FAYETTEVILLE
STATE UNIVERSITY

Compliance Alerts!
November 2021: Information Security Safeguards

All University-owned or managed systems and data are property of the University. The security of these systems and data must be maintained according to University policies, procedures, and standards, and all applicable laws and regulations. University faculty, students, staff, temporary employees, contractors, outside vendors and visitors to campus (“Users”) must adhere to these requirements.

- Sensitive Information must always be protected against possible unauthorized access.
- The transmission of Sensitive Information must be done with the utmost attention to protecting the privacy of the information.
- Sensitive Information must not be stored on mobile devices or disposable media devices except in accordance with the Information Security Standards.
- All computing devices must be physically secured, password-protected, and encrypted, if required by the Information Security Standards.
- When verbally communicating Sensitive Information to other authorized personnel, individuals must be aware of their surroundings to prevent unauthorized disclosure of Sensitive Information.
- The destruction of Sensitive Information must be in accordance with the University record retention schedules and consistent with the standards defined in the Records Retention and Disposition Schedule.
- Any department intending to surplus devices that process or store electronic information, such as computers, servers, smartphones/PDAs, and certain copiers, must first destroy the electronic information by wiping, then keep the devices physically secure until the devices are in the possession of University Surplus personnel.
- Sensitive Information must not be copied, printed, or stored in a manner that would leave it vulnerable to unauthorized access.
- Sensitive Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the University network.
- Physical and electronic access to Sensitive Information and computing resources must be controlled.
- Computing Devices that contain or have access to Sensitive Information, including any mobile devices, must be secured against use, including viewing, by unauthorized individuals.

For more detailed information, please consult the following documents.

- Acceptable Use of Information Resources
- Business Continuity and Disaster Recovery
- End User Information Security
- Information Security Related to University Personnel
- Information Systems Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Systems Operations Security
- Network Management Security
- Information Security Standards
- Policy on Identity Theft Compliance (Red Flag Rules)

Please contact ITS if you have any questions about these requirements.

To keep the community informed, all **Compliance Alerts!** are maintained on the University's Compliance and Enterprise Risk Management webpage. Compliance Alerts (uncfsu.edu)