Notre Dame of Maryland University
Information Security Policy

The Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq. (the "GLB Act") requires that financial institutions, including colleges and universities, develop, implement and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of the customer information or data at issue. Notre Dame of Maryland University (NDMU) has adopted this Information Security Program in order to comply with the GLB Act and the rules and regulations promulgated thereunder, to continue to ensure the security and confidentiality of customer information and data, to protect against anticipated threats or hazards to the security and confidentiality of such information, and to protect such information against unauthorized access or use which could result in substantial harm to a customer. This Information Security Program applies to customer financial information ("covered data and information") that the University receives in the course of

This Information Security Program has five components:

(i) Designation of departments and employees within those departments, responsible for coordinating the program;

(ii) Implementation of risk assessment procedures to identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information;

(iii) Design and implementation of information safeguards to control the risks identified, monitoring of the effectiveness of the safeguards' key controls, systems and procedures, and updating the safeguards as necessary;

(iv) Overseeing of service providers;

(v) Evaluation and adjustment of the program in response to the results of the monitoring conducted pursuant to the program as well as changes in operations or operating systems;

Notre Dame of Maryland University will designate the Vice President of Finance and Administration as the Security Program Coordinator. The Functional Coordinator will be primarily responsible for the development and implementation of information security policies and procedures of general application throughout NDMU. The Director of IT will be primarily responsible for the development of policies and procedures relating to security in the area of information technology. Together, these two offices will be responsible for implementing this Information Security Program and will work with University personnel to implement the program.

The Coordinator will consult with appropriate NDMU personnel to identify departments within the University with access to Covered Data and Information and shall maintain a list of such departments. For each such department, the Coordinators will ensure that the risk assessments and monitoring, addressed in sections V and VI hereof, are performed and that appropriate safeguards are instituted to control the risks identified.

The Coordinator, in conjunction with appropriate NDMU personnel, will ensure that adequate training and education is provided to all University employees with access to covered data and information.

The Coordinator, in conjunction with appropriate NDMU personnel, will identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Covered Data and Information and evaluate the effectiveness of the safeguards currently in place for controlling these risks. The Coordinator, in conjunction with appropriate NDMU personnel, will conduct risk assessments which shall include, but not be limited to: an assessment of employee training and management; a review of information systems utilized, including network and software design, and information processing, storage, transmission and disposal systems; and a review of the university's procedures for detecting, preventing and responding to attacks, intrusions and system failures.

Risk assessments will include campus-wide risks, as well as those unique to each department having access to Covered Data and Information. Risk assessments will be conducted at least biannually, and more frequently as required.

A. Information Safeguards: The Coordinator, in conjunction with appropriate NDMU personnel, will develop and implement information safeguards designed to control the risks to th the-(th)5e-(p)3ersonn)4el)1,)5 4Tm[13 4a)3ndteg8d)3e)-26egr)-5i)3ty)8)4of)]

(vii) Consulting with software vendors and others to regularly obtain and install updates to correct software vulnerabilities;

(viii) Adherence to the existing program for responding to attempted and actual unauthorized access to covered data and information;

(ix) Maintenance of a disaster recovery program for all servers which contain covered data and information, which program includes the daily backup of electronic information and the storage of tapes at a secure location;

(x) Alerting those with access to Covered Data and Informationof threats to security; and

(xi) Use of complex passwords that are changed periodically.

B. Testing and Monitoring: The Coordinator will take appropriate steps to ensure that monitoring systems are implemented to regularly test and monitor the effectiveness of the information safeguards' key controls, systems and procedures, and that those controls, systems and procedures are updated as necessary. The monitoring performed will include regular review of logs, employment of various system checks and restrictions, and other reasonable measures adequate to ensure that the controls, systems and procedures are functioning properly.

C. Managing System Failures: The Coordinator will take appropriate steps to ensure that the University implements and maintains effective systems to prevent, detect and respond to attacks and intrusions upon the system, as well as system failures. The systems which NDMU currently employs, and will continue to employ, includes utilizing current anti-virus and intrusion detection software, regularly obtaining and installing updates to address software vulnerabilities, utilizing appropriate filtering and/or firewall technologies, backing up data regularly, alerting employees with access to Covered Data and Informationof system failures, installing and maintaining uninterruptible power supplies, and installing and maintaining environmental control systems. NDMU will implement other reasonable measures to protect the integrity and security of its information systems as appropriate.

D. Employee Training and Management: The Coordinator will, in conjunction with appropriate NDMU personnel, identify categories of employees with access to covered data and information. The Coordinator will ensure that appropriate information security training is provided to all new and existing employees who have or will have access to Covered Data and Information. The training provided will cover relevant NDMU policies and procedures relating to access to Covered Data and Information, and, as appropriate, the safeguards in place or developed to protect such data and information. In connection with such training, new and existing employees will be provided copies of those NDMU policies and procedures relating to information security which are relevant to their positions. The Coordinator will ensure that updated versions of NDMU policies and procedures