TITLE: SM1.44 Gramm-Leach-Bliley Act (GLBA) Compliance Policy V1.0

Issue Date: TBD
Effective Date: TBD

Purpose

The Gramm Leach Bliley Act (GLBA) is a law that applies to financial institutions and includes privacy and information security provisions that are designed to protect consumer financial data. This law applies to institutions of higher education, like Ivy Tech Community College (ITCC), and addresses the way that those institutions collect, store, and use student financial records (e.g., records regarding tuition payments and/or financial aid) containing personally identifiable information. ITCC must comply with the GLBA Safeguards Rule (16 CFR 314) which is enforced by the Federal Trade Commission (FTC) for higher education institutions.

Revision History

Date	Version	Revision	Reviser
06/20/2019	1.0	Draft	T. McClelland

Affected Users, Groups, or Systems

All ITCC systems that store, process, transmit, receive, and/or manipulate; and
All ITCC users who have a business need to access and/or manipulate Non-public financial information as defined by the GLBA

Policy

This policy explains the procedure by which Ivy Tech Community College's (ITCC) comprehensive written Information Security Program (the "Program") as mandated by the GLBA Standards for Safeguarding Customer Information Rule shall be maintained and followed. The Program includes the components described below pursuant to which ITCC intends to:

1. Protect the security and confidentiality of customers' nonpublic financial information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

I. Introduction
   A. Federal law requires that financial institutions comply with the Gramm-Leach-Bliley Act and, in so doing, safeguard the confidentiality of nonpublic financial information of its constituents.
   B. This guideline is issued to aid ITCC in drafting Information Security Programs to comply with the Federal Trade Commission's "Standards for Safeguarding Customer Information" Rule promulgated under the authority of the Gramm-Leach-Bliley Act.

II. Scope of Program: Non-public Financial Information
   A. The Program shall apply to any paper or electronic record maintained by an institution that contains nonpublic financial information about an individual or a third party who has a relationship with the institution.
   B. Such nonpublic financial information shall be kept confidential and safeguarded by the institution, its affiliates and service providers pursuant to the provisions of the Program.

III. Requirements of an Information Security Program
   A. Program Coordinator
      1. The institution's Security Information Program must include the designation of a Program Coordinator ("Coordinator") who shall be responsible for implementing the Program.
      2. The Coordinator may be a single employee as designated by the Program.

a. In the alternative, the Program may designate several employees as Coordinators such that one employee serves as the institution's primary Coordinator who works in conjunction with departmental Coordinators who are responsible for oversight of safeguarding records in their departments in accordance with the institution's Program.

3. The Coordinator shall, at a minimum, perform the following duties:
    a. Consult with the appropriate offices to identify units and areas of the institution with access to customers' nonpublic financial information and maintain a list of the same;
    b. Assist the appropriate offices of the institution in identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customers' nonpublic financial information and make certain that appropriate safeguards are designed and implemented in each office and throughout the institution to safeguard the protected data;
    c. Work in conjunction with the institution's contract officer(s) to guarantee that all contracts with third party service providers that have access to and maintain nonpublic financial information of the institution's customers include a provision requiring that the service provider comply with the GLBA safeguarding rule;
    d. Work with responsible institutional officers to develop and deliver adequate training and education for all employees with access to customers' nonpublic financial information; and
    e. Periodically evaluate and monitor the effectiveness of the current safeguards for controlling security risks by periodically verifying that the existing procedures and standards delineated in the Program are adequate.

B. Security and Privacy Risk Assessments
1. The Program shall identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise of such information, and assess the sufficiency of any safeguards in place to control those risks.
2. Risk assessments should include consideration of risks in each office that has access to customers' nonpublic financial information.
3. The GLBA requires that the risk assessment section of the Program must, at a minimum, include consideration of the risks in the following areas:
    a. Employee training and management.
        1. A GLBA employee training program shall be developed by the Coordinator in conjunction with the human resources department and legal counsel, if necessary, for all employees who have access to individuals' nonpublic financial information, such as information technology/systems employees and those employees who use such data as part of their essential job duties.
        2. The training shall occur on a regular basis, as deemed appropriate by the Coordinator, and it shall include education on relevant policies and procedures and other safeguards in place or developed to protect nonpublic financial information.
    b. Safeguards of information systems/technology processing, storage, transmission and disposal (including network and software design).
        1. Programs should include safeguards so that network and software systems are reasonably designed to limit the risk of unauthorized access to nonpublic financial information.
    c. Methods to detect, prevent, and respond to attacks, intrusions, or other system failures.

