Pensacola State College

Information Security and GLBA Plan

Contents

Purpose

The Gramm-Leach-Bliley Act (GLBA) addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions. Colleges are subject to GLBA because they collect and maintain financial information through student lending and alumni processes. Primary objectives of GLBA include:

- Ensuring the security and confidentiality of customer financial information
- Protecting against any anticipated risks or threats to the security and integrity of covered data
- Protecting against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to the customer.

This plan applies to customer financial information Pensacola State College (PSC) receives during business as required by GLBA and other confidential information the institution has chosen to include within its scope.

Overview

This plan outlines PSC's comprehensive written information security program, specifically in compliance with GLBA.

This IT security framework is based on the National Institute of Standards Technology Special Publication 800-53 (NIST 800-53). It provides a set of baseline security controls and is used to meet multiple compliance requirements. The Federal Trade Commission (FTC) uses NIST 800-53 framework to assess an organization's security posture. Further, Student Financial Aid (FSA) recommends using NIST 800-53 controls as GLBA safeguards. Using the NIST 800-53 allows an organization to assess and evaluate its specific environment and determine what security controls are necessary to best protect its organizational operations and assets. The NIST 800-53 prescribes different sets of controls for systems considered low, medium, or high impact and is continuously updated to respond to newly discovered threats or breaches.

The practices outlined in this document will be carried out by and impact diverse areas of PSC.

PSC is committed to protecting the confidential financial information it collects from faculty, staff, students, alums, and others. GLBA is enforced by the FTC. A data security breach that results from non-compliance is a violation of federal law. Failure to protect customer information may result in financial loss for customers, fines imposed on the institution, as well as related reputational damage.

Definitions

Customer – any individual who receives a financial service from PSC. Customers may include students, parents, spouses, faculty, staff, alumni, and third parties.

Non-public personal information - any personally identifiable financial or other personal information, not otherwise publicly available that PSC has obtained from a customer in the process of offering or providing a financial product or service; such information provided to the

College by another financial institution; or any list, description, or another grouping of customers (and publicly available information about them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include:

- Addresses
- Telephone numbers
- Bank and payment card numbers
- Income and credit histories
- Social Security numbers
- Health information

Financial product or service - student loans, employee loans, activities related to extending credit, economic and investment advisory activities, management consulting and counseling, community development, and other miscellaneous financial services.

Covered data and information - customers' non-public personal information must be protected under GLBA. In addition to this required coverage, the College also chooses to define covered data and information to include any bank and credit card account numbers, income and credit information, tax returns, asset statements, and social security numbers (SSNs) received during business by the College, whether or not GLBA covers such financial information. Generally, PSC should avoid using Social Security numbers as primary identification numbers. Covered data and information includes both paper and electronic records.

Scope/Applicability

The PSC GLBA Plan applies to all faculty, staff, students, organizations, contingent workers, third-party vendors, individuals, systems, and networks handling covered data. This includes transmission, storage, and processing of data, in any form (electronic or paper), on behalf of PSC.

Information Security Program

The GLBA establishes a Safeguards Rule that requires PSC to develop, implement, and maintain a comprehensive information security program with appropriate administrative, technical, and physical safeguards to protect customer information. This Information Security Program has five components:

1. Designating one or more employees responsible for coordinating the program
2. Conducting risk assessments to identify reasonably foreseeable security and privacy risks
3. Ensuring that safeguards are implemented to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored
4. Overseeing service providers
5. Maintaining and adjusting the Information Security Program periodically

Information Security Advisory Team (ISAT)

PSC's Information Security Advisory Team (ISAT) will be responsible for implementing the Information Security Program.

The ISAT will consult with responsible offices to identify units and areas of PSC with access to covered data. ISAT will conduct an audit, or utilize other reasonable measures, to confirm that all sites with protected information are included within the scope of this Information Security Program. ISAT will maintain a list of areas across the College with access to covered data.

The ISAT will ensure that risk assessments and monitoring are carried out for each area that has covered data and that appropriate controls are in place for the identified risks. The ISAT will work with responsible parties to ensure adequate training and education are developed and delivered for all workers and third parties with access to covered data. The ISAT will, in consultation with other College offices, verify that existing policies, standards, and guidelines that provide for the security of protected data are reviewed and adequate. The ISAT will make recommendations for revisions to this plan, or the development of a new plan, as appropriate.

The ISAT will periodically update the Information Security Program, including the GLBA Plan and related documents. The ISAT will maintain a written security plan and make the plan available to the PSC community.

Risk Assessment

The Information Security Program will identify 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 another compromise of such information and assess the sufficiency of any safeguards in place to control these risks.

