Gramm-Leach-Bliley Act, (GLBA)

Gramm-Leach-Bliley Act, (GLBA), effective May 23, 2003, addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA contains no exemption for colleges or universities. In 2021, The Federal Trade Commission (FTC) issued amendments that were approved by its governing agency, the Gramm-Leach-Bliley Act (GLBA); subsequently, these changes updated the compliance requirements for those higher educational institutions with a financial connection to the Title IV Program.

As a result, educational entities that engage in financial activities, such as processing student loans, are required to comply. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices (employee, student, customer, alumni, doner, etc.), both electronic and physical. Current Compliance Policies will have a direct impact from the changes listed below:

- designate a qualified individual to oversee their information security program,
- develop a written risk assessment,
- limit and monitor who can access sensitive customer information,
- encrypt all sensitive information,
- train security personnel,
- develop an incident response plan,
- periodically assess the security practices of service providers and implement multi-factor authentication or another method with equivalent protection for any individual accessing customer information

These updates to current Compliance Policies at Piberry Institute are for certain highly critical and private financial and related information. This Compliance Program applies to customer financial information (covered data) that the School receives in the course of business as required by GLBA as well as other confidential financial information included within its scope.

GLBA Compliance Program:

The GLBA Compliance Program covers the entirety of the activities and practices of the following offices and individuals:

- Academic and administrative offices that handle electronic or printed personnel records, financial records, transactional records, or student records.
- Academic and administrative offices that transmit confidential information (protected data) to off-site locations as part of a periodic review or submission requirement.
- Centers and Institutes that provide services and acquire personal or financial information from participants or constituents.
- Faculty serving as directors, coordinators, principal investigators, or program directors for programs collecting protected data.
- Faculty, staff, and administrators with contracts to use, access, or provide protected data to or receive from a non-campus entity (e.g., government databases, science databases).

Categories of Information under the Plan:

Information covered under the plan is defined by three categories:

1. Personal Identifiable Information (PII) – Also known as protected data, PII includes first and last name, social security number, date of birth, home address, home telephone number, academic performance record, physical description, medical history, disciplinary history, gender, and ethnicity.
2. Financial Information – Information that the School has obtained from faculty, staff, students, alumni, auxiliary agencies, and patrons in the process of offering financial aid or conducting a program. Examples include bank and credit card account numbers, and income and credit histories.
3. Student Financial Information – Information that the School has obtained from a student in the process of offering a financial product or service, or such information provided to the School by another financial institution. Examples include student loans, income tax information received from a student's parent when offering a financial aid package, bank and credit card account numbers, and income and credit histories.

Key Points:

1. The Compliance Program is a continuous process that is undertaken at periodic intervals.
2. The GLBA Compliance Program Coordinator is responsible for implementing this Compliance Program.
3. IT, with the collaboration of HR, develop appropriate training programs to ensure staff is aware of protocols for protecting customer information.
4. The Coordinator works with the Office of the General Counsel and Procurement Office and other offices as appropriate to make certain that service provider contracts contain appropriate terms to protect the security of covered data.
5. The Coordinator, working with responsible units and offices, monitors, evaluates and adjusts the Compliance Program in light of the results of the risk management process.

Purpose

In order to continue to protect private information and data and to comply with the provisions of the Federal Trade Commission's safeguard rules implementing applicable provisions of the GLBA, the School has adopted this Compliance Program for certain highly critical and private financial and related information. The Compliance Program forms part of the overall strategic information security program of the School. This program applies to customer financial information (covered data) the School receives during business as required by GLBA as well as other confidential financial information the School has voluntarily chosen as a matter of policy to include within its scope.

Gramm-Leach-Bliley Act, (GLBA)

This page describes many of the activities undertaken by the School to maintain the security and privacy of the covered data according to GLBA requirements.

Scope and Applicability

The program is poised to protect private information and data and to comply with the provisions of the Federal Trade Commission's safeguard rules implementing applicable provisions of the GLBA, the School has adopted this Compliance Program for certain highly critical and private financial and related information. The Compliance Program forms part of the overall strategic information security program of the School. This program applies to customer financial information (covered data) the School receives during business as required by GLBA as well as other confidential financial information the School has voluntarily chosen as a matter of policy to include within its scope.

