

**Athens State University
Data/Information Protection and Confidentiality
Employee Agreement**

Pursuant to the *Information Security* Program policy, Athens State University employees (faculty, staff, and student workers) are responsible for protecting access to all data/information managed and stored on Athens State University computer and technological systems hosted on and off premises. This requirement is also applicable to all third-party contractors whose work allows them to have access to such data/information. Each employee/applicable contractor contributes to this effort by continuously reviewing and practicing the following:

1. **Maintain the safe keeping of all assigned accounts and password credentials** to university computer systems used by university employees/applicable contractors. Assigned accounts are to only be used in the performance of duties as a university employee/applicable contractor.
2. **Comply with all rules and controls** established for the use of digital and paper records maintained on or in conjunction with all information systems described in item 1 of this agreement.
3. **Practice safe computing at all times.** Think before you click, be aware of the latest online threats; do not respond to e-mail requests for personal information about yourself or others; verify that websites are legitimate and secure, and use complex passwords for all accounts.
4. **Avoid disclosure of personal and confidential information** to unauthorized persons in accordance with the federal Family Educational Rights and Privacy Act. <https://www.athens.edu/pdfs/policies/Operating/Academics/Privacy-of-Student-Records-FERPA.pdf>
5. **Exercise care to protect personal and confidential information** against accidental or unauthorized access, modifications, disclosures, or destruction. Ensure sensitive and confidential information is kept private and managed only by those individuals authorized to have access to it.
6. **Notify your supervisor and the Help Desk immediately if system security is compromised or a data breach has occurred,** whether inadvertent or intentional, that allows an unauthorized release of University data/information to internal or external parties.
7. **Read all Information Technology Policies** published at: <https://www.athens.edu/about/governance-policies/policies/information-technology/>
8. **Understand that undisclosed violations of this policy can cause serious harm to individuals and the university.** The open and honest reporting of violations is essential to improve processes and share knowledge about preserving the confidentiality, integrity, and access to data and systems.
9. **Complete the assigned annual *Data Security Awareness Training*.**

As an employee or applicable contractor of Athens State University, I acknowledge that I have read, understood, and will follow the requirements of this agreement and all referenced university policies. I understand that I should ask questions and raise concerns about anything I observe that could impact the integrity, confidentiality, and access to university data and information during my employment.

Name: _____

Department Name: _____

Signature: _____

Date: _____