Frostburg State University

GLBA Information Security Program

Introduction

This document outlines the Frostburg State University (FSU)'s **GLBA Information Security Program**. FSU is required by the Gramm-Leach-Bliley Act (GLBA) and its implementing regulation called the Safeguards Rule (the Rule) (16 CFR Part 314) to develop, implement, and maintain a comprehensive written Information Security Program (ISP) to safeguard customer information in the University's care.

The objectives of the ISP are:

1. To ensure the security and confidentiality of customer information;
2. To protect against anticipated threats or hazards to the security or integrity of such information; and
3. To protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.

Scope

The ISP applies to any record containing nonpublic personal information in paper, electronic or other form, about a student or other third party who has a continuing relationship with the University, where such information *is* ***obtained in connection with the provision of a financial service or product*** *by the University*, and that is maintained by the University or on the University's behalf.

Nonpublic personal information means information:

i. A student or other third party provides in order to obtain a financial service or product from the University,
ii. About a student or other third party resulting from any transaction with the University involving a financial service or product, or
iii. Otherwise obtained about a student or other third party in connection with providing a financial service or product to that person.

For example, nonpublic personal information includes bank account numbers, income and credit histories as well as names, address, and social security numbers associated with financial information. Customer information does not include records obtained in connection with single or isolated financial transactions such as ATM transactions or credit card purchases.

Related Policies and Programs

The University has adopted comprehensive policies and practices to protect the privacy and security of information in its care. The University maintains a mandatory CyberSecurity Awareness training program for all employees. The ISP incorporates by reference the CyberSecurity Awareness Training Policy, the exemplar policies enumerated below and other institutional policies and practices that may be required under federal and state laws and regulations.

- *Information Security Plan*
- *Disclosure of Student & Educational Records*
- *Data Classification Policy and Data Use Standards*
- *Privacy Policy*
- *Acceptable Use of University Computing Resources*

Elements of the Frostburg State University GLBA Information Security Program

1. GLBA Information Security Program Coordinator(s)

The University has designated the Director of IT Security as its ISP Coordinator (Coordinator). The Coordinator may designate others to oversee particular elements of the ISP.

2. Risk Identification and Assessment

Each college or major administrative unit must identify and assess reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. Further, each unit must assess the sufficiency of any safeguards in place to control these risks. This applies to information in any format, whether electronic, paper, or other form.

The Office of Information Technology offers guidance materials to help managers evaluate current data protection practices and assess reasonably anticipated risks in day-to-day operations including:

3. Designing and Implementing Safeguards

Each college or major administrative unit with customer data must design and implement safeguards to control the risks identified in assessments and to regularly test or otherwise monitor the effectiveness of such safeguards.

Testing and monitoring may be accomplished through existing network monitoring, problem escalation procedures, and other data management practices.

4. Overseeing Service Providers

The Office of Information Technology will work with the Office of General Counsel (OGC) to develop and incorporate standard contractual provisions for service providers that will require providers to implement and maintain appropriate safeguards. In conjunction with OGC and Purchasing, the OIT will assist in instituting methods to select and retain only those service providers capable of maintaining appropriate safeguards for customer information to which they will have access.

5. Adjustments to Program

The Coordinator will evaluate and adjust the ISP as needed, based on risk identification and assessment activities and when material changes to the University's operations or other circumstances may have a material impact on the ISP.

Revision History

Version Number	***Date***	***Author***	***Description***
1.0	*June 2021*	*Lori Bennett*	*Initial Document*