually open, and the connections are not encrypted attracting attackers who may eavesdrop on the network communications. Thus, employees should connect to the University’s VPN when using public wireless networks to ensure that the connection is secure and protected.

V. COMPLIANCE / ENFORCEMENT / SANCTIONS

University employees found to have violated this Policy may be subject to disciplinary action. In addition, violators may be subject to criminal and/or civil action.