UnitekLEARNING

# POLICIES AND PROCEDURES

| | |
|---|---|
| **Policy Name:** | Gramm-Leach-Bliley Act (GLBA) Information Security |
| **Policy Number:** | IT 3.0 |
| **Effective Date:** | January 1, 2020 |
| **Revision Date:** | January 1, 2021; June 8, 2022 |
| **Applies To:** | All students, staff, employees and instructors of Unitek Learning |
| **References:** | None |

## 1. PURPOSE

It is the position of the company to provide safeguards to protect information and data in accordance with the Financial Services Modernization Act of 1999, also known as the Gramm Leach-Bliley Act (GLBA). Therefore, in compliance with the GLBA, Unitek Learning ensures the following:

- Any department that stores or processes customer financial information ("covered data") must implement data protection standards in order to ensure compliance;
- Individuals or departments that access or utilize covered data understand their responsibility with respect to complying with the GLBA;
- Identification of the corresponding Unitek standards that are to be implemented by owners and/or custodians of GLBA data.

## 2. SCOPE

These policies and procedures apply to all employees of Untek Learning.

## 3. DEFINITIONS

"Covered data" means all information required to be protected under the Gramm-Leach-Bliley Act. "Covered data" also refers to financial information that the Institution, as a matter of policy, has included within the scope of the GLBA Information Security Program. Covered data includes information obtained from a student in the course of offering a financial product or service, or such information provided to the Institution from another institution. "Offering a financial product or service" includes offering student loans, receiving income tax information from current or prospective students and their parents as a part of a financial aid application, offering credit or interest bearing loans, and other miscellaneous financial services.

Examples of student financial information relating to such products or services are bank and credit card account numbers, income and credit histories, and social security numbers. "Covered data" consists of both paper and electronic records that are handled by the Institution or its affiliates.

## 4. RESPONSIBILITIES

The major responsibilities each party has in conjunction with the GLBA policy are as follows:

A. **Information Security Coordinator.** The Chief Executive Officer will designate a qualified Information Security Coordinator to implement, oversee and enforce the institution's information security program and to facilitate the GLBA compliance activities of the business units processing covered data. The coordinator, in conjunction with the Responsible Executive and the Responsible Office for this policy, will assist business units in meeting their obligations and responsibilities associated with protecting covered data, and corresponding policies and processes. Based upon the feedback collected from the business units, the coordinator will report on an annual basis the status of compliance, and communicate these findings to those with authority over the data.

The Information Security Coordinator (currently Kamran Mokhtari, CIO) will collect the status from all units and provide annual reports to the Unitek Learning Executive Leadership Team and Campus Directors. Additionally, the Information Security Coordinator submits an information security report in writing, regularly and at least annually, to Unitek's Board of Directors, which includes the following:

- The overall status of the information security program and the institution's compliance with the Rule;
- Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.

B. **Institutional Administrators.** An Institutional Administrator responsible for managing employees with access to "covered data" is also responsible for ensuring protection of covered data through the application of the GLBA control standards and required processes outlined in this document.

Administrators or designated responsible point(s) of contact will work with the Information Security Coordinator to assist in implementing this program. The Administrator or the designated contact, along with the Information Security Coordinator, will ensure that applicable risk assessments are carried out for that unit and that monitoring based upon those risks takes place. The Administrator or designated responsible contact will report the status of their Information Security Program for covered data accessible in that unit to the GLBA Program Coordinator at least annually and more frequently where appropriate.

C. **Employees with Access to Covered Data.** Employees with access to covered data must abide by company policies and procedures governing covered data, as well as any additional practices or procedures established by their unit heads or directors.

D. **Compliance with this Policy.** Departmental compliance with this policy is subject to review by the Sr. Vice President of Compliance and the Chief Information Officer.

