GLBA Information Security Program

Policy Number:	Responsible Office:	Governing Body:	Last Review Date:
	Human Resources	College Council	07/24/2024
Scope: Any individual or department that has access to Covered Data			

I. Overview

The Federal Trade Commission's Safeguard Rule, which implements the security provision of the Gramm-Leach-Bliley Act (GLBA), went into effect on May 23, 2003. The Safeguard Rule requires financial institutions, which includes colleges that are significantly engaged in providing Financial Services, to protect the security, confidentiality, and integrity of customer financial records, including non-public personally identifiable financial information. To ensure these protections, the GLBA Safeguards Rule mandates that all covered financial institutions establish appropriate administrative, technical and physical safeguards.

Therefore, any Antioch College departments that collect, store or process Covered Data must implement data protection standards in order to ensure compliance. This is in addition to any other College policies and procedures that may be required pursuant to federal and state laws and regulations, including Family Educational Rights and Privacy Acts (FERPA).

II. Purpose

To ensure that individuals and departments that access or utilize Covered Data understand their responsibility with respect to GLBA compliance.

II. Definitions

Customer: is any individual (student, parent, faculty, staff, or other third party with whom the college interacts) who receives a financial service from the college and who, in the course of receiving that service, provides the college with sensitive, non-public, personal information about themselves.

Covered Information: is sensitive, non-public, personally identifiable information includes, but may not be limited to, and individual's name in conjunction with any of the following:

- social security number
- credit card information
- income and credit history
- bank account information
- tax return
- asset statement

Covered Information includes both paper and electronic records.

Principle of least privilege: maintains that system users will be granted access to only those functions and data needed to perform their job duties and no more.

NPI:

III. Policy and Process

GLBA requires that the GLBA Information Security Program include the following elements. College's procedures as they relate to these elements are as follows.

1.Designate Qualified Individual(s):

Designated qualified individuals are responsible for overseeing and implementing the institution's information security program and enforcing the information security program in compliance (16 CFR 314.4(a)).

Antioch College designates the Director of Financial Aid and Assistant Director of Human Resources to serve as qualified individuals, who will administer Antioch College's Information Security Program. Qualified Individuals have ultimate responsibility and accountability for implementing and enforcing the institution's information security program.

In addition, the Director of each department shall designate an Information Security Program coordinator for their department.

2. Identification of Risks and Risk assessments:

Antioch College recognizes that there are both internal and external risks associated with the protection of Covered Data. These risks include, but are not limited to:

- Unauthorized access to Covered Data;
- Compromised system security as a result of system access by an unauthorized person
- Loss of data integrity
- Physical loss of Covered Data in a disaster;
- Errors introduced into the system;
- Unauthorized requests for Covered Data;
- Corruption of data or systems;
- Unauthorized access to hard copy files or reports containing Covered Data;
- Unauthorized transfer or release of Covered Data by third parties contracted by the College;
- Unauthorized disposal of Covered Data; and
- Unsecured disposal of Covered Data.
- Misuse or alteration of Covered Data;
- Unauthorized disclosure of Covered Data;

Antioch College recognizes that the aforementioned may not be a complete list of risks associated with the protection of Covered Data. Possibility of new risks may arise, thus Antioch College data custodians will actively seek to identify and address all potential risks to Covered Data.

Access to the Covered Data related information systems and services is provided on an as-needed basis with the principle of least privilege. Access is requested by the individual's supervisors and approved by the Department Director. Directors are responsible for identifying need for access and an appropriate level of access for each employee.

Antioch College shall incorporate continuous monitoring and identification of security risks and controls into its Annual Risk Assessment/internal control review process.

3. Design and implementation of a Safeguard Program:

a.) Qualified Individuals will perform an annual review to ensure that those with access to Covered Data are still active and that their access levels are appropriate. Role-based authorizations will be applied in adherence to the principle of least privilege. Roles are regularly reviewed and maintained. In addition to this annual review, there is a monthly review of access to verify that those with access remain appropriate.

b.) Departments should provide to the Qualified Individuals, upon request, a written inventory of Covered Data, noting where it is collected, stored, and/or transmitted. An accurate list of all systems, devices, platforms, and personnel that process Covered Data should be maintained by the department and qualified individuals. Inventory items include, but not limited to:

- Keys and key cards
- Computers, tablets and laptops

c.) All databases and imaged documents containing Covered Data must be appropriately protected, including use of passwords or other authentication, encryption and other access restrictions as appropriate.

d.) Access to Covered Data through College networks and stand-alone systems shall be limited to those employees who have a business reason to have such information per IT security procedure requirements. Only employees with the need to have access to certain Covered Data shall be granted access to that data or be authorized to collect such data from Customers.

