SCHOOL OF VISUAL ARTS

2025 SVA Information Security Program GLBA Compliance Program

Version: 2026.03.11.5

Category: Data Privacy & Compliance

1.0 Purpose

This document is designed to provide a framework of the Information Security program adopted by School of Visual Arts (SVA) designed to protect the critical and sensitive information held by SVA. The purpose of this program is to ensure the protection of this information and to comply with applicable legal requirements, including the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act (GLBA). The practices set forth in this document will be carried out by and impact diverse areas of SVA. For information on SVA's compliance with the Family Educational Rights and Privacy Act (FERPA) please see SVA's FERPA Policy .

2.0 Scope

This security program applies to consumer financial information (covered data) SVA receives in the course of business as required by GLBA as well as other confidential financial information SVA has voluntarily chosen as a matter of policy to include within its scope.

3.0 Policy

3.1 Gramm–Leach–Bliley Act (GLBA)

The GLBA (113 Stat. 1338; also called the Financial Services Modernization Act of 1999) imposes various obligations on "financial institutions" notably including obligations regarding data privacy and security. GLBA defines the term "financial institution" broadly as "companies that offer financial products or services to individuals, like loans, financial or investment advice, [and] insurance". The Federal Trade Commission (FTC), the agency with primary oversight authority over GLBA has

issued guidance confirming that educational institutions offering student financial assistance are subject to GLBA as “financial institutions.”

In addition to FTC enforcement, through two guidance “Dear Colleague” letters in 2015 and 2016, the U.S. Department of Education (DoE) has stated its intent to enforce GLBA obligations through the Program Participation Agreement (PPA) institutions sign to participate in the Title IV federal student financial assistance programs. Through its guidance, DoE has also stated that institutions have an obligation to “immediately” notify DoEof suspected data breaches.

3.2 Security Program Framework

The GLBA requires that SVA develop, implement, and maintain a comprehensive information security program containing the administrative, technical, and physical safeguards that are appropriate based upon SVA's size, complexity, and the nature of its activities.

3.3

3.4 Security Program Coordinator

The GLBA Security Program Coordinators (Coordinators) will be responsible for implementing this Information Security Program. The Coordinators shall be appointed by the Executive Leadership Team. The Coordinators will work closely with Institutional Technology, the Registrar’s Office, Human Resources, Student Financial Services, Student Financial Aid, and other offices or departments that may use or own covered data.

3.5 Key GLBA Data Security Provisions

Most notably, GLBA contains a provision known as the “Safeguard Rule” (codified at 15 U.S.C. §§ 6801–6809) which imposes significant data security obligations on impacted entities. These obligations include:

• Designating appropriate individuals (Coordinators) to oversee SVA’s privacy matters

· Cosmin Tomescu – Chief Information and Privacy Officer

· Geanine Rando – Director of Student Accounts & Data Privacy Officer

• The Coordinators should conduct a thorough, internal risk analysis that identifies technical, physical, and administrative risks and vulnerabilities.

The Coordinators should meet at least bi-weekly to discuss ongoing privacy concerns and improving the process for the future. At least biweekly or monthly, the officers should discuss various issues with outside legal counsel.

• The Coordinators should review third-party agreements for vendors that have access to sensitive data (including, but not limited to student data) to ensure that the contractual obligations provide reasonable data security protections. Such obligations should also be included in all future vendor agreements.

All contracts for outside vendors should be reviewed first by SVA Campus Store, second by SVA Resource Management group (Purchasing) and finally by the Coordinators if data privacy and information security terms are included.

• Based on this risk assessment, the Coordinators should oversee the development and implementation of a comprehensive data security plan designed to address identified technical, physical, and administrative risks and vulnerabilities.

• The Coordinators should oversee the communication and training for employees detailing relevant obligations and duties.

Implement a cybersecurity and data privacy training program for all employees, based on everyone’s functional role. The training should be annually and updated as new regulations are implemented. Information Security training should be included.

