Policy Number: VI.07
Policy Level: Operating Policy
Originally Issued: October 10, 2023
Revised: November 18, 2024
Policy Owner: President
Policy Implementation: Chief Information Officer and Information Security Officer

# Information Security Program

## I. Policy Statement

Athens State University is committed to protecting the confidentiality, integrity, and availability of its information assets as required by *University's Information Systems Security Policy* established by the Athens State University Board of Trustees. This policy is also established for compliance with the Gramm-Leach-Bliley Act (GLBA) (16 CFR 314.4) and other regulatory requirements. This policy establishes the Information Security Program that will include the framework for safeguarding sensitive information and complying with GLBA requirements within the university environment.

## II. Scope

This policy applies to all faculty, staff, students, contractors, and third-party vendors who manage, access, or process sensitive information on behalf of Athens State University.

## III. Definitions

Sensitive Information: Any non-public personal information obtained by Athens State University in the course of providing financial services, including but not limited to social security numbers, financial account numbers, credit card information, and other personally identifiable information.

Employment Separation/Termination of Services: Any change from active employment status to inactive employment or end of contracted services with the University

## IV. Information Security Controls

### Access Control

User Accounts: Access to sensitive information will be granted based on the principle of least privilege and password protected in accordance with the *Athens State University Password Management Policy*. User accounts must be unique, properly authorized, and regularly reviewed for appropriateness. A formal written request will be required to access systems that manage and house sensitive data.

User Termination: Access to sensitive information will be promptly revoked for terminated employees, students, and contractors.

## Data Protection

Data Classification: Sensitive information shall be classified according to its level of sensitivity and handled accordingly in accordance with the Athens State University *Data Governance policy*. Proper controls, such as encryption and data anonymization, should be applied to protect sensitive data throughout its lifecycle.

Data Transmission: Sensitive information transmitted over public networks must be encrypted using approved encryption mechanisms.

Data Storage: Sensitive information stored electronically or in physical form should be adequately protected using appropriate security controls, including access controls and encryption.

## Security Awareness and Training

Regular Training: All employees, including student employees, will receive annual training on information security policies, procedures, and best practices and will be required to sign the *Data/Information Protection and Confidentiality Agreement*. This training is intended to help reduce the risks of ransomware, data theft, or unauthorized access to systems and data.

Phishing Awareness: Individuals will be trained to recognize and report phishing attempts or suspicious activities to the appropriate authorities.

The University will utilize qualified information security personnel sufficient to manage its information security risks and to perform/oversee its information security program. The University will provide those personnel with security updates and training sufficient to address relevant security risks and verify that key personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

## Incident Response

Incident Reporting: Any suspected or actual security incidents involving sensitive information must be promptly addressed in accordance with the *Incident Response/Recovery and Data Backup* policy.

**Risk Assessment, Evaluation and Adjustment**

The Chief Information Officer will conduct a risk assessment at the University to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of sensitive information, and assess the sufficiency of any safeguards in place to control these risks. The risk assessment shall meet the criteria set forth in 16 CFR §314.4. Additional risk assessments shall be conducted on a periodic basis.

Based on the results of the assessment, the University will make adjustments to the Information Security Program to ensure continued security.

**Minimum Safeguards**

The University will design and implement safeguards to control the risks identified through risk assessment by:

- Implementing and periodically reviewing access controls, including technical and physical controls.
- Identifying and managing the data, personnel, devices, systems and facilities that enable the achievement of business purposes.
- Protecting by encrypting all sensitive information held or transmitted both in transit over external networks and at rest.
- Adopting secure development practices for in-house developed applications for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications.
- Implementing multi-factor authentication of any individual accessing any information system.
- Regularly testing and monitoring the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems; and then adjusting the information security program in light of the results.

### Vendor/Service Providers Management

Third-Party Assessment: 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.

Contractual Obligations: Contracts with third-party vendors should include specific provisions addressing the protection of sensitive information and compliance with applicable data security standards including the requirement to complete the *Data/Information Protection and Confidentiality Agreement*

The Chief Information Officer and the Information Security Officer will periodically assess IT service providers based on the risk they present and the continued adequacy of their safeguards.

## V. Compliance and Monitoring

Compliance Assessment: Periodic assessments and tests will be conducted to monitor the effectiveness of implemented safeguards and to ensure compliance with this policy and GLBA requirements. Non-compliance will be addressed through appropriate disciplinary measures.

Failure to comply with this information security policy may result in disciplinary action, up to and including termination or legal consequences, as applicable.

By adhering to this policy, Athens State University aims to protect the privacy and security of sensitive information and fulfill its obligations under the Gramm-Leach-Bliley Act (16 CFR 314.4).

## VI. Reporting

The Chief Information Officer will provide an annual report to the Board of Trustees on the University's Information Security Program. The report shall discuss the overall status of the

information security program and its compliance with 44 CFR § 314.4. It shall also include material matters related to the information security program, and any recommendations for changes in the program.

## VI. Responsibilities

**Chief Information Officer (CIO)** is responsible for establishing and supporting an effective information security program and ensuring resources are allocated for its implementation.

**Information Security Officer (ISO)** will oversee the implementation and maintenance of the Information Security Program as required for compliance.

**Employees, Students, and Contractors:** All individuals accessing or managing sensitive information must comply with this policy, adhere to security controls, and report any security incidents or concerns.

## VII. Responsibility for this Operating Policy

### Policy Owner

As part of the initial approval of this policy by the President and subsequent to the original dissemination of the policy, the President is the policy owner for the ongoing evaluation, review, and approval of this policy. Subsequent reviews and revisions to this policy must be in accordance with approved operating policy procedures and processes.

This policy will be reviewed every year or more frequently as needed by the Policy Owner. Revisions will be reviewed/affirmed by the Cabinet and approved by the University President. This policy will be updated/published in the University's Policy Library.

### Responsibility for Policy Implementation

The President has assigned the responsibility of implementing this policy to the Chief Information Officer and Information Security Officer.