Gramm-Leach-Bliley Act Safeguards Rule with Seven (7) Elements (2023_Guide_C.8.6) (2023_Guide_C.8.6)

Overview of the School

The Information Security Program for our School serves to protect school information from unauthorized and/or unlawful access, use, destruction, or loss, while helping to ensure the integrity and availability of data and IT resources at Latin Beauty Academy. Various components work together and serve as pillars in supporting the school's integrated program, including policies and standards, guidance on employee security best practices, security awareness and education, cyber security defense capabilities, information security risk management, vulnerability management, and security incident response.

An important aspect of the Latin Beauty Academy Information Security Program is the integration of relevant compliance regulations into the overall program. To support compliance with the GLBA Safeguards Rule, the program is designed to achieve key GLBA objectives such as ensuring the security and confidentiality of customer information, protecting against anticipated threats to the security or integrity of such information, and protecting against unauthorized access that could result in harm to any customer. The program implements administrative, technical, and physical safeguards to ensure the security and confidentiality of customer records and information. The revised Safeguards Rule outlines requirements that should be covered in an institution's Information Security Program (EDUCAUSE, 2021; FTC, 2022a; FTC, 2022b), and our program and its components are designed to meet such requirements.

Definition of the Act

The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule pertains to the safeguarding of customer financial information. The rule mandates that financial institutions, including schools receiving federal funds, must create policies to protect this information.

The GLBA broadly defines "financial institution" as any institution engaging in the financial activities enumerated under the Bank Holding Company Act of 1956, including "making, acquiring, brokering, or servicing loans" and "collection agency services." Because higher education institutions participate in financial activities, such as making Federal Perkins Loans, FTC regulations consider them financial institutions for GLBA purposes.

Rule Summary

Safeguards Rule

The information below describes the various components of the school's information security program that are in accord with, and support compliance with, the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, and provides references to additional materials and to applicable policies and guidelines.

In its capacity as a financial institution, Latin Beauty Academy is required to maintain an information security program, the Financial Office develops and supports this program. This program must include the following elements:

a. **Designate a "Qualified Individual" responsible for overseeing, implementing, and enforcing the information security program.** The School's "Qualified Individual" responsible for the information security program is President/CEO.

b. **Base the information security program on a risk assessment of the security, confidentiality, and integrity of customer information, and assess the sufficiency of any safeguards in place to control these risks.** School information security program follows a risk-based approach, risks are assessed and addressed on a regular basis. Significant components of the program are established in School Information Technology Security Policy.

c. **Design and implement safeguards to control the risks identified in the risk assessment.** The Latin Beauty Academy has established the Data Classification Policy, Gramm-Leach-Bliley Policy, Data Breach Notification Policy and Information Technology Security Policy to direct all relevant offices and employees on standards and requirements for safeguarding data, including "Covered Information" in scope of GLBA. All Covered Offices that are responsible for Covered Information must establish their own practices and procedures for information and documents. If additional safeguards are needed to address identified risks, President/CEO will work with Directors to develop or update them.

d. **Regularly test or otherwise monitor the effectiveness of safeguards.** For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Units are responsible for routine monitoring, testing, and assessing the effectiveness of safeguards implemented by them. The Office of Information Technology offers additional monitoring and vulnerability assessment capabilities and can arrange for penetration testing as needed.

e. **Implement policies and procedures for security awareness training.** People who have access to GLBA data are required to take GLBA training and information security training at least annually.

f. **Oversee service providers.** Contracts with third parties involving information technology and that include the processing of personal data are reviewed by the Procurement and Contracts Department, Information Security team, and other relevant parties (e.g. Office of General Counsel, Risk Management, and Director, Cyber Policy). Latin Beauty Academy has established its own Data Protection Agreement in the case of a third-party vendor having a missing or deficient agreement. The review process must take place at initiation and renewal of agreements and may also occur in the case of a significant triggering event.

g. **Evaluate and adjust the information security program in light of the results of testing and monitoring.** The Office of Information Technology regularly reviews and adjusts the information security program following established governance practices.

h. **Establish an incident response plan.** Latin Beauty Academy has established policy that requires the implementation of safeguards for Covered Information and encourages reporting of real or suspected data breaches.

i. **Require of Qualified Individual to report in writing, regularly and at least annually, to the board of directors or equivalent governing body.** The Vice President & Chief Information Officer will provide a written report at least annually to the Board of Trustees on behalf of the Qualified Individual. The report will include: (1) The overall status of the information security program and (2) material matters related to 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 and substantive changes in the information security program.

Privacy Rule

The GLBA Privacy Rule (16 CFR 313) enforces several requirements related to the handling of nonpublic personal information.

For example, financial institutions must issue an initial privacy notice to consumers as soon as they become customers of that financial institution.

Colleges and universities are deemed to be in compliance with the GLBA Privacy Rule if they are in compliance with the Family Educational Rights and Privacy Act (FERPA).

Latin Beauty Academy is subject to and complies with the requirements of the **Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99, as amended)**.

Latin Beauty Academy Information Security Program and GLBA Safeguards Rule Compliance

As mentioned above in the Overview, this article highlights how the various components of the Information Security Program are in accord with, and support compliance with, the provisions and requirements in the revised Safeguards Rule of the Gramm-Leach-Bliley Act (GLBA). The school's program is intended to meet the following requirements of the GLBA Revised Safeguards Rule that will be discussed in the following sections below:

- Designate a qualified person to oversee the information security program
- Implement appropriate safeguards and conduct a risk assessment
- Limit and monitor who can access sensitive customer information
- Encrypt sensitive information
- Train personnel
- Maintain an incident response plan
- Periodically assessing the security practices of service providers
- Implement multi-factor authentication to protect sensitive information

References

- East Carolina School. (2016, May 23). Information security regulation. School Policy Manual. https://www.ecu.edu/prr/08/05/08
- EDUCAUSE. (2018). Gramm-Leach-Bliley Act (GLB Act). Policy and Law. https://library.educause.edu/topics/policy-and-law/gramm-leach-bliley-act-glb-act
- EDUCAUSE. (2021, December 2). Policy analysis: Revised, highly prescriptive FTC Safeguards Rule. Educause Review. https://er.educause.edu/articles/2021/12/policy-analysis-revised-highly-prescriptive-ftc-safeguards-rule
- Federal Trade Commission. (2022a, May). FTC Safeguards Rule: What your business needs to know. Business Guidance. https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
- Federal Trade Commission. (2022b, November). Compliance deadline for certain revised FTC Safeguards Rule provisions extended to June 2023. Business Guidance. https://www.ftc.gov/business-guidance/blog/2022/11/compliance-deadline-certain-revised-ftc-safeguards-rule-provisions-extended-june-2023
- National Archives. (2002). Part 314 – Standards for safeguarding customer information. Code of Federal Regulations. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314