UNIVERSITY OF MINNESOTA
Driven to Discover℠

GLBA Information Security Program: Compliance Guidance and Certification Form

PURPOSE: As mandated by the Federal Trade Commission (FTC) under the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, the University of Minnesota 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 Controller's Office 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 maintain an inventory of all systems, individuals and equipment that access GLBA protected data;
(B) Identify and assess reasonably foreseeable risks associated with customer data;
(C) Design, implement, test and monitor administrative, technical, and physical safeguards to protect the data;
(D) Oversee service providers; and
(E) Evaluate and adjust processes and procedures at least annually, reporting back to the Controller's Office.

The Compliance Guidance Template must be completed and maintained on file by colleges and major administrative units that must comply with the University's GLBA Information Security Program. Additional guidance is available on the Controller's Office business processes web page, in the GLBA section.

College or Major Administrative Unit:

Department:
Contact Name:
Contact Phone Number:
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. **Inventory**
   Under the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, the University must maintain an inventory of the systems, equipment and individuals that access GLBA protected data. Please confirm that you have reviewed the

shared inventory sheet and edited it to reflect the current inventory for your area. This inventory should be updated throughout the year when changes occur.

Complete the following:

☐ There were no changes to the inventory for my area.

Or:

☐ There were changes to the inventory for my area. (Use the space below to identify the changes to the inventory for your area.)

3. Describe risks that could jeopardize the security or confidentiality of GLBA covered information in your care. Include the safeguards in place to mitigate these risks.

A. Employee training and management:
Examples:
Risk: Employees and management must understand and follow University policies and practices to protect customer information from external or internal risks.
Safeguard: All new employees complete Information Security Awareness training within the first two months of employment. This training is repeated at least annually, or until the employee no longer has access to GLBA covered data. Sufficient tracking mechanisms are in place to notify managers if a new employee has not completed the required training, and managers follow-up to ensure completion. Employee access needs should be reviewed periodically to ensure only those who require access keep it.

B. Information systems:
Examples:
Risk: Employees only access electronic records using University provided and protected devices.
Safeguard: We continually provide GLBA specific training to ensure that employees follow proper protocols.

C. Detecting, preventing, and responding to attacks against University systems:
Examples:
Risk: University systems must be monitored and tested to ensure customer data is protected from internal or external compromise.
Safeguard: Follow the information security standards in the University Information Security Policy. University provided devices and networks are protected and continually monitored to detect possible security issues.

D. Risks and safeguards in other areas of operations:

4. Describe additional administrative, technical, and physical safeguards that are used to manage risks identified above. Describe how you monitor and test the effectiveness of these safeguards.

Administrative Safeguards: *Examples:* Background checks are conducted before hiring employees who will have access to customer information covered by the GLBA Safeguards Rule. All new employees must sign an agreement to follow University data handling policies and practices. New employees must complete Information Security Awareness training within the first two months of employment. Completion is tracked in the University Training Hub. Breach notification policies are in place. (Incident response plan?) **Technical Safeguards**: *Examples:* Employees with access to information covered by the GLBA Safeguards Rule must use "strong" passwords and multi-factor authentication. Employees with access to information covered by the GLBA Safeguards Rule must follow the University Information Security Policy, Standards, and Procedures regarding data protection. Employees only access electronic records using University provided and protected devices.

Physical Safeguards:
Examples:
Paper records with customer information are stored in a locked cabinet or drawer when unattended.
Servers that contain customer information are stored in physically secure areas.
Employees with access to information covered by the GLBA Safeguards Rule must 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.

Methods used to monitor and test the effectiveness of these safeguards:
Examples:
Manager follows up with new employees who have not completed required Information Security Awareness training.
The University has methods in place to regularly monitor and test devices and networks.

5. Third Party Service Providers

Under the Gramm-Leach-Bliley Act (GLBA) 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. Included with this requirement is the periodic assessment of your service providers based on the risk they present and the continued adequacy of their safeguards. Currently this requirement is managed by Purchasing Services for contracts over $50,000. Managers must work with the Office of General Counsel (OGC) to include appropriate contract language in contracts under $50,000.

Complete the following:

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

Or:

☐ We use service providers in connection with accounts covered by the GLBA Safeguards Rule. (Use the space below to name the service providers used in connection with accounts covered by the GLBA 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 space below to describe the situation and how you plan to comply with this requirement.)

6. Record Retention

Under the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, the University must follow certain record retention requirements. The University must adopt controls for securely disposing of customer information no later than two years after the last date that the information was accessed unless retention is otherwise required or necessary for legitimate business purposes.

Complete the following:

☐ We follow the record retention requirements outlined in the GLBA Safeguards Rule including notifying central units when data should be destroyed.

Or:

☐ We have a business reason or superseding regulatory reason for keeping data covered under the GLBA Safeguards Rule for longer than required. (Use the space below to describe the business reason or superseding regulatory reason for keeping the data longer than outlined in the GLBA Safeguards Rule.)

7. Annual Information Security Program Certification

To help maintain the effectiveness of the University's Information Security Program, colleges and major administrative units must complete an annual review and submit this certification form to the ISP Coordinator (Controller's Office). This certification will confirm department/unit compliance with the University's Information Security. Colleges and major administrative units must evaluate and adjust processes and procedures on an ad hoc basis when a material change, or other circumstance occurs that may have a material impact on safeguarding customer information in its care.

Please check all certification statements that apply:

☐ I certify that an annual review has been completed of the risks and safeguards to protect customer information according to the GLBA Information Security Program. Based on this review, or other changes in our unit, any necessary changes have been made to procedures or practices to ensure adequate safeguarding of data in our care.

☐ I certify that my college or major administrative unit is aware of, understands, and complies with standard University policies and practices regarding the protection and appropriate use of data in our care.

Submitted By (print name): _____

Signature: _____

Title: _____

Date: _____