42 S. Catalina Ave.
Pasadena, CA 91106
T 626.577.1751
www.ccmla.edu

Title: Gramm-Leach Bliley (GLBA) Security Program

Overview

California College of Music (CCM) is committed to ensuring compliance with the Gramm- Leach-Bliley Act (GLBA) to protect the privacy and security of our students' nonpublic personal information (NPI). We recognize the importance of maintaining the trust and confidence of our students, faculty, and staff, and we have implemented the necessary policies and procedures to meet GLBA requirements. This document provides evidence of our GLBA compliance efforts:

Privacy Notice: CCM has developed and distributed a comprehensive privacy notice that outlines the types of NPI we collect, how we use it, and the circumstances under which we disclose it to third parties. Our privacy notice is easily accessible on our institution's website, and physical copies are available upon request. The notice is provided to students during the enrollment process and is included in our student handbook.

Procedures

The GLBA stipulates that the Information Security Program must encompass specific components. The College's procedures regarding these components are outlined below.

Element 1: Designates a qualified individual responsible for overseeing and implementing the school's or servicer's information security program and enforcing the information security program (16 C.F.R. 314.4(a)).

The designated privacy officer oversees all facets of the GLBA security program and manages day-to-day operations, fulfilling the requirement outlined in 16 C.F.R. 314.4(a) to designate a qualified individual for implementing and enforcing the information security program.

Element 2: Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks. (16 C.F.R. 314.4(b)).

The Privacy Officer and Student Records Officer will work closely together, adhering to the guidelines and protocols outlined in the policy and procedures handbook. They will conduct a thorough risk assessment to identify both internal and external risks to the security, confidentiality, and integrity of customer information, as defined within the institution's context. This assessment will encompass potential scenarios that could lead to unauthorized disclosure, misuse, alteration, destruction, or any compromise of such information. Additionally, they will evaluate the effectiveness of existing safeguards in place to mitigate these risks. Through their collaborative efforts and adherence to the handbook, they

will ensure the development and implementation of a robust information security program that aligns with regulatory requirements and safeguards customer information effectively.

In addition to their collaboration, the Privacy Officer and Student Records Officer will consult with the Director to ensure comprehensive handling of documentation. This consultation process will involve discussing strategies for documenting risk assessment findings, safeguard evaluations, and any necessary adjustments to the information security program. By working together and seeking guidance from the Director, they will ensure that documentation practices align with organizational standards and regulatory requirements, contributing to the overall effectiveness of the information security program.

Element 3: Provides for the design and implementation of safeguards to control the risks the school or servicer identifies through its risk assessment (16 C.F.R. 314.4(c)). At a minimum, the written information security program must address the implementation of the minimum safeguards identified in 16 C.F.R. 314.4(c)(1) through (8).

- Access Controls: We implement access controls to restrict NPI access to authorized personnel on a need-to-know basis. User accounts are created with unique identifiers and passwords, and access permissions are regularly reviewed and updated to prevent unauthorized access.

- Data Encryption: CCM employs encryption techniques to protect NPI during transmission and storage. We utilize industry-standard encryption protocols for data transmitted over public networks and employ encryption methods for NPI stored on our systems and databases.

- Security Assessments: We conduct periodic assessments of our information security controls to identify vulnerabilities and implement necessary improvements. These assessments include internal audits and external third-party security evaluations to ensure the effectiveness of our security measures.

- Incident Response Plan: CCM has established an incident response plan to address and mitigate any security incidents or breaches. This plan includes procedures for incident reporting, investigation, containment, and notification. We maintain documentation of security incidents, response actions taken, and measures implemented to prevent future occurrences.

Element #4: Provides for the institution or servicer to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 C.F.R. 314.4(d)).

Regular testing and monitoring for effectiveness will be conducted in accordance with California College of Music's standard processes.

Third-Party Oversight: CCM exercises due diligence in selecting and engaging third-party service providers who may have access to NPI. We carefully evaluate their security practices and review their GLBA compliance efforts before entering contracts. Contracts with third-party service providers include provisions that address data privacy and security obligations.

Element #5: Provides for the implementation of policies and procedures to ensure that personnel are able to enact the information security program (16 C.F.R. 314.4(e)).

Employee Training and Awareness: Our commitment to data security extends to all individuals involved in handling non-public personal information (NPI), including our faculty, staff, and third-party contractors. We provide thorough training programs covering GLBA compliance, data privacy, and best practices in information security. Upon onboarding, employees and contractors tasked with NPI responsibilities undergo comprehensive training sessions to familiarize themselves with our policies and procedures. Recognizing the evolving nature of cybersecurity threats and regulatory changes, regular refresher courses are conducted to ensure that our personnel remain well-informed and equipped to mitigate risks effectively. We maintain meticulous records of training activities to demonstrate our ongoing commitment to compliance.

Moreover, we extend our vigilance to third-party contractors, engaging them in robust training initiatives to instill a culture of data security and confidentiality. Collaboratively, we work to establish and uphold the highest standards of care in handling sensitive data, minimizing the potential for breaches and ensuring the integrity of our information systems.

Element 6: Addresses how the school or servicer will oversee its information system service providers (16 C.F.R. 314.4(f)).

Through its Information Security Procedures, the College has established standardized language pertaining to safeguards for handling Non-Public Personal Information (NPI). This language is integrated into contracts and agreements with service providers who may necessitate access to NPI. As part of the College's procurement process, contracts for technology requiring access to NPI undergo a security review during initial contracting. Depending on the assessed risk level, these contracts may undergo re-evaluation during the renewal period.

Element #7: Provides for the evaluation and adjustment of its information security program in light of the results of the required testing and monitoring; any material changes to its operations or business arrangements; the results of the required risk assessments; or any other circumstances that it knows or has reason to know may have a material impact on the information security program (16 C.F.R. 314.4(g)).

In accordance with Element #7, California College of Music (CCM) ensures the ongoing evaluation and adjustment of its information security program. This process includes analyzing the results of mandatory testing and monitoring, assessing any material changes to operations or business arrangements, and considering the outcomes of required risk assessments. Additionally, we remain vigilant for any circumstances that may materially impact our information security program, promptly making adjustments as necessary to uphold the integrity and effectiveness of our security measures.