FAYETTEVILLE STATE UNIVERSITY

PHYSICAL AND ENVIRONMENTAL 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 – March 27, 2024 (Technical Corrections)
Issued – October 26, 2021

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

Contact for Info: Vice Chancellor for Information Technology and Chief Information Officer | (910) 672-1200

I. PURPOSE

The purpose of this policy (Policy) is to define requirements for protecting Fayetteville State University (University) information resources from physical and environmental threat. This Policy establishes minimum guidelines 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.

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

- **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.

III. THREATS AND SECURITY

A. Physical Security Threats

Employees and students who encounter a threat to their safety or well-being should immediately do one or more of the following:

- Move to a secure location.
- If on-campus, report the issue to the University's Police and Public Safety Department at extension 1911.
- If off-campus, report the issue to 911 emergency services.

B. Secure Areas

In addition to implementing technical controls to ensure the security and safety of University information resources, controlling physical access to areas that house information resources is critical to ensuring those resources are properly secured. University employees must protect physical areas under their control in a manner consistent with the sensitivity of the information resources located in that area. This Policy applies to any information resource, regardless of the format (hard copy, electronic copy, laptop, server, network infrastructure, etc.).

It is the responsibility of all University employees and students to take positive action to ensure physical security. All visitors to restricted University facilities must be escorted by University employees while visiting a restricted location. Unrecognized and unescorted persons in a restricted location should be asked for their identification and the name of their University contact, reported to a University employee or reported to the Police and Public Safety Department.

Physical access rights must be removed immediately for University employees upon termination of their employment. These rights must also be modified accordingly when an employee changes roles within the University. Temporary access may be granted to employees, contractors, or vendors when required for special circumstances. These temporary access rights must be properly revoked when the special circumstance has concluded.

All University employees and students are responsible for understanding the appropriate access restrictions and guidelines for secure areas they access, and are responsible for complying with these restrictions and guidelines to ensure these areas are appropriately secured.

C. Equipment Security

The University will take reasonable action to protect University equipment, including cabling, from physical and environmental threats, and unauthorized access. Equipment requiring special protection must be isolated or employ special physical protections according to need as defined in the University Data Classification and Handling Policy. Equipment must be reasonably appropriately protected from power failures and surges as well as from heat, cold, and moisture.

When equipment has been damaged or has reached the end of its useful life, it must be disposed of securely, according to University guidelines and procedures for asset disposal as defined in the University Data Classification and Handling Policy.

D. Facility Physical Security

University data centers, server rooms, and network routing facilities house servers and network equipment that process sensitive information and control access to the University network. Physical access to these assets must be tightly controlled in order to protect this equipment and the information they process.

All University data centers, server rooms, and network routing facilities must operate a physical security program to protect the safety and security of the University community and the information resources in these facilities. Precautions should be taken to ensure proper environment alarms and backup systems are available to ensure critical components remain online.

E. Video Surveillance and Access to Video Footage

The University maintains a system of cameras and video recording tools that provide video surveillance of University facilities. Cameras are placed in strategic locations throughout University facilities to monitor and record activity of interest.

University departments and individuals may request access to information gathered, processed, and archived through electronic security systems (video footage or access logs) to aid in the investigation of security incidents. All such requests must be made in writing to the University's Chief Information Officer (CIO). The request must be reviewed and approved by the following:

- CIO
- Information Security Office/Officer (ISO) (or designee)
- Campus Safety
- General Counsel

Once the request has been approved, the requestor will be allowed to access any available video footage or access logs pertaining to the incident investigation. The review of video footage and/or access logs (paper or electronic copies) must be performed on-site at University facilities and under the supervision of University Information Technology Services (IT Services) staff. As a rule, requestors will not be permitted to retain copies of video footage or access logs, although special requests for copies of video footage and/or access logs may be considered on a case-by-case basis.