Boston College
Gramm-Leach-Bliley Act
Information Security Program

I. Purpose

The Gramm-Leach-Bliley Act (GLB), together with an implementing Federal Trade Commission (FTC) "Safeguards Rule," regulate the security and confidentiality of customer information collected or maintained by or on behalf of financial institutions or their affiliates. Because Boston College is classified as a financial institution under GLB, by virtue of processing or servicing student loans, or offering other financial products or services, the University has established this Information Security Program (Program) to assure compliance with GLB and the Safeguards Rule. As required by the Safeguards Rule, the Program is designed to ensure the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

II. Policy Statement

Boston College complies with, and requires its employees and other agents to comply with, all applicable federal, state, and local laws and regulations, as well as University policies and procedures, that govern information security, confidentiality, and privacy. This Information Security Program incorporates, by reference, future and existing University-wide or departmental policies and procedures that address the security and confidentiality of data encompassed by the definition of "covered data," below. Please see University policy 5-100-100, Gramm-Leach-Bliley Act, for additional information.

III. Definitions

Customer information is defined as any record containing nonpublic, personally identifiable financial information, whether in paper, electronic, or other form, that the University obtains from a student, a student's parent(s) or spouse, employee, alumnus, or other third party, in the process of offering a financial product or service; or such information provided to the University by another financial institution; or such information otherwise obtained by the University in connection with providing a financial product or service. Examples of customer information include names; addresses; phone numbers; bank and credit card account numbers; income and credit histories; and social security numbers. In general, the **financial products or services** offered by a college or university include making student loans and other miscellaneous financial services as defined in 12 CFR § 225.28.

Covered data is defined as all information required to be protected under GLB. This includes **customer information**, as well as financial information that the University, as a matter of policy, has included within the scope of this Information Security Program, whether or not such information is covered by GLB. This may include financial and personal identifying information obtained by the University outside of a financial service transaction covered by GLB.

Service providers are defined as all third parties who, in the ordinary course of University business, are provided access to covered data. Examples of service providers include businesses retained to transport and dispose of covered data, collection agencies, and systems support providers.

IV. Information Security Program Components

GLB requires financial institutions to develop, implement, and maintain a comprehensive 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 any customer information it handles. The five components of the program require each institution to: (1) designate one or more employees to coordinate the program; (2) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; (3) ensure that safeguards are employed to control the identified risks, and that the effectiveness of these safeguards is regularly tested and monitored; (4) select service providers that are capable of maintaining appropriate safeguards and require them, by contract, to implement and maintain such safeguards; and (5) evaluate and adjust the information security program based on the results of the testing and monitoring, any material changes to operations, or any other circumstances that have or may have a material impact on the information security program.

1. Information Security Program Committee

   The GLB Information Security Program Committee (Committee) is responsible for implementing and maintaining this Information Security Program. The Committee is comprised of the Director of Computer Policy and Security in Information Technology Services, the Director of Operations and Student Accounts in the Office of Student Services, the Director of the Internal Audit Department, and the Office of the General Counsel. In implementing this Program, the Committee is to work closely with Information Technology Services, the Office of Student Services, the Internal Audit Department, the Office of the General Counsel, the Controller's Office, Human Resources, and all other relevant academic and administrative organizational units.

   The responsibilities of the Committee include, but are not limited to, the following:

   - The Committee is to consult with responsible offices to identify organizational units with access to covered data, ensure that all such units are included within the scope of this Program, and maintain a current listing of these units.

- The Committee is to work with all relevant organizational units to:
  - identify potential and actual risks to the security and privacy of covered data;
  - evaluate the effectiveness of current safeguards for controlling these risks;
  - design and implement additional required safeguards; and
  - regularly monitor and test the Program.

- The Committee is to work with appropriate organizational units to ensure that adequate training and education programs are developed and provided to all employees with access to covered data, and that existing policies and procedures that provide for the security of covered data are reviewed and adequate. The Committee is to make recommendations for revisions to policy, or the development of new policy, as appropriate.

- The Committee is to consult with responsible organizational units to identify service providers with access to covered data, ensure that all such service providers are included within the scope of this Program, and maintain a current listing of these service providers.

- The Committee is to review the Information Security Program, including this and related documents, annually, and make adjustments as needed. The Committee is to maintain a current, written Program and make it available to the University community.

In carrying out these responsibilities, the Committee may require organizational units with substantial access to covered data to develop and implement supplemental information security programs specific to those units, to provide the Committee with copies of the program documents, and to designate responsible individuals to carry out activities necessary to implement this Information Security Program.

2. Risk Identification and Assessment

Under the guidance of the Committee and the Internal Audit Department, organizational units with access to covered data are to take steps to identify and assess internal and external risks to the security, confidentiality, and integrity of that data. At a minimum, this process is to consider the risks to covered data, and the safeguards currently in place to manage those risks, in each relevant area of University operations including: employee management and training; information systems, including network and software design, as well as information processing, storage, transmission, and disposal for both paper and electronic records; and security management, including the prevention, detection, and response to attacks, intrusions, or other systems failures.

