2701 Information Security

SECTION:	**INTERNAL CONTROLS**
EFFECTIVE:	**JULY 1, 2010**
REVISED:	
RESPONSIBLE OFFICE:	**VPAF**
APPROVAL:	**VPAF**

PURPOSE

The Gramm-Leach-Bliley Act (GLB) was enacted in 2002 to repeal Depression-era restrictions prohibiting banks from engaging in "risky" financial practices under the Glass-Steagal Act. These restrictions have now been lifted in a way that will permit the creation of "one-stop financial services supermarkets," in which a variety of financial services can be offered.

The law also mandates extensive new privacy protections for consumers. The GLB Act requires financial institutions to take steps to ensure the security and confidentiality of customer records such as names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers.

The GLB Act broadly defines "financial institution" as any institution engaging in the financial activities enumerated under the Bank Holding Company Act of 1956, including "making, acquiring, brokering, or servicing loans" and "collection agency services." Because the Graduate Theological Union participates in financial activities, such as making Federal Perkins Loans, FTC regulations consider it a financial institution for GLB Act Purposes.

The GTU is deemed to be in compliance with the *privacy* provisions of the GLB Act if it is in compliance with the Family Educational Rights and Privacy Act (FERPA). However, the GTU is subject to the provisions of the GLB Act related to the administrative, technical, and physical *safeguarding* of customer information.

POLICY

The designated employee for the coordination and execution of the information security plan is the Vice President for Administration and Finance (VPAF) of the Graduate Theological Union. All correspondence and inquiries should be directed to the VPAF's office.

DEFINITIONS

Customer information means any record containing nonpublic personal information about a student or employee, whether in paper, electronic, or another form. An example would be information that a student provides on the Free Application for Federal Student Aid (FAFSA).

Information security program means the administrative, technical, or physical safeguards the GTU uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle student and employee information.

Service provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its direct provision of services to the GTU.

The following have been identified as relevant areas and responsible offices to be considered when assessing the risks to customer information:

Customer Information	Responsible Office
Employee Records	Personnel Director
Information Systems	Director of Computing Services and Computer Cooperative Systems Administrator
Student Loans	Financial Aid
Admissions	Admissions
Registrar's Office	Registrar
Financial Aid Office	Financial Aid
Accounts Receivable Office	Business Office
Student Housing	Business Office

POLICY STATEMENT

The VPAF's office will coordinate with the Responsible Offices to maintain the information security program. The VPAF's office will provide guidance in complying with all privacy regulations. Each relevant area is responsible for securing customer information in accordance with all privacy guidelines. A written security policy that details the information security policies and processes will be maintained by each relevant area and will be made available to the VPAF's office upon request. In addition, the information technology department will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information.

The Graduate Theological Union will select appropriate service providers that are given access to customer information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to customer information, the evaluation process shall include the ability of the service provider to safeguard customer information. Contracts with service providers shall include the following provisions:

1. an explicit acknowledgment that the contract allows the contract partner access to confidential information;
2. a specific definition of the confidential information being provided;
3. a stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
4. a guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
5. a guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
6. a provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;

7. a stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles the GTU to immediately terminate the contract without penalty;
8. a provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and
9. a provision ensuring that the contract's protective requirements shall survive any termination agreement.

This information security plan shall be evaluated and adjusted in light of relevant circumstances, including changes in the GTU's business arrangements or operations, or as a result of testing and monitoring the safeguards. The GTU shall conduct periodic auditing of each relevant area's compliance.