

**Athens State University**  
**Data/Information Protection and Confidentiality**  
**Vendor Agreement**  
**(When Applicable)**

Pursuant to the *Information Security Program* policy, third-party vendors that have access to sensitive information on behalf of Athens State University must be assessed for their security practices and compliance with GLBA requirements prior to engaging services. The University will take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for information and require the service provider, by contract, to implement and maintain such safeguards.

Each applicable vendor/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 applicable vendors/contractors. Assigned accounts are to only be used in the performance of duties.
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.
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/org/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 the University 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. **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.

As an applicable vendor/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 the contractual agreement. I further understand and agree that if I violate or do not follow the above requirements, that the same shall be treated as a breach of my contract and/or the terms of my vendor relationship with the university, which will permit the university to limit or remove my access to university data/information, to suspend or terminate my contract and/or vendor relationship, or to obtain such other remedies as are permitted by law.

Name: \_\_\_\_\_

Company/Contractor Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_