FAYETTEVILLE STATE UNIVERSITY

INFORMATION SECURITY RELATED TO UNIVERSITY PERSONNEL

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* ●*Employment Background and Reference Checks*

Contact for Info: Deputy Chief Information Officer (910) 672-1958

I. PURPOSE

The purpose of this policy (Policy) is to ensure coordination between the Office of Information Technology and the Office of Human Resources (HR) as such pertains to information security at Fayetteville State University's (University).

II. DEFINITIONS

The following definitions are used in this Policy:

- **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.

- **Information Systems.** shall mean a hardware or virtual computing environment that is installed or configured to collect, process, store, or transmit information for multiple users or, that communicates with other systems to transmit data or process transactions.

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

- **Risk** shall mean the probability or threat of damage, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action.

III. APPLICANTS FOR EMPLOYMENT

In accordance with its *Background and Reference Check* policy, the University conducts background checks on applicants who are selected as the final candidate for employment to a full-time and/or part-time position.

IV. TRAINING OF EMPLOYEES

University employees are required to become familiar with the University's *Acceptable Use* policy and other information security policies. Training on such policies is the responsibility of the University's Information Security Office/Officer (ISO). The ISO will define and explain employees' security responsibilities and the consequences for failing to comply.

V. ENDING OF EMPLOYMENT

To the extent possible, the Office of Human Resource (HR) will coordinate with Information Technology Services (ITS) when an individual's employment with the University has ended. If advance coordination is not possible, the employee's supervisor and/or HR must contact ITS immediately to revoke or adjust access rights. If the individual whose employment has ended is deemed to be high risk, HR shall be required to immediately inform the ISO and ITS .

When notice of an individual's employment ending is provided ITS, ITS shall ensure the following:

- Access accounts are disabled within twenty-four (24) hours of the notice of termination.
- Information resource-related property is recovered.
- Information the terminated employee was responsible for is identified and accounted for.

The Office of Human Resources or the employee's supervisor shall ensure that University owned-equipment (laptops, keys, badges) is collected.