## 5. POLICY STATEMENT

**GLBA Requirements** - Any person or department using or processing covered data shall ensure protection against anticipated threats or hazards to the security or integrity of covered data by implementing the GLBA control standards. Further, business units, along with the Information Security Coordinator, are responsible for ensuring that the following activities and processes are implemented:

A. Conduct an annual risk assessment of likely security and privacy risks.

B. Institute a training program for all employees who have access to covered data and information.

C. Oversee service providers and contracts by periodically assessing providers based on the risk they present and the continued adequacy of their safeguards.

D. Evaluate, assess and test third-party software applications.

E. Evaluate and adjust their information security processes in light of testing and monitoring activities.

## 6. PROCEDURES

### Written Risk Assessment

The Information Security Coordinator ensures that a written risk assessment is completed and periodically reassessed, which includes the following at a minimum:

- Criteria for evaluating identified risks faced by the institution;
- Criteria for the assessment of the confidentiality, integrity and availability of the institution's information systems and customer protection; and
- How identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the institution's risks.

### Written Incident Response Plan

The Information Security Coordinator ensures that a written incident response plan is maintained and followed, which includes the following at a minimum:

- Goals of the plan;
- Procedures to support timely and effective execution and support of a return to business as usual in the event of a tragic event or critical incident;

- A notification plan which includes a list of internal departments, management, business partners, vendors, etc.;
- Company structure and roles to include who has the authority to confiscate or disconnect equipment and to monitor suspicious activity and hand-off/escalation points within the process;
- Who is to speak with press, media, business partners, etc., and what those discussions should contain;
- Process for documenting, contacting and reporting to local, state and federal law enforcement; and
- Requirements for remediation to include evaluation and revision to response plan following security event.

**Training Requirements**

The Information Security Coordinator ensures that all personnel with GLBA security responsibilities receives applicable and ongoing training, which includes:

- Providing personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;
- Utilizing qualified information security personnel employed by the institution or service provider sufficient to manage information security risks and to perform or oversee the information security program;
- Providing information security personnel with security updates and training sufficient to address relevant security risks; and
- Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

**GLBA Security Standards and Controls**

The institution designs and implements safeguards to control risks. The GLBA Security Control Standards have been developed in order to provide direction on the appropriate logical, administrative, and physical security controls to apply to GLBA Data. Therefore, GLBA Institution data will be protected by implementing the GLBA Security Control Standards, which include the following processes:

- Implementing and periodically reviewing access controls, including technical and physical controls;
- Encrypting all customer information held, when in use, or transmitted by the institution both in transit over external network and at rest;
- Identifying and managing the data, personnel, devices, systems, and facilities that enable the institution to achieve business purposes in accordance with their relative importance to their business objectives and risk strategy;
- Implementing multi-factor authentication for any individual accessing any information system;
- Procedures for change management;
- Developing, implementing, and maintaining procedures for the secure disposal of customer information; and

Implementing policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

## I. Purpose

The purpose of the Gramm-Leach-Bliley (GLBA) Security Standard is to provide the data protection security necessary to comply with Unitek's GLBA Security Policy. These standards are mandatory requirements, and establish an effective baseline of appropriate system, administrative, and physical controls to apply to covered data. Specific information security guidelines and checklists are available to provide guidance on how to comply with these standards.

## II. Security Standards and Controls

### 1 Network

1.1 A network based firewall shall be implemented that denies traffic from "un-trusted networks and hosts.

1.2 Network traffic shall be limited to only those services and ports considered essential, unless exceptions to allow access to required services are requested and granted.

1.3 Networks that house devices with GLBA data shall be scanned for vulnerabilities at least semi-annually. Vulnerabilities detected shall be remediated in a timely manner.

1.4 Additional security detection tools (Intrusion Detection (IDS)) should be considered in cases where a high degree of GLBA data exists.

### 2 Host

2.1 Devices that process or store GLBA information shall be housed in a physically secure location, accessible to only those with a business purpose.

2.2 Security updates and patches shall be applied in a timely manner, or automatically when possible.

2.3 Computer system support must monitor for announced vulnerabilities in their hardware and software.

2.4 Where possible, computer anti-virus shall be implemented, and updated in a timely manner, or automatically where appropriate.