Departments Covered Under the GLBA

- Admissions
- Financial Aid
- Academic Department
- Finance Department

Compliance Program Plan

Compliance means following the laws, regulations, and School policies that govern our everyday activities as members of the School community. This Compliance Program is a continuous process that is evaluated and adjusted in light of the following:

- The results of the required testing/monitoring, Any material changes to Piberry Institute's operations or business arrangements
- Any other circumstances that may have a material impact on Piberry Institute's information security program.
- Data Mapping
- Risk Assessment and Implementation of Safeguards
- Access Control
- Encryption
- Awareness, Training, and Education
- Incident Response Plan and Procedures
- Evaluate Service Providers' Agreements and Processes
- Continuous Program Maintenance
- Defined Policies and Standards
- This section highlights the approach taken by the School to ensure compliance with the GLBA requirements.

- Defined Policy and Standards
- Data Mapping
- Risk Assessment and Implementation of Safeguard
- Conduct Risk Assessment
- Design and Implement Safeguards

As a result of the risk assessment, recommendations are made as necessary to change management practices to improve business controls and/or to implement information safeguards. The School has developed a set of policies and procedures to guide the security and privacy of data covered by GLBA:

- Testing and Monitoring of the Systems
- Vulnerability Assessment
- Access Control
- Encryption
- Data Retention and Disposal
- Provide Awareness, Training and Education
- Incident Response Plan and Procedures
- Evaluate Service Providers' Agreements and Processes
- Program Maintenance

Contact Information

Persons who may have questions regarding the security of any of the categories of information that is handled or maintained by or on behalf of the School may contact:

Marion Carberry
Piberry Institute
30356 Old Dixie Hwy
Homestead, FL 33033
(305) 245-2581

The complete Gramm Leach Bliley Information Security Program is available at the President's Office.

Definitions

This section highlights some of the key terminologies used under the GLBA.

Customer Information - means any record containing non-public personal information as defined in 16 CFR 313.3(n), about a faculty, staff, and student of Piberry Institute's, whether in paper, electronic, or other forms, that is handled or maintained by or on behalf of Piberry Institute's or its service providers.

The following are examples of data elements, but not limited, that fall under customer information, whether they are stored as paper records or electronically:

- Name
- Home address
- Home phone number
- Date/location of birth
- Driver's license number
- Name of spouse or other relatives
- Citizenship
- Bank and credit card number
- Income and credit histories
- Social Security numbers
- Students performance evaluations or letters related to performance
- Other information within the definition of "customer information

Non-public personal information - means any personally identifiable financial or other personal information, not otherwise publicly available, that the School has obtained from a customer in the process of offering a financial product or service; such information provided to the School by another financial institution; such information otherwise obtained by the School in connection with providing a financial product or service; or any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any information listed above that is not publicly available. Examples of personally identifiable financial information include names, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

Financial Information - includes student financial aid, student, faculty and staff loans.

Covered data and information - for this program, this includes non-public personal information of customers required to be protected under GLBA. In addition to this required coverage, the School chooses as a matter of policy to also 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 received in the course of business by the School,

whether or not such financial information is covered by GLBA. Covered data and information includes both paper and electronic records.

Service provider - means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to Piberry Institute's that is subject to this part.

POSTED ON LMS INTRANET:

What is Identity Theft?

Identity theft occurs when someone uses another person's personal information such as name, Social Security number, driver's license number, credit card number, or other identifying information to take on that person's identity in order to commit fraud or other crimes.

How to Protect Yourself from Identity Theft

The following tips can help lower your risk of becoming a victim of identity theft.

