

Version 1.0

Version Date: 05/08/2023



ALABAMA STATE UNIVERSITY (ASU)

Office of Technology Services (OTS)

Privacy Policy

Contents

Document	3
Annual Review and Revision Tracking	3
Overview	3
Purpose	3
Scope	3
Roles and Responsibilities	4
Policy	4
Health Insurance Portability and Accountability Act Compliance	4
Graham Leach Billey Act Compliance	5
Family Education Rights and Privacy Act Compliance	5
Compliance Mapping Matrix	5
References	5
Responsibility for Policy and Procedures Maintenance	5
Definitions	6
Violation of Policy	6
Disclosure	6

Document

Document	Privacy Policy
References	HIPPA, GLBA, FERPA
Control	
Last Approved	
Next Review	

Annual Review and Revision Tracking

Date	Summary of Changes Made	Changes Made By (Name/title)	Version History

Overview

This Privacy Policy outlines the principles and practices governing the collection, use, disclosure, and protection of personal information in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA) and Payment Card Industry (PCI) compliance. In accordance with mandated organizational security requirements set forth and approved by management, ASU has established a formal Electronic Payment policy.

In accordance with mandated University security requirements set forth and approved by the Board, ASU has established a formal Privacy policy. This policy is to be implemented immediately. Additionally, this policy is to be evaluated on an annual basis for ensuring its adequacy and relevancy regarding ASU's needs and goals.

Purpose

This Privacy Policy describes how ASU OTS collect, use, disclose, and protect the Personal Identifiable Information (PII) of personnel in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA). We are committed to maintaining the privacy and confidentiality of PII entrusted to the University. Additionally, this policy is to be evaluated on an annual basis for ensuring its adequacy and relevancy regarding ASU's needs and goals.

Scope

This policy and supporting procedures encompasses all information systems that are owned, operated, maintained, and controlled by ASU and all other information systems, both internally and externally, that interact with these systems.

- Internal information systems are those owned, operated, maintained, and controlled by ASU and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both

physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other information systems deemed in scope.

- External information systems are those owned, operated, maintained, and controlled by any entity other than ASU, but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal information systems".

Note: While ASU does not have the ability to actually provision, harden, secure, and deploy another organization's information systems, ASU will follow due-diligence and best practices by obtaining all relevant information ensuring that such systems are safe and secure

Roles and Responsibilities

Implementing and adhering to the University's policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, students, and users of information systems, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to ASU information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

- **Management Commitment:** Responsibilities include providing overall direction, guidance, leadership and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The Vice President of Technology Services is to report to other members of Board on a regular basis regarding all aspects of the University's information systems posture.
- **Personnel:** Responsibilities include adhering to the University's information security policies, procedures, practices, and not undertaking any measures to alter such standards on any ASU information systems. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of ASU information systems and are to also report such instance immediately to senior authorities.

Policy

This Privacy Policy applies to all PII (Personal Identifiable Information) collected, used, disclosed, and maintained by the University in the course of providing healthcare services, financial services, and educational services. ASU is to ensure that all applicable community users adhere to the following policies for purposes of complying with the mandated University security requirements set forth and approved by the board. ASU OTS shall:

Health Insurance Portability and Accountability Act Compliance

Comply with HIPAA, which governs the privacy and security of Protected Health Information (PHI). In accordance with HIPAA, ASU OTS shall:

1. Collect and use PHI solely for the purposes permitted under HIPAA, such as treatment, payment, and healthcare operations.
2. Implement appropriate safeguards to protect the confidentiality, integrity, and availability of PHI.

3. Disclose PHI only as authorized by law or as necessary for the provision of healthcare services.

Graham Leach Billey Act Compliance

Comply with GLBA, which regulates the handling of non-public personal information by financial institutions. In compliance with GLBA, ASU OTS shall:

1. Collect and use non-public PII solely for the purpose of providing financial services and related transactions.
2. Restrict access to non-public PII to authorized personnel and maintain safeguards to protect its confidentiality.
3. Limit the disclosure of non-public PII to non-affiliated third parties except as permitted or required by law.

Family Education Rights and Privacy Act Compliance

Comply with FERPA, which safeguards the privacy of student educational records. In accordance with FERPA, ASU OTS shall:

1. Collect and use student educational records only for legitimate educational purposes and in compliance with FERPA.
2. Maintain the confidentiality and security of student educational records to prevent unauthorized access or disclosure.
3. Disclose student educational records in compliance with FERPA, such as for legitimate educational interests, with student consent, or as required by law.

Compliance Mapping Matrix

The following Matrix is to be completed for purposes of cross-referencing and effectively mapping the basic and derived security requirements with existing information security policies and procedures for ASU.

Basic and Derived Security Requirements	Listing of Applicable POLICY and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments

References

Related Regulations, Statutes, Policy and/or STANDARD OPERATING PROCEDURES (SOP) Documentation	Notes and Comments
FTC Safeguard Rules Section 314.4	

Responsibility for Policy and Procedures Maintenance

ASU is responsible for ensuring that the aforementioned policy initiatives, and if applicable – the relevant procedures – are kept current as needed for purposes of compliance with mandated University security requirements set forth and approved by the Board.

Definitions

Personnel – All community users of all information systems that are the property of ASU. Specifically, it includes:

- All faculty, staff and student workers, whether employed on a full-time or part-time basis by ASU.
- All contractors and third parties that work on behalf of and are paid directly by ASU.
- All contractors and third parties that work on behalf of ASU but are paid directly by an alternate employer.
- All employees of partners and clients of ASU that access ASU’s non-public information systems.
- All volunteers and alumni that serve on behalf of ASU.
- All students attending ASU.

Violation of Policy

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

1. First Incident of a minor breach will result in verbal reprimand by the policy owner as outlined in the Personnel Disciplinary Policy found in the ASU Personnel Handbook. If the offender already has a verbal reprimand for the same infraction, the incident will be remanded to Human Resources as outlined below.
2. Multiple minor breaches or a major breach will be remanded to Human Resources and Executive Management for disciplinary action as outlined in the Personnel Disciplinary Policy found in the ASU Personnel Handbook.
3. In the case of a student, the breach will also be remanded to the Dean of Students.

Disclosure

ASU reserves the right to change and modify the aforementioned document at any time and to provide notice to all users in a reasonable and acceptable timeframe and format.

Signature
Name
Title

Date