FAYETTEVILLE STATE UNIVERSITY

DEVICE ENCRYPTION

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 ●Students
History:	March 23, 2022
Related Policies/ Regulations/Statutes:	● Information Classification and Handling
Contact for Info:	Chief Information Officer and Vice Chancellor for Information Technology (910) 672-1200

I. PURPOSE

The purpose of this policy (Policy) is to establish guidelines for the use of encryption to ensure the confidentiality and integrity of Fayetteville State University (University) sensitive data in transit on a network or stored on mobile devices or removable media. Encrypting data in transit protects the confidentiality of the data from accidental or malicious disclosure. Encrypting mobile devices (e.g., laptops) and removable media (e.g., USB thumb drives) protects the data in the event the device is lost or stolen.

II. SCOPE

A. The Policy applies to all University employees, as well as any individuals who are not University employees but have access to University data, to include, but not be limited to retired or emeritus staff and faculty, contractors and volunteers, and any student handling University information.

B. This Policy applies to all University-owned and personally owned, desktop and portable computing devices storing University-managed data to include the following:

- mobile computing and storage devices used by University constituents in the performance of their duties.
- all sensitive data when accessed through, or stored on, mobile computing and storage devices, regardless of the device's ownership; and
- all access, storage, processing, or transmission of sensitive University data, including:

    - transfer of information between users using electronic communication systems (e.g., email, instant message).

- access, storage, processing, or transmission of information using mobile devices (e.g., laptops, tablets, mobile phones) or removable media (e.g., USB drive or CD/DVD).

III. DEFINITIONS

The following definitions are used in this Policy:

- **Encryption:** A process by which data is transformed into a format that renders it unreadable without access to the encryption key and knowledge of the process used.

- **Encryption key**: A password, file or piece of hardware that is required to encrypt and decrypt information – essentially "locking" and "unlocking" the information.

- **Desktop computing device**: Any end user computing device that is not readily portable and is capable of processing and storing Fayetteville State University-managed electronic data.
  - **Examples**: desktop computer, shared lab workstation, computer kiosk.

- **Portable computing device**: Any readily portable computing device capable of processing and storing Fayetteville State University-managed electronic data.
  - **Examples**: laptop computer, smart phone, personal digital assistant

- **Portable data-storage device**: Any readily portable device or storage medium capable of storing Fayetteville State University managed electronic data.
  - **Examples**: laptop computer, smart phone, personal digital assistant (PDA), USB drive, CD-R or DVD-R.

- **Transient Data:** Data of any classification that may temporarily exist on a computing or data storage device for a limited amount of time (e.g., print spool files, website content cached by the browser, temporary files created while editing documents) but does not persist beyond a system power off or reboot.

- **Whole Disk Encryption:** Encryption process in which the entire hard disk (or storage device) is encrypted thereby protecting all the data on the storage device.

IV. PROTECTION OF INFORMATION RESOURCES

A. <u>Required and Recommended Situations</u>

1. Portable Computing Devices

All portable computing devices must employ whole disk encryption, as defined in this policy, to protect this data.

2. Desktop Computing Device Encryption

All desktop computing devices must employ whole disk encryption, as defined in this policy, to protect this data.

B. Transient Data Exception

Portable computing devices and desktop computing devices that contain confidential or restricted information solely in transient data files (i.e., files that do not remain on the computing device after a system power down or reboot) are not required to employ whole disk encryption to protect the information. However, whole disk encryption is still recommended in these situations.

C. Encryption Implementation Standard

1. Only whole disk encryption solutions approved by the Chief Information Officer (CIO) and/or Chief Information Security Officer (CISO) may be utilized to satisfy the requirements of this policy.

2. The entire disk, or all user-writable local disk volumes, will be encrypted.

3. The whole disk encryption solution will centrally manage whole disk encryption client software for all systems, including encryption format, key management, and logging.

4. Fayetteville State University will centrally maintain copies of encryption keys and encryption audit logs.

5. Fayetteville State University retains the right to decrypt data using the centrally maintained key as required, using the employee data access approval process.

D. Deployment Responsibilities

It is the responsibility of Information Technology Services (ITS) to ensure that systems requiring encryption is identified, and that encryption is properly deployed on these systems.

E. End User Responsibilities

1. Users must report any known, unencrypted restricted data on portable computing devices ITS support staff and request assistance in removing the data or acquiring encryption software.

2. Users must not attempt to disable, remove, or otherwise tamper with the encryption software.

V. PROCEDURES

The CIO and CISO shall develop, manage, and review operating procedures to create the proper security posture for protecting university information resources. Such procedures shall be periodically reviewed as required.