FAYETTEVILLE STATE UNIVERSITY

REMOTE WORK 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: Revised – May 17, 2024 (Technical Changes)
Revised – February 2, 2024
Issued – October 26, 2021

Related Policies/ Regulations/Statutes: ●Information Classification and Handling

Contact for Info: Vice Chancellor for IT and Chief Information Officer (910) 672-1958

I. PURPOSE

The purpose of this policy (Policy) is to outline the standards that remote employees must adhere 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, remote work 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 remote. work. 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 or University owned information technology services from a remote location.

II. UNIVERSITY OWNED EQUIPMENT

Based on University need, 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. Thus, University employees must ensure that University issued equipment is 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 should not utilize their personal computers to conduct University business, to ensure compliance with all University policies and security requirements for remote access and data protection.

III. DATA SECURITY PROTECTIONS

The University has established procedures to ensure that data is backed up in a secure manner. Employees who are approved for remote work should work with the Division of Information Technology Services 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 to avoid using public wireless networks (airports, hotels, coffee shops, etc.). These networks are usually open, and the connections are not always encrypted attracting attackers who may eavesdrop on the network communications.

IV. 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.