GLBA Information Security Program and Risk Management Policy for Summit Salon Academy Kansas City

Effective: 1/1/2022
Last Updated: 5/8/2023
Policy Owner: Information Security / Technology Officer (Jeremiah Griffith)
Revision Cycle: Biennial

The Gramm Leach Bliley Act addresses the safeguarding and confidentiality of customer and student information held in the possession of financial institutions. This GLBA Information Security Program describes the safeguards implemented by the Summit Salon Academy of Kansas City to protect covered data and information in compliance with the Federal Trade Commission's Safeguards Rule of the Gramm Leach Bliley Act (GLBA) and further pursuant to 16 CFR 314.4(b). These safeguards are provided to:

- Ensure the security and confidentiality of covered data and information.
- Protect against anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any customer.

Policy Statement:

Summit Salon Academy Kansas City (SSAKC) follows the GLBA guidelines and has appointed Jeremiah Griffith as our Information Security Program Coordinator. In this position he conducts a risk assessment of likely security and privacy risks, institutes a training program for all employees who have access to covered data and information, oversees service providers and contracts, and evaluates and adjusts the GLBA Information Security Program periodically. He works closely with Director, Jason York.

GLBA Program Coordinator

Jeremiah Griffith (Security Officer) and Jason York (Director) are responsible for the development of the GLBA Program at SSAKC. The Information Technology Services (ITS) Information Security Officer (Jeremiah Griffith), the Director of Financial Aid (Marcia Kelley), and the Director of the Admissions Office (Ginger West) are considered the GLBA program coordinators for their respective areas.

Each program coordinator is responsible for assessing the risks associated with unauthorized transfers of covered data and information, and implementing procedures to minimize those risks, instituting a training program for covered employees, and overseeing assigned service providers and contracts. Internal Audit personnel (Jason York and Jeremiah Griffith) will also conduct reviews of areas that have access to covered data and information to assess the internal control structure put in place by the administration and to verify that all departments comply with the requirements of the security policies and practices delineated in this program.

Covered Data and Information

For the purpose of this program, covered data includes student financial information that is protected under the GLBA. SSAKC considers student financial information to be that which SSAKC has obtained from a student or customer in the process of offering a financial product or service, or such information provided to SSAKC by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student or a parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

Departments Covered by GLBA

The following describes the mapping of department and data that fall under the GLBA.

Admissions: PII (SSN, date of birth, driver's license number.)

Financial Aid: Loans, Payment Plans, Financial Aid Disbursement information, 1098T's, tax returns. PII (SSN, billing information, credit card info, banking account info, date of birth, driver's license number)

ITS/Saltech/FAME: Responsible for storage of all covered data previously mentioned.

Identification and Assessment of Risks to Customer Information

SSAKC recognizes that it is exposed to both internal and external risks, including but not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Recognizing that this may not represent a complete list of the risks associated with the protection of covered data and information, and that new risks are created regularly, information security program coordinators will ensure periodic risk assessments are conducted. The SSAKC ITS Risk Assessment Procedure will be used to ensure risk assessments and subsequent remediation actions are conducted.

Employee Management and Training

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. Jason York – Director, is responsible for ensuring that new employee training and annual refresher training occurs and is documented. Jeremiah Griffith (Security Officer) is responsible for reviewing the training material for completeness.

Physical Security

Physical security of covered data and information is available to only those employees who have a legitimate business reason to handle such information. For example, financial aid applications, income and credit histories, accounts, balances and transactional information are available only to employees with an appropriate business need for such

information, our Director and Financial Aid Director. Furthermore, each department responsible for maintaining covered data and information is instructed to take steps to protect the information from destruction, loss, or damage due to environmental hazards, such as fire and water damage or technical failures. SSAKC Data Storage and Management Procedures and Media/Hardware Disposal Procedures support the GLBA Program.

Information Systems

Access to covered data and information via SSAKC's computer information systems is limited to those employees and faculty who have a legitimate business reason to access such information. SSAKC has policies and procedures in place to complement the physical and technical (IT) safeguards in order to provide security for the information systems. These policies and procedures are listed in the "Related Information" section below.

Oversight of Service Providers

GLBA requires the institution to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. SSAKC ITS has a Third-Party Agreement that defines how service providers may store, use, and dispose of SSAKC data. ITS, Purchasing Services and SSAKC Legal Counsel work together to ensure service providers contracts contain appropriate terms to protect the security of covered data.

Continuing Evaluation *and* Adjustment

This document will be managed by the ITS Document Development process to ensure that it is periodically reviewed and remains current.

Maintenance Practices and Vulnerability Awareness

A daily virus monitor is in place as well as a firewall system.

Communication

This policy shall be published to the SSAKC Internal Policy Manual and be available for review. The following offices and individuals shall be notified via email updates/changes to our program and upon any subsequent revisions or amendments made to the original document:

- Admissions – Ginger West
- Financial Aid – Marcia Kelley
- Information Technology Services – Jeremiah Griffith

Related Information:

Gramm-Leach-Bliley Act
FTC: Final Rule--Standards for Safeguarding Customer Information (16 CFR Part 314)
FTC: Final Rule--Privacy of Consumer Financial Information (16 CFR Part 313)
FTC Guidance: Financial Institutions and Customer Data--Complying with the Safeguards Rule

Document Revision History

Periodic review of this document is managed by Jeremiah Griffith and Jason York.

Date	***Revision Notes***	***Revision Number***
Oct. 2019	Creation	0
May. 2023	Contact Updates	1