C. Implementation of Safeguards

1. The Program must include information regarding the design and implementation of information safeguards to control the risks identified through the risk assessment described in the previous component, “B. Security and Privacy Risk Assessments.”
2. The Program shall also include methods to regularly test or otherwise monitor the effectiveness of the safeguarding procedures.
    a. The Program’s monitoring may include technology system checks, reports of access to technology systems, and audits.

D. Oversight of Service Providers and Contracts
1. The GLBA requires institutions to take reasonable steps to select and retain third party service providers that are capable of complying with the GLBA by maintaining appropriate safeguards for the customer information to which they have access.
2. The GLBA requires that the institution’s current and potential service providers that have access to customers’ nonpublic financial information maintain sufficient procedures to detect and respond to security breaches.
3. The Program must include a reference to the institution’s duty to require, by contract, that all applicable third party service providers implement and maintain appropriate GLBA safeguards for customers’ nonpublic financial information.

E. Evaluation and Revision of Program
1. The GLBA mandates that an institution’s Program be subject to periodic review, evaluation, and adjustment.
2. The Program must include a plan by which it will be evaluated on a regular basis and a method to revise the Program, as necessary, for continued effectiveness.

IV. Assessment of the Information Security Program
A. The Coordinator, in conjunction with the appropriate administrators, shall assess the effectiveness of the Program annually.
    1. The Coordinator shall make certain that necessary revisions to the Program are made at the time of the annual review to address any changes in the institutional organization that may affect the implementation and effectiveness of the Program.

V. Publication of the Information Security Program
A. To promote uniform compliance with the Program by all personnel employed by ITCC and to achieve the institution’s duty to safeguard the confidentiality of customers’ nonpublic financial information, the institution shall, at a minimum, display and disseminate the Program in accordance with the institution’s standard distribution methods.
B. The institution’s current Program shall be available upon request for review and copy at all times.

Any questions about this policy and the procedures involved should be sent to infosec-engineer@ivytech.edu

All policies and procedures shall be annually reviewed and maintained by the ITCC Office of Information Technology's Information Security Office and are subject to immediate change without prior user notification based on mitigation of an immediate threat to ITCC technology resources, new industry best practices, regulatory compliance, and/or new technologies. All changes will be reviewed and approved by the ITCC Executive Security Council or in the case of an immediate threat, changes will be reviewed and approved by the ITCC Chief Information Officer.

Approved by:

_____ _____

INSERT NAME **Date**
INSERT ITCC TITLE, Ivy Tech Community College

_____ _____

INSERT NAME **Date**
INSERT ITCC TITLE, Ivy Tech Community College

Appendix A

EU 1.11 Portable Electronic Device (PED) Usage Policy Appropriate Measures

- The PED is to be used for authorized business purposes only.
- Restrict physical access to the PED to only authorized personnel, do not share your PED with anyone including other co-workers, family or friends.
- Must comply with ITCC Computing Standards and Policies
- Never install unauthorized software on the PED.
- Secure the PED prior to leaving area to prevent unauthorized access (screen lock or logout).
- Enable a password/PIN protected screen saver with a short timeout period.
- Must comply with all applicable password policies and procedures.
- Must comply with the applicable Anti-Virus Policy.
- If wireless network access is used, ensure that access is secure by following the Wireless Access Policy.
- If remote access is used to connect to the Ivy Tech Community College network, ensure that the Remote Access Policy (VPN) is followed.
- When left at Ivy Tech Community College premises, ensure that the PED is left on but logged off in order to facilitate after-hours updates.
- Keep all operating system service packs, patches, and application security related hotfixes up to date.
- All protected information should be stored on network servers, unless specifically allowed by the data owner
- Back up ITCC data to ITCC managed file servers
- Ensure that the PED is not left unattended in public places on or off Ivy Tech Community College premises.
- Ensure that view screen are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- Public Wi-Fi hotspots should be avoided if at all possible. Great caution should be used when connecting to non-Ivy Tech Community College operated networks.
- A lost or stolen PED should be reported to the ??????? as soon as possible.