The Committee, with the assistance of the Internal Audit Department, is to establish procedures for identifying and assessing risks in each relevant area of the University's operations outlined above. Each affected organizational unit, in consultation with the Committee, is to perform the risk identification and assessment, and is to identify a responsible individual to serve as that unit's contact person with the Committee.

Risk assessments are to include system-wide risks, as well as risks unique to each area with covered data. The Committee is to ensure that risk assessments are conducted at least annually, and more frequently where required.

3. Information Safeguards and Monitoring

The Committee is to verify that organizational units with access to covered data design and implement reasonable safeguards to control identified risks to the security, confidentiality, and integrity of that data, and that the effectiveness of these safeguards is monitored regularly. Such safeguards and monitoring are to include the following:

A. Employee Management and Training
Safeguards for information security are to include the management and training of those individuals with authorized access to covered data. University policy 1-100-025, Professional Standards and Business Conduct -- Use of University Technological and Information Resources, sets forth policies, procedures, and security controls for the security of University information and information resources.

In consultation with Information Technology Services and other responsible organizational units, the Committee is to identify categories of employees and others with access to covered data. The Committee is to work with Human Resources and other responsible organizational units to develop appropriate training and education programs for all affected current and new employees. These programs may be developed as part of the University's Employee Development Program and/or as a component of the New Employee Orientation Program. Training and education may also include brochures, web sites, and other means of increasing awareness of the importance of preserving the confidentiality and security of covered data.

B. Information Systems
Information systems include network and software design, as well as information processing, storage, transmission, and disposal. Each affected organizational unit is to implement and maintain in writing administrative, technical, and physical safeguards to control the risks to information systems, as identified through the unit's risk assessment process. Safeguards are to be designed and implemented in accordance with the nature and scope of a unit's activities and the sensitivity of the covered data to which it has access. The Committee, Information Technology Services, and other responsible organizational units are to work with individual units as requested or appropriate in the design and implementation of safeguards.

Safeguards may include: creating and implementing access limitations; using secure, password-protected systems, and encrypted transmissions within and outside the University, for covered data; regularly obtaining and installing patches to correct software vulnerabilities; prohibiting the storage of covered data on transportable media (floppy drives, zip drives, etc); permanently removing covered data from computers, diskettes, magnetic tapes, hard drives, or other electronic media prior to disposal; storing physical records in a secure area with limited

access; protecting covered data and systems from physical hazards such as fire or water damage; disposing of outdated records under a document disposal policy; and other reasonable measures to secure covered data during the course of its life cycle while in the University's possession or control.

C. Security Management

In consultation with Information Technology Services and other responsible organizational units, the Committee is to develop and implement effective procedures for preventing, detecting, and responding to actual and attempted attacks, intrusions, and other systems failures. Such procedures may include implementing and maintaining current anti-virus software; maintaining appropriate filtering or firewall technologies; regularly obtaining and installing patches to correct software vulnerabilities; imaging documents and shredding paper records; regular data back up and off site storage; implementing incident response plans; and other reasonable measures. The Committee, working with Information Technology Services, is to assist affected organizational units in implementing the appropriate security management procedures.

The Committee may elect to delegate to an appropriate individual in Information Technology Services responsibility for monitoring and disseminating information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the University.

D. Monitoring and Testing

In consultation with Information Technology Services and other responsible organizational units, the Committee is to develop and implement procedures to test and monitor the effectiveness of information security safeguards. Monitoring levels are to be appropriate to the probability and potential impact of the risks identified, as well as the sensitivity of the information involved. Monitoring may include sampling, systems checks, systems access reports, and any other reasonable measures adequate to verify that Information Security Program safeguards, controls, and procedures are effective.

4. Service Providers and Contract Assurances

The Committee, by survey or other reasonable means, is to identify service providers with access to covered data and the organizational units that provide this access. Working with these units, the Committee is to ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for covered data, and are to require service providers, by contract, to implement and maintain such safeguards. Working with the Office of the General Counsel, the Committee is to develop and send to each covered service provider a form letter that requests assurances of GLB compliance. Contracts entered into prior to June 24, 2002, are grandfathered until May 24, 2004. The Office of the General Counsel is to take steps to ensure that all relevant future contracts incorporate a "GLB compliance clause" that requires service providers to implement and maintain safeguards for covered data.

5. Periodic Review and Adjustment of Program

The Committee, working with Information Technology Services and other responsible organizational units, is to evaluate and adjust annually the Information Security Program in light of the results of the testing and monitoring described in paragraph (3)(D), above, as well as any material changes to operations or business arrangements, including changes in technology, the sensitivity of covered data, and the nature of internal and external threats to information security, and any other circumstances that may reasonably impact the Information Security Program.

The Committee, in consultation with the Office of the General Counsel, is to review the Program annually to assure ongoing compliance with GLB and the FTC Safeguards Rule, as well as consistency with other existing and future laws and regulations.