- Protect your Social Security number. Don't carry your Social Security card or other cards that show your Social Security number. Read "Protecting your Social Security Number from Identity Theft"
- Use caution when giving out your personal information. Scam artists "phish" for victims by pretending to be banks, stores, or government agencies. They do this over the phone, in emails, and in postal mail. Most institutions wouldn't ask for your Social Security number (SSN) or other personal information over the phone, and many emphasize that they do not ask for this information. Do not send your SSN or credit card information via email. If you wouldn't feel comfortable putting this information on a postcard, you probably wouldn't want to send it by email either.
- Treat your trash carefully. Shred or destroy papers containing your personal information, including credit card offers and "convenience checks" that you don't use.
- Protect your postal mail. Retrieve mail promptly. Discontinue delivery while out of town.
- Check your bills and bank statements. Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.
- Check your credit reports. Review your credit report at least once a year. Check for changed addresses and fraudulent charges.
- Stop preapproved credit offers. Preapproved credit card offers are a target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists by calling 888-5OPTOUT (888-567-8688).
- Ask questions. Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. If you're not satisfied with the answers, don't give your personal information.
- Protect your computer. Protect personal information on your computer by following good security practices.

- Use strong passwords that cannot be easily guessed.
- Use firewall, antivirus, and antispyware software that you update regularly.
- Download software only from sites you know and trust and only after reading all the terms and conditions.
- Don't click on links in pop-up windows or in spam email.
- Use caution on the Web. When shopping online, check out a website before entering your credit card number or other personal information. Read the privacy policy and take opportunities to opt out of information sharing. Only enter personal information on secure Web pages that encrypt your data in transit. You can often tell if a page is secure if "https" is in the URL or if there is a padlock icon on the browser window.

Steps to Take if Your Data Becomes Compromised or Stolen

Credit Reporting Agencies

If you have reason to believe your personal information has been compromised or stolen, contact the Fraud Department of one of the three major credit bureaus listed below. Individuals whose personal information was involved in this incident can request a free initial (90-day) fraud alert to be placed on their credit files by calling any one of the three major national credit bureaus or completing an online form. Submit one online form request and all three agencies will add the fraud alert.

Equifax
1-888-EQUIFAX
http://www.equifax.com

Experian
888-397-3742
http://www.experian.com

TransUnion
800-680-7289
http://www.transunion.com

When contacting the credit reporting agency, you should request the following:

Instruct them to flag your file with a fraud alert, including a statement that creditors should get your permission before opening any new accounts in your name.

Ask them for copies of your credit report(s). (Credit bureaus must give you a free copy of your report if it is inaccurate because of suspected fraud.) Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. NOTE: To ensure that you are issued free credit reports, we strongly

encourage you to contact the agency's DIRECT LINE (listed above) for reporting fraud. We do not recommend that you order your credit report online.

You may want to ask about the option to freeze your credit. Forty-seven states and the District of Columbia have enacted legislation allowing consumers to place a "security freeze" on their credit reports. A consumer report security freeze limits a consumer reporting agency from releasing a credit report or any information from the report without authorization from the consumer.

Be diligent in following up on your accounts. In the months following an incident, order new copies of your reports to verify your corrections and changes and to make sure no new fraudulent activity has occurred.

If you find that any accounts have been tampered with or opened fraudulently, close them immediately. To ensure that you do not become responsible for any debts or charges, use the ID Theft Affidavit Form developed by the Federal Trade Commission (FTC) to help make your case with creditors.

You may request a free annual credit report, one per year, from AnnualCreditReport.com as recommended by the Federal Trade Commission.

Social Security Administration
SSA Fraud Hotline: 800-269-0271
http://www.ssa.gov/

If you are the victim of a stolen Social Security number, the Social Security Administration (SSA) can provide information on how to report the fraudulent use of your number and how to correct your earnings record. We encourage you to contact the SSA Fraud Hotline immediately once you suspect identity theft.

The website also provides tips on using and securing your Social Security number. Visit the SSA website for advice on keeping your number safe.

- ID Theft Clearinghouse
- 1-877-ID-THEFT (1-877-438-4338)

1. Call the ID Theft Clearinghouse to report identity theft. Counselors will take your complaint and advise you how to deal with the credit-related problems that could result from identity theft.
2. Your Local Law Enforcement
3. It is important that you report identity theft to your local police department as soon as you become aware that you are a victim. Get a copy of the police report; it will assist you when notifying creditors, credit reporting agencies, and if necessary, the Social Security Administration.

Resources:

The following is information related to identity theft and protecting yourself.

- Department of Justice - https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud
- Federal Trade Commission - https://consumer.ftc.gov/features/identity-theft
- National Consumer League's Fraud Center
- Identity Theft Resource Center (888-400-5530)