2.5 Where appropriate, a host based firewall shall be implemented.

2.6 Services and applications should be the minimum necessary to accomplish the required business functions.

2.6.1 Passwords shall be changed from the vendor defaults.

2.6.2 Systems should be "hardened" to a recognized standard, where available.

2.7 Individual access to data shall be limited to only those authorized and/or needing access for business purposes.

2.7.1 For employees, only to the extent needed to perform their duties and functions.

2.7.2 For customers, only to the extent needed to access their own information.

2.8 The amount of GLBA information collected and stored shall be the minimum amount required for the efficient and effective conduct of business functions.

2.9 Where possible, secure (encrypted) data transmission and storage shall be utilized, for all devices, including laptops and portable media, where appropriate.

2.10 Devices processing or storing GLBA data shall log all significant security event information. Logs are reviewed if there is a breech, and are retained for at least 90 days.

2.11 Files shall be backed up and tested on a regular schedule, and stored in a secured location both on and off-site.

2.12 Hardware, software and data destruction shall be securely disposed at the termination of business need.

## 3 User Accounts

3.1 A process shall be established to create and assign, maintain, and verify a unique system identifier (i.e. UserID) for each user.

3.2 Authentication to a system identifier shall be controlled by a mechanism implemented based upon the sensitivity of the data.

3.3 In cases where UserID and Password are used for authentication purposes, whether for interactive or file transfer purposes, the password must be encrypted.

3.4 Multi-factor authentication for any individual (employee, customer or otherwise) accessing customer information or internal networks which contain customer information.

## 4 Data Retention

4.1 This institution maintains a retention policy to securely dispose of customer data after two (2) years unless it's necessary for business operations, a legitimate business purpose, or as required by law.

4.1.1 Policies are periodically reviewed to minimize the unnecessary retention of data.

## 5 Software Development

5.1 As of the revision date of this policy, the institution does not develop any software internally.

## 6 Testing Effectiveness of Controls

6.1 Effectiveness of the information security program must be tested through:

6.1.1 Continuous monitoring; or

6.1.2 Annual penetration testing AND

6.1.3 Vulnerability assessment at least twice a year to determine any material change to the operations or business and any circumstances that arose which would materially impact the security program.

## 7 Policy and Procedure

7.1 Each department processing or storing GLBA data shall establish a security policy, and corresponding procedures to address the following:

7.1.1 Computer Incident Response

7.1.2 Computer Incident Reporting

7.2 Each department processing or storing GLBA information shall provide security awareness training (i.e. seminar, podcast, etc) on an annual basis.

7.3 Each external vendor processing or storing GLBA data will be required to meet the security requirements set forth in this standard.

## Glossary

**Authentication:** The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

**Availability:** To ensure that the information remains accessible to authorized users.

**Baseline Requirement:** A baseline requirement is a requirement that represents a minimum security requirement from a body of minimum requirements. Baseline requirements are directed at maintaining a minimum level of security.

**Baseline Control:** A baseline control is a minimum security control.

**Confidentiality:** To ensuring that only authorized people have access to information.

**Data Owner:** Department head, manager or delegate within the University who has responsibility and authority for a particular set of information

**"Hardened":** The process of securing a system, which is done to protect systems against attackers.

**Server(s) :** Computer systems engaged in providing data or services across the network.

**User(s):** Users are identified as all individuals who make use of Unitek Learning Systems

**END OF PROCEDURES**

Campus management is responsible for the training of campus staff and monitoring continued compliance with the policy and procedures.

## POLICY KEY

**ACA –** Academics
**ADM –** Admissions
**BOM –** Business Office
**CSR –** Career Services
**COM –** Compliance
**FAC –** Facilities
**HRS –** Human Resources
**LGL –** Legal
**IT –** Information Technology
**SFS –** Student Financial Services
**SSR –** Student Services
**FIN –** Finance/Accounting