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, Frostburg 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 Office of Information Technology 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 risks associated with customer data;
(b) Design, implement, test and monitor administrative, technical, and physical safeguards to protect the data;
(c) Oversee service providers; and
(d) Evaluate and adjust processes and procedures at least annually, reporting back to the Office of Information Technology.

The Compliance Guidance Template must be completed and maintained on file by colleges and major administrative units that must comply with University's GLBA Information Security Program. Additional guidance is available on the Office of Information Technology website.

College or Major Administrative Unit:

Department:
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 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 employees complete CyberSecurity Awareness training. 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 an employee has not completed the required training, and managers follow-up to ensure completion.

B. Information systems:

Examples:
Risk: Employees only access electronic records using University provided and protected protocols.
Safeguard: We continually provide 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:

3. **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.

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 Acceptable Use Policy, Standards, and Procedures regarding data protection.

Employees only access electronic records using University provided and protected protocols.

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 CyberSecurity Awareness training.

The University has methods in place to regularly monitor and test devices and networks.

4. 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. Currently this requirement is managed by Purchasing, the Office of Information Technology, and the Office of General Counsel (OGC).

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 box 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 box below to describe the situation and how you plan to comply with this requirement.

5. Annual Information Security Program Certification

In an effort to 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 (Office of Information Technology). 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: ____

Title: ____

Date: ____