Guidelines

- The physical security of the PED is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks.
- Keep food and drink away from PEDs in order to avoid accidental spills.
- Keep your PED in your possession and within sight whenever possible, just as if it were your wallet or handbag. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended PED.
- Avoid subjecting the PED to extreme temperature changes. Components can become very brittle and easy to break in cold temperatures and can melt or warp in high temperatures. As a general rule, your PED is safest at temperatures that are comfortable for you.
- Keep a note of the make, model, serial number and the Ivy Tech Community College Asset Tag (if Applicable) of your PED. If it is lost or stolen, notify the Police immediately and inform the ???????? as soon as practicable (within hours, not days, please).

Appendix B

EU 1.11 Portable Electronic Device (PED) Usage Policy Technical Controls

Procedure:

All PED's that access and/or store ITCC protected information must be fully encrypted using a Central OIT accepted technologies and methods. Regional IT will be responsible for installing and aiding the user when setting up encryption

Encryption Procedure for Microsoft Windows based Laptops

1. Install Client software (should be baked into the Windows 10 image for all computers)
2. Verify client's AD computer object is in the main OU where the GPOs are linked
3. Add AD computer object to the co-mbam-encrypted-computers security group
4. While on the network, issue a gpupdate /force OR reboot the computer to ensure it pulls the latest GPO changes.
5. A pop-up window will appear on the client, prompting the user to set a boot password. Once entered the encryption process will start\- The password set will be used to boot the computer.
   - Boot passwords are independent of all other types of Ivy Tech Community College authentication and DO NOT sync with other passwords
   - Device must be connected to the domain via internal network or VPN in order to change password and store recovery key in AD.
   - The device may be safely rebooted throughout the encryption process.

Encryption Procedure for Mac OSX based Laptops

1. Choose Apple menu > System Preferences, then click Security & Privacy.
2. Click the FileVault tab.
3. Click the Lock button, then enter an administrator name and password.
4. Click Turn On FileVault.
   - If other users have accounts on your Mac, you might see a message that each user must type in their password before they will be able to unlock the disk. For each user, click the Enable User button and enter the user's password. User accounts that you add after turning on FileVault are automatically enabled.
   - Boot passwords/Passcodes are independent of all other types of Ivy Tech Community College authentication and DO NOT sync with other passwords
   - create a local recovery key and store it ??????????????????????

Encryption Procedure for Red Hat Linux based Laptops

1. Enable Full Disk Encryption using LUKS application
2. Minimum 256-bit AES encryption
3. End user is responsible for encrypting the PED as well as maintain the passphrase and bulk encryption keys

Encryption Procedure for Windows based Tablets

1. Install Client software (should be baked into the Windows 10 image for all computers)
2. Verify client's AD computer object is in the main OU where the GPOs are linked
3. Add AD computer object to the co-mbam-encrypted-computers security group
4. While on the network, issue a gpupdate /force OR reboot the computer to ensure it pulls the latest GPO changes.
5. A pop-up window will appear on the client, prompting the user to set a boot password. Once entered the encryption process will start.
   -The password set will be used to boot the computer.

-Boot passwords are independent of all other types of Ivy Tech Community College authentication and DO NOT sync with other passwords

-Device must be connected to the domain via internal network or VPN in order to change **Procedure for Apple IOS Tablets and Mobile Phones**

1. Enable data protection by configuring a passcode for your device:
2. Tap Settings > General > Passcode.
3. Follow the prompts to create a passcode.
4. After the passcode is set, scroll down to the bottom of the screen and verify that "Data protection is enabled" is visible.

Encryption Procedure for Android based Tablets and Mobile Phones

1. Enable data protection by configuring a passcode for your device:
2. Ensure that the PED is plugged in
3. Tap Settings > Security > Screen Lock > PIN
4. Create a Passcode
5. Tap Settings > Security > Encrypt Phone or Encrypt Tablet