Examples of relevant areas to be considered when assessing the risks of unauthorized customer information disclosures include, but are not limited to:

- Unauthorized access to covered data by workers, third parties, or through requests
- Compromised system security because of criminal hacking or unauthorized access
- Failure to adequately protect passwords
- Interception of data during transmission
- Physical loss of data in a disaster
- Corruption of data or systems
- Paper forms containing covered data that are not restricted to authorized workers
- Paper forms and computer systems vulnerable to break-in after hours
- Paper forms and computer systems left unattended during business hours
- Errors introduced into the system by authorized or unauthorized persons

The ISAT will work with all relevant areas to conduct comprehensive risk assessments. Risk assessments will include system-wide risks and risks unique to each area with covered data. The risk analysis methodology and approach will be conducted using guidelines in the NIST Special Publication 800-30 (Revision 1), Guide for Conducting Risk Assessments.

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. The Information Security Program will create a comprehensive IT security framework based on NIST 800-53.

The ISAT will implement reasonable safeguards and monitoring and cover each area with access to protected data. Such safeguards and monitoring will include the following:

Employee Management and Training
The ISAT will, working with other responsible offices and units, identify those individuals and roles with access to covered data and advise them of their responsibilities to protect customer information and systems from compromise.

Comprehensive policies, procedures, and recommendations for protecting covered data will be implemented. Training for all individuals with authorized access to covered data will include physical handling and disposal of non-electronic information and procedures for processing and storing electronic information.

Information Systems
The ISAT should maintain inventories of all computer systems accessing or controlling covered data. Information systems include network and software systems and information processing, storage, transmission, retrieval, and disposal.

Network and software systems will be reasonably designed to limit the risk of unauthorized access to covered data. This may include preparing role-based access through system IDs and passwords, regularly expiring and updating passwords, maintaining appropriate screening programs to detect criminal hackers and viruses, and implementing security patches within a defined period.

Managing System Failures
The College will maintain effective systems to prevent, detect, and respond to attacks, intrusions, and other system failures.

Such systems may include maintaining and implementing current anti-virus software, critical patches, appropriate filtering or firewall technologies, intrusion detection systems that monitor and detect attacks and intrusions, and vulnerability scanning, alerting those with access to covered data of potential security threats; shredding paper documents; backing up data regularly and storing back up information off-site, as well as other reasonable measures to protect the integrity and safety of information systems.

Monitoring and Testing
Monitoring systems will be implemented to regularly test and monitor information security safeguards' effectiveness.

Monitoring will be conducted to ensure that safeguards are being followed and to detect security gaps quickly. The level of monitoring will be appropriate based on the potential impact and probability of the risks identified, as well as the sensitivity of the

information provided. Monitoring may include sampling, system checks, reports of access to systems, reviews of logs, audits, and any other reasonable measures adequate to verify that information security controls, systems, and procedures are working.

Service Providers

During business, PSC may share covered data with third parties. Such activities may include collection activities, the transmission of documents, the transfer of funds, the destruction of documents or equipment, or other similar services. PSC will ensure that reasonable steps are taken to select and retain service providers capable of maintaining appropriate safeguards for protecting customer information. All third-party contracts must also incorporate specific language requiring that service providers implement and maintain such safeguards.

Physical Security of Paper Records

Only PSC workers with a legitimate and valid reason to have covered data shall have access to physical paper records. The records should be kept in a secure place, such as a locked office or file drawer, to prevent unauthorized access. Such records should be secured in locked cabinets whenever an authorized employee is absent with the records, particularly overnight.

Information Disposal

PSC should only keep physical paper records and electronic documents for as long as they are being actively used by the College or as necessary to comply with retention requirements established by the Department of State, Division of Library and Information Services, by the statutory provisions of Chapters 119 and 257, Florida Statutes. Duplicate paper documents containing covered data should be shredded with a cross-cut shredder at the time of disposal. Primary paper documents and electronic records should be destroyed as directed by the Department of State, Division of Library and Information Services, by Rule 1B-24.003(10) of the Florida Administrative Code.

Incident Response

It is the responsibility of all workers of PSC to promptly report any suspected compromise or confirmed breach of covered data. Please refer to the institution’s Incident Response Plan.

Notification and Reporting

PSC will follow the institution’s Incident Response procedures for promptly notifying customers if their non-public personal information is compromised.

Program Maintenance

The ISAT, working with responsible units and offices, will evaluate and adjust the Information Security Program based on the risk assessments, monitoring, and testing, as well as in response to any material changes to operations and any other circumstances which may reasonably have an impact on the Information Security Program.

Non-Compliance

Any PSC employee found to violate this plan may be subject to disciplinary action, up to and including termination.