• The Coordinators should also develop a process for routinely monitoring, evaluating, and revising the plan (and communicating updates to employees). This process should take into account the changing nature of likely threats and available protective technologies.

Annually a gap assessment questionnaire should be distributed to all department heads and managers. The Coordinators assess each department's privacy practices in their own groups and align those practices with corporate policies.

• The Coordinators should also develop, implement, and test a response plan for unauthorized disclosure of sensitive data (i.e. data breaches).

The SVA data breach incident response plan was revised following the completion of a tabletop exercise/training in Q4 2018 with the entire Emergency Management Committee team.

Summary of Key Plan Requirements

3.6 Administrative

• Cataloging all stored and/or transmitted data to categorize by sensitivity (and therefore identify for heightened security);

• Developing hiring policies that assess data security risks associated with key positions;

• Developing safe computing policies (password management, ID protection, training);

• Developing and enforcing data retention and destruction policies balancing anticipated needs with risk reduction

3.7 Technical

• Encryption methods used to store and transmit sensitive data;

• Anti-malware software on institution computers;

• Secure log-in systems for remote employee access to College's systems or databases (i.e. VPN);

• Monitor data transfers to flag potentially suspicious activity

3.8 Physical

• Clean desk policy;

• Laptop recovery and remote cleaning capabilities;

• Limited, recorded access to physical spaces containing sensitive data

• Develop back-up and recovery plan in case of inability to access local or remote systems

3.9 Risk Assessment

The Information Security Program identifies reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks.

The Coordinators will work with relevant areas to carry out comprehensive risk assessments. Risk assessments will include system-wide risks as well as risks unique to each area with covered data.

3.10 Information Safeguards and Monitoring

The Information Security Program will verify that information safeguards are designed and implemented to control the risks identified in the risk assessments set forth above. The Coordinators will ensure that reasonable safeguards and monitoring are implemented and cover each unit that has access to covered data. Such safeguards and monitoring will include the following:

3.11 Employee Management and Training

Safeguards for security will include management and training of those individuals with authorized access to covered data.

The Coordinators will, working with other responsible offices and units, identify categories of employees or others who have access to covered data.

3.12 Information Systems

Information systems include the hardware and software used for the storage, transmission, creation and access to College information.

These systems will be reasonably designed to limit the risk of unauthorized access to covered data. This may include designing limitations to access and appropriate monitoring programs to detect and identify malicious activity.

3.13 Managing System Failures

SVA will maintain effective systems to prevent, detect, and respond to disasters, intrusions, data breaches, and other system failures.

3.14 Monitoring and Testing

Monitoring systems will be implemented to regularly test and monitor the effectiveness of information security safeguards.

3.15 Service Providers

In the course of business, SVA may from time to time appropriately share covered data with third parties. Such activities may include collection activities, transmission of documents, transfer of funds, destruction of documents or equipment, or other similar services. This Information Security Program will ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.

3.16 Program Maintenance

The Coordinators, working with responsible units and offices, will evaluate and, if appropriate, adjust the Information Security Program in response to any material changes to operations or business arrangements; results of assessments, testing or monitoring; or any other circumstances

which may reasonably have an impact on the Information Security Program. Related Policies, Standards, Guidelines

The Information Security Program incorporates by reference SVA's policies and procedures regarding the legal requirements of the programs referenced below and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations. Public facing policies can be found at policy.sva.edu . Other policies may be available upon request by emailing the Privacy Office at privacy@sva.edu .

Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of SVA property (physical or intellectual) are suspected, SVA may report such activities to the applicable authorities.

4.0 Definitions

· None

5.0 Revision History

This policy shall be subject to periodic review to ensure relevancy.

Date

Description of Change

Reviewer

7/1/2021

Rev 1.0

C. Tomescu

6/21/24

Rev 2.0 – Periodic review and update

C. Tomescu

6/1/2025

Rev 3.0 – Periodic review and update

C. Tomescu