



Gramm-Leach-Bliley Act Privacy Notice

NORTHWOOD UNIVERSITY

Reviewed March 2011

Discover the leader in you

Developing the future leaders of a global, free-enterprise society.

Table of Contents

Gramm-Leach-Bliley Act.....	1
Gramm-Leach-Bliley Act Notice	3
Information Security Program	3

Gramm-Leach-Bliley Act Notice

In 1999, Congress enacted the Gramm-Leach-Bliley Act (Public Law 106-102). This Act requires that lenders provide certain information to their customers regarding the collection and use of nonpublic personal information.

We disclose nonpublic information to third parties only as necessary to process financial information and as permitted by the Privacy Act of 1974 (FERPA). We do not sell or otherwise make available any information about you to any third parties for marketing purposes.

We protect the security and confidentiality personal information by implementing the following policies and practices. All physical access to the sites where nonpublic personal information is maintained is controlled and monitored. Our computer systems offer a high degree of resistance to tampering and circumvention. These systems limit data access to our staff and contract staff on a “need-to-know” basis, and control individual users’ ability to access and alter records within the systems. All users of these systems are given a unique user ID with personal identifiers. All interactions by individuals with the system are recorded.

Information Security Program

Scope

This document summarizes Northwood University’s (the “Institution’s”) comprehensive written information security program (the “Program”) mandated by the Federal Trade Commission’s Safeguards Rule and the Gramm – Leach – Bliley Act (“GLBA”). In particular, this document describes the Program elements pursuant to which the Institution intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. These practices will impact diverse areas of the University, including but not limited to Business Office, Financial Aid, the

Office of the Registrar, Advancement, Student Services, the Library, and many third party vendors. The Program incorporates by reference the Institution’s policies and procedures enumerated below and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

Designation of Representatives

The Institution’s Director of Information Technology (Bob Wisler) and Associate Dean of Academics (Tina Brisbois) are designated as the Program Officers who shall be responsible for coordinating and overseeing the Program. The Program Officers may designate other

representatives of the Institution to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officers or his or her designees.

Scope of Program

The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Elements of the Program

1. **Risk Identification and Assessment.** The Institution intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and

integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Program, the Program Officers will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

- Employee training and management. While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, the Program Officers will work in cooperation with the Human Resources to develop training and education programs for all employees who have access to covered data. These employees typically fall into three categories: professionals in information technology who have general access to all university data; custodians of data as identified in the data handbook, and those employees who use the data as part of their essential job duties.
 - Information Systems and Information Processing and Disposal. The Program Officers will coordinate with representatives of the Institution's Information Technology to assess the risks to nonpublic financial information associated with the Institution's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the Institution's current policies and procedures relating to Acceptable Use of the Institution's network and network security, as well as backups and the destruction/disposal of retired equipment that may store university data. The Program Officer will also coordinate with the Institution's Information Technology department to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.
 - The Program Officers will also coordinate with appropriate departments in the creation of policies on document retention and destruction for paper records that contain nonpublic financial information.
 - Detecting, Preventing and Responding to Attacks. The Program Officers will coordinate with the Institution's Department of Information Technology and other relevant units to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officers may elect to delegate to a representative of the Department of Information Technology the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.
2. **Designing and Implementing Safeguards.** The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officers will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing monitoring and problem escalation procedures.
 3. **Overseeing Service Providers.** The Program Officers shall coordinate with those responsible for the third party service procurement activities among all departments of university to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the Program Officers will work with the Controller's and Compliance Office to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Vice President of Finance. These standards shall apply to all existing and future contracts entered into with such third party service providers, provided that amendments to

contracts entered into prior to June 24, 2002 are not required to be effective until May 2004.

4. **Evaluation and Revision of the Information Security Program.** The Program Officers are responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program. Processes in relevant offices of the university such as data access procedures and the training program should undergo regular review. The program itself as well as the related data retention policy should be reevaluated annually in order to assure ongoing compliance with existing and future laws and regulations.

Definitions

Covered data and information for the purpose of this policy includes student financial information required to be protected under the Gramm-Leach-Bliley Act (GLB). In addition to this coverage which is required by federal law, Northwood University chooses as a matter of policy to also define covered data and information to include any credit card information received in the course of business by the university, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

Student financial information is that information the university has obtained from a student in the process of offering a financial product or service, or such information provided to the university by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.