While the College utilizes industry-standard protocols and cybersecurity technologies, including firewall, intrusion prevention, encryption, anti-malware, email security and restricted physical access to its data, it is every employee's requirement to ensure that reasonable and appropriate steps are taken to protect Covered Data and to safeguard the integrity of records in storage and transmission. These steps include maintain operating systems and applications, applying security-related updates in timely manner after appropriate testing,

All Covered Data shall be handled with care and scrutiny and shall be protected and controlled, including by not limited to storage on College servers. All College information security software and hardware protections shall be maintained with vendor support at current or higher levels. Sensitive data discovery and data loss prevention tools shall be utilized in areas of high risk to ensure that Covered Data is identified and protected as required.

e). Multi-factor authentication: Antioch College has implemented multi-factor authentication for any individual accessing the College's information system.

Multi-factor authentication is defined as authentication through verification of at least two of the following types of authentication factors:

1. Knowledge factors, such as a password

2. Possession factors, such as a token; or

3. Inherence factors, such as biometric characteristics.

Other multi-factor authentications include:

- Phone or text verification
- Out of network log in verifications and alerts
- One time generated codes

f). Access to Covered Data shall be limited to those employees who have a business reason to have such information per IT Security Procedure requirements. Whether this information is stored in hard copy form or electronically, employees must exercise appropriate care for its safekeeping by following these guidelines:

Safeguard Paper Information:

- Secure Covered Data by locking file cabinets and offices when not in use.
- Do not leave Covered Data unattended and unsecured.
- Access to Covered Data shall only be granted to those who need such access.
- Printouts containing Covered Data should be immediately removed from printers/copiers/fax machines.
- Ensure that fax transmissions are monitored and secured as soon as received.

Safeguarding Electronic information:

- Password-protect computers and systems with access to Covered Data, and log off of computers and systems when access to Covered Data is no longer needed. Shut down and turn off computers at the end of each day where possible.
- Do not leave Covered Data unattended and unsecured
- Access to computers and systems shall only be granted to those who need such access.
- Upon termination of employment, all electronic access is promptly removed and passwords discontinued.
- Encrypt Covered Data when transmitting or storing it electronically.
- Monitor systems for actual or attempted attacks, intrusions, or other systems failures.
- Comply with other applicable College Policies and procedures:

Disposal of Records Containing Covered Data

Stored records containing Covered Data shall be maintained only until they become inactive or are no longer required under applicable rules and regulations. When no longer active or required, records shall be destroyed or retired in accordance with Antioch College's Records Retention Schedule governing the disposition of such records. Paper records that are no longer required to be kept by the College shall be shredded at the time of disposal. Electronic documents shall be deleted.

g.) Department heads and College personnel who handle or are involved in the management of Covered Data must continually assess the vulnerabilities of their electronic as well as paper-based systems. Information Technology and Qualified Individuals are available to assist in assessing the efficacy of existing safeguards and to propose improvements if needed.

h.) Qualified Individuals will maintain a log of authorized users and will review access levels for accuracy monthly.

4. Testing and Monitoring

The IT department periodically conducts tests and vulnerability assessments on its network and key information systems. These measures are designed to test and monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusion into, Antioch College's information systems.

5. Employee training and Management

All Antioch College employees in departments that collect, access, retain, transmit or dispose of Covered Data will receive a copy of this Information Security Program. Each department's designated Information security program coordinator is responsible for ensuring that all employees in their department receive this document and for clarifying how the information security program is applicable to the employees in their department. Qualified Individuals shall ensure that each designated information security coordinator is aware of this responsibility.

References and/or background checks (as appropriate, depending on position) of new employees working in areas that regularly work with covered data and information are checked/performed. During employee orientation, each new employee in these departments receives proper training on the importance of confidentiality of student records, student financial information, and all other covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual, as well as how to properly dispose of documents that contain covered data and information. These training efforts should help minimize risk and safeguard covered data and information.

All employees are required to complete annual training in cybersecurity and FERPA to ensure compliance. Cybersecurity awareness training also includes controls and procedures to detect and identify ransomware, phishing and social engineering tactics to prevent employees from providing Covered Data to an unauthorized individual.

Qualified Individuals will arrange annual training of the various groups impacted by the GLBA Safeguards Rule

6. Oversight of Service Providers and Contracts

GLBA requires Antioch College to take reasonable steps to select and retain services providers who maintain appropriate safeguards for covered data and information. Vendors who will have access to covered data must undergo a security risk assessment to identify and document risks associated with

them transmitting and/or storing covered data. Appropriate data security provisions are included in contracts with such vendors.

7. Evaluation and Adjustment

Department heads and College personnel who handle or are involved in the management of Covered Data must continually assess the vulnerabilities of their electronic as well as paper-based systems. Information Technology and Qualified Individuals are available to assist in assessing the efficacy of existing safeguards and to propose improvements if needed.

Risk assessment activities will be periodically performed to reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and to reassess the sufficiency of any safeguards in place to control these risks.