GLBA Safeguards Rule Information Security Program

Compliance Guidance Form

PURPOSE: As mandated by the Federal Trade Commission (FTC) under the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, Wayne State University must develop and maintain an Information Security Program (ISP) to protect the security, confidentiality and integrity of customer information. Customer information in this context includes any nonpublic personally identifiable financial information obtained in connection with a financial product or service, such as student loans.

The Chief Information Officer (CIO) or their delegate coordinates the ISP for the University. Each college or major administrative unit that handles or maintains customer information must have processes and procedures to:

> (a) Identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer data that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of safeguards;
> (b) Design, implement, test and monitor administrative, technical, and physical safeguards to control the identified risks;
> (c) Oversee service providers; and
> (d) Evaluate and adjust processes and procedures at least annually, reporting back to the Chief Information Security Officer & Chief Privacy Officer.

The Compliance Guidance Template must be completed and maintained on file by colleges and major administrative units that must comply with University's Information Security Program.

College or Major Administrative Unit:

Contact Name:
Contact Phone No:
Contact Email Address:
Date:

1. **Describe activities in your college or administrative unit that involve customer information subject to the Safeguards Rule.**

   Examples: Financial aid administration. We collect and maintain financial aid forms, FAFSA forms and associated documentation such as tax forms.

2. **Describe internal and external risks that could jeopardize the security, confidentiality, and integrity of customer information in your care that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. Assess the sufficiency of the administrative, technical, and physical safeguards against those risks, including how the effectiveness of the safeguards' key controls, systems, and procedures are regularly tested or monitored. Include risks and safeguard assessments in the following three areas of operation and in other areas as applicable.**

A. Employee training and other administrative safeguards:

*Example*s

Risk: Employees and management must understand and follow University policies and practices in order to protect customer information from external or internal risks.

Safeguard: All new employees complete training within the first two months of employment. Sufficient tracking mechanisms are in place to notify managers if a new employee has not completed the required modules.

B. Technical and Physical safeguards of the Information systems:

*Example*s

Risk: A risk exists if an employee downloads customer data to a laptop to work at home without following current policies.

Safeguard: We are instituting additional training to ensure that employees follow proper protocols.

C. Detecting, preventing and responding to attacks against University systems:

*Example*s

Risk: Systems must be monitored and tested to ensure customer data is protected from internal or external compromise.

Safeguard: Current C&IT practices include firewalls, anti-virus protection, and activity logs sufficient to control risks. Anomalies in logs are reviewed in order to detect possible security issues.

D. Risks and safeguards in other areas of operations:

E. Methods used to monitor and test the effectiveness of these safeguards:

3. **If any safeguards assessed above are found to be insufficient to manage the risk, explain the additional administrative, technical and physical safeguards that are needed to manage those risks and how you intend to design, implement and regularly monitor and test the effectiveness of these safeguards.**

a. **Administrative Safeguards**:

Examples

Background checks are conducted before hiring employees who will have access to certain customer information.

All new employees sign an agreement to follow University data handling policies and practices.

New employees must complete relevant modules of private data training. Completion is tracked in Learning System.

Breach notification policies are in place.

b. **Technical Safeguards**:

Examples

Employees with access to customer information must use “strong” passwords that must be changed on a regular basis.
Customer information is protected in transit through a Secure Sockets Layer (SSL) or other secure connection.
Follow University C&IT policies and procedures regarding data protection.
End user device encryption is enabled on University laptops.
Firewalls, anti-virus solutions, and patch management are maintained by C&IT.
Systems lock after a period of inactivity and screensaver passwords are required for an inactive system.

c. **Physical Safeguards**:

Examples

Paper records with customer information are stored in a locked cabinet when unattended.
Servers that contain customer information are stored in physically-secure areas.
Follow University policies and procedures regarding data retention and destruction.
Data center environments are secure areas with limited access to those with a need to access the area.

d. **Methods used to monitor and test the effectiveness of these safeguards**:

Examples

Manager follows up with new employees who have not completed training modules.
C&IT has methods in place to regularly monitor and test network security.

4. Third Party Service Providers

Under the Safeguards Rule the University must select and retain only those service providers that maintain appropriate safeguards for customer information as established by the University's Information Security Program. In addition, the University must contractually require service providers to implement and maintain such safeguards. Currently this requirement is managed by Purchasing, who will work with the Office of General Counsel to include appropriate contract language.

Complete the following:

□ We do not use service providers in connection with accounts covered by the Safeguards Rule.

Or:

□ We use service providers in connection with accounts covered by the Safeguards Rule.

And one of the following:

□ All service providers are contractually bound to safeguard data in covered accounts.

Or:

□ Not all service providers are contractually bound to safeguard data in covered accounts. If this box is checked, use the box below to describe the situation and how you plan to comply with this requirement.

5. Annual Information Security Program Review

In an effort to maintain the effectiveness of the University's Information Security Program, colleges and major administrative units must review and submit this form to the Information Security Office on an annual basis or when a material change or other circumstance occurs that may have a material impact on safeguarding customer information in its care.