# FAYETTEVILLE STATE UNIVERSITY

## END USER INFORMATION 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:** | ●*Acceptable Use*<br>●*Information Classification and Handling* |
| **Contact for Info:** | Deputy Chief Information Officer (910) 672-1958 |

---

## I. PURPOSE

The purpose of this policy (Policy) is to ensure the protection of Fayetteville State University (University) information resources from accidental or intentional damage or loss of data, interruption of University business, or the compromise of sensitive information. This Policy establishes minimum guidelines for End Users to protect the confidentiality, integrity, and availability of University information resources accessed, managed, and/or controlled by the University.

## II. DEFINITIONS

The following definitions are used in this Policy:

- **Availability** shall mean degree to which information and critical College services are accessible for use when required.
- **Confidentiality** shall mean the degree to which confidential University information is protected from unauthorized disclosure.
- **End User or User** shall mean University students, employees (permanent or temporary), contractors and consultants.
- **End User Device** shall mean a device used by End User to accomplish access to information technology resources, including PCs, laptops, tablets, or smartphones.
- **Information Resource** shall mean data, information, and information systems used by the 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.

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

- **Security Incident** shall mean an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information system operation; or violation of information security policy.

## III. PROTECTION OF INFORMATION RESOURCES

Members of the University community have a responsibility to protect the confidentiality, integrity, and availability of the University's information resources. To protect University information resources, End Users are expected to follow the guidelines provided in this Policy, the rules and responsibilities for acceptable use defined in the University's *Acceptable Use* policy, and to exercise good judgment in the protection of University information resources.

### A. End User Devices

End Users shall protect devices in their possession by the following means:

- Using strong passwords.
- Logging off, locking, or shutting down devices before leaving the devises unattended.
- Enabling a password protected auto-lock or automatic screensaver to activate after no more than 15 minutes of inactivity.
- Securing portable and mobile devices at all times by locking the devices or ensuring the device is in the End User's possession.
- Locking the device in a secure location (e.g. drawer, cabinet, office, room, trunk) if away for an extended period of time.

### B. Passwords

Passwords are confidential University information and End Users shall abide by the following guidelines to protect devices utilizing passwords.

- Passwords shall not be shared.
- Long passwords should be used.
- The following should not be used as passwords:
    - Words that refer to personal data (i.e. children's names or your birth date).
    - Dictionary words .
    - Short words.
- Passwords should not be revealed on questionnaires or security forms.
- The "Remember Password" feature in Windows or applications (e.g. Internet Explorer, Outlook, Firefox, Google Chrome, etc.) should not be used.
- Passwords should not be written down and stored where accessible by others.
- Passwords should not be input while individuals are watching.
- Passwords should be changed immediately if inadvertently compromised.

### C. Virus and Malware Protection

End Users should protect University information resources utilize virus and malware protections as follows:

- Employ anti-virus software and update on a regular basis.
- Do not open unexpected or suspicious attachments received in an email.
- Scan removable or portable media for viruses prior to using on any machine connected to the University's network. Examples of removable or portable media devices include laptops, USB memory sticks, external Hard Disk Drives, CDs, DVDs, Compact Flash or SD memory cards and magnetic tapes,.

### D. Distribution and Transmission of Information

Sensitive FSU information that is transmitted electronically, transported physically, or spoken in conversation must be appropriately protected from unauthorized interception. The University's *Information Classification and Handling* policy includes specific requirements on the handling of University information.

### E. Destruction and Disposal of Information and Devices

Sensitive University information must be securely disposed of to ensure it cannot be retrieved and recovered by unauthorized persons. The University's *Information Classification and Handling* policy provides information on the proper destruction and disposal of information and devices.

### F. Incident Reporting

All members of the University community are required to report suspected or actual information security incidents or security breaches. These incidents include thefts of computer devices, viruses, worms, or computer "attacks" that may lead to unauthorized access to confidential information.

Information security incidents should be reported to:

- Information Security Office / Officer - InfoSec@uncfsu.edu
- IT Services Help Desk, (910) 672-4357 – www.uncfsu.edu/help
- A University manager or supervisor.

## IV. PROCEDURES

The CIO and ISO 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.

## V. 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.