PN 3.113

FROSTBURG STATE UNIVERSITY POLICY ON GRAMM-LEACH-BLILEY ACT INFORMATION SECURITY PROGRAM

I. PURPOSE AND APPLICABILITY

This policy describes the University's information security program mandated by the Federal Trade Commission's Safeguard Rule and the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (hereafter referred to collectively as the "GLBA"). This mandate requires institutions of higher education to implement administrative, technical, and physical safeguards for certain types of nonpublic personal financial information.

Some GLBA designated nonpublic personal financial information is protected under other federal or state laws which also require the securing and safeguarding of data. Accordingly, this information security program incorporates and is in addition to institutional policies and procedures required by other federal and state laws and regulations, including, without limitation, the Family Educational Rights and Privacy Act ("FERPA"). When another University policy governs GLBA designated nonpublic personal financial information, the more specific policy will take precedence, provided that the specified safeguards meet the minimum GLBA information security program requirements.

II. DEFINITIONS

A. "GLBA Information Security Program." The administrative, technical, or physical safeguards the University uses to access, collect, distribute, protect, store, use, transmit, dispose of, or otherwise handle Nonpublic Personal Financial Information as required under the Federal Trade Commission's Safeguard Rule and the Gramm-Leach-Bliley Act.

B. "Financial Service." Federal law defines financial services to include, but not be limited to, activities such as the lending of money; investing for others; providing or underwriting insurance; providing financial, investment or economic advisory services; marketing securities, and the like. Examples of Financial Services covered by GLBA include University activities such as offering or processing loans or other types of financial aid to students.

C. "Nonpublic Personal Financial Information." Any personally identifiable information handled or maintained by or on behalf of the University whether in paper, electronic or other form that:
(i) a student or other third party provides in order to obtain a Financial Service from the University;
(ii) is about a student or other third party resulting from any transaction with the University involving a Financial Service; or
(iii) is otherwise obtained about a student or other third party in connection with providing a Financial Service to that person.

Examples of Nonpublic Personal Financial Information includes student financial information received when processing student loans or grants, such as students' or parents' addresses, phone numbers, income and credit histories, social security numbers, and bank account and credit card information.

D. "Service Provider." Any person or entity that receives, maintains, processes, or otherwise is permitted access to Nonpublic Personal Financial Information through its direct provision of services to the University. Examples of Service Providers include loan servicing agents and collection agencies to whom student loan data may be transferred or who may gather it on behalf of the University.

E. "Collection Unit." Any University department or unit that collects Nonpublic Personal Financial Information. Collection units will be identified through procedures established under this policy, and include, but are not limited to, the Office of Information Technology; Bursar's Office; Financial Aid Office; and Office of Admissions.

III. RESPONSIBLE ADMINISTRATOR

A. The University's Chief Information Officer, or designee, (hereinafter referred to as the "Program Officer") is responsible for coordinating and overseeing the GLBA Information Security Program. The Program Officer shall perform these duties in conjunction with representatives from offices identified as Collection Units, including but not limited to, the University's Financial Aid Office, Comptroller's Office, Bursar's Office, and Office of Admissions.

IV. IMPLEMENTATION

As required by federal law, the University's GLBA Information Security Program has the following four components: (i) risk assessments to identify reasonably foreseeable security and privacy risks; (ii)

implementation of information safeguards and monitoring procedures to control the risks identified; (iii) overseeing service providers; and (v) periodic evaluation and adjustment of the Program based upon the results of testing and monitoring as well as changes in operations or operating systems.

A. Conduct a risk identification and assessment. Risk assessment shall include the identification of University Collection Units subject to this Program. Procedures shall be established for identifying and assessing external and internal risks to the security, confidentiality, and integrity of Nonpublic Personal Financial Information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In compliance with federal law, risk assessment shall include, but not be limited to, evaluation of:
(i) Collection Unit employee training regarding procedures and practices relating to access to and use of Nonpublic Personal Financial Information;
(ii) Information systems, including network and software design, information processing, and the storage, transmission and disposal of Nonpublic Personal Financial Information;
(iii) Systems for detecting, preventing, and responding to attacks, intrusions or other system failures.

B. Information Safeguards and Monitoring. Procedures shall be established to ensure that information safeguards for each Collection Unit are designed and implemented to control, monitor, and test risks identified in the assessment set forth above, including but not limited to the areas of employee training, information systems, and managing system failures. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified, as well as the sensitivity of the information provided.

C. Oversee Service Providers. The Program Officer shall work with representatives from each Collection Unit, the Procurement Office, and the Legal Office to ensure reasonable steps are taken to select capable Service Providers and to require Service Providers by specific contract terms and conditions to implement and maintain appropriate GLBA required safeguards.

D. Periodically evaluate and adjust the GLBA Information Security Program. The Program Officer, working with responsible units and offices, will evaluate and adjust the GLBA Information Security Program in light of results of Program testing and monitoring, as well as any material changes to operations or business arrangements, and any other circumstances which may reasonably have an impact on the Program.