University of Hartford
Information Security Program

The purpose of this document is to formalize the University of Hartford's Information Security Program for the University community and as required by the Federal Trade Commission (FTC) for the administrative, technical, and physical safeguarding of constituent information.

The template used for this program was provided by the National Association of College and University Business Officers (NACUBO) Advisory Report 2003-01 and includes input from the Federal Trade Commission's Commercial Practices Publication on Standards for Safeguarding Customer Information. This Information Security Program is in compliance with the University of Harford Information Technology Security Policy draft dated August 6, 2005.

Background

In order to protect University of Hartford's critical business information and data and to comply with The Financial Services Modernization Act of 1999 (also known as Gramm-Leach-Bliley Act), Information Technology Services (ITS) and the Technology Policy Committee (TPC) recommend the adoption of the University's various practices pertaining to the safeguarding and dissemination of University community information and information about the University's constituents. This Information Security Program builds upon the Information Technology Security Policy, the Responsible Technology Use Policy and other polices and procedures documenting the authorization of access and use of the University's data.

The University's Information Technology Security Policy and related policies and procedures have a broad University community-wide impact, including third-party service providers. The purpose of this document is to define the University's Information Security Program, to provide an outline to assure ongoing compliance with federal regulations related to the program, and to position the University to address future changes in privacy and security regulations.

Financial institutions, including colleges and universities, must meet a general standard in order to comply with the requirements of the Gramm-Leach-Bliley Act (GLB Act) "to 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 any customer information at issue. This Information Security Program was developed to address the needs of the University of Hartford community.

The FTC final rules for safeguarding customer information, to which the University must comply, identify objectives of an institution's Information Security Program. For the purposes of clarity the University's objectives of this Information Security Program are:

- ensure the security and confidentiality of constituent information;
- protect against any anticipated threats or hazards to the security or integrity of such information; and,
- protect against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any constituent.

Information Security Program Specifics

I. The designated group for the review and recommendation of Information Technology Security Policy is the Technology Policy Committee (TPC). The TPC will recommend new policy or policy modifications to the Provost.

II. The designated group for the coordination and execution of the Information Security Program is Information Technology Services (ITS). University senior management will appoint the Information Security Program Coordinator. All correspondence and inquiries concerning this Information Security Program should be directed to Information Security Program Coordinator.

III. The Coordinator will provide assistance to those responsible for risk assessment and safeguards. Because each member of the University of Hartford community is responsible for the security and protection of information resources over which he or she has control, all University community areas must be considered when assessing the risks to constituent information.

The Coordinator will provide guidance in complying with applicable regulations and overall University policies. The Coordinator and the internal auditor will assist University departments as follows:

- Communicate notice of specific Information Security Program requirements.
- Assist in the identification of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of the University's constituent information.
- Assist in the development of departmental information security policies and procedures.
- Assist in the evaluation of the effectiveness of the current safeguards for controlling information security risks.
- Assist in the design and implementation of information security safeguard programs, periodically monitor and test the programs, and coordinate reviews with the internal auditor.

Each major organization unit will conduct an annual information security review with the assistance of the Coordinator and the internal auditor. This includes access validation of all employees in their respective areas that work with data and information that is covered by the GLB Act and other laws and University policies. The senior manager of each major organization units will be responsible for ensuring appropriate information security department-level policies and procedures are documented, current, and employees are knowledgeable about specific procedures for their departments.

The Coordinator will periodically review the University's Disaster Recovery Plan and Business Continuity Plans and report annually on the University's state of readiness.

IV**.** ITS will coordinate with the TPC and various University community areas to maintain the Information Security Program. The TPC will provide guidance in complying with all privacy regulations. Each relevant area is responsible to secure constituent 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 TPC or the internal auditor upon request. Such a policy would include procedures to physically and electronically protect both hard copy and electronic data. In addition, ITS will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic constituent information and that guard against the unauthorized use of such information.

V. All contracts with service providers and technology consultants shall require that the service provider or consultant implement and maintain adequate safeguards for constituent information. A Technology Consultant Contract template has been developed by the Office of the University Secretary to provide for these safeguards.

VI. While supervisors are responsible for ensuring compliance with information security practices and providing department-specific and function-specific training in their areas, ITS and the Banner module owners will provide broad-based training and education programs for employees, as appropriate. This includes the requirement to adhere to appropriate safeguards and confidentiality of protected data.

VII. This Information Security Program shall be evaluated and adjusted as appropriate, including changes in the University's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic Information Security Program audits of each major organization unit may include an annual risk assessment process.

Definitions:

Constituent financial information is information the University has obtained from a constituent (student, employee, parent, alumni, donor, etc.) 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 as defined in 12 CFR § 225.28. A non-exhaustive list of examples of constituent 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.

Constituent information means any record containing non-public personal information or covered data about a constituent of the University (student, employee, alumnus/ae,

donor, parent, trustee, etc.) whether in paper, electronic, or another form, that is handled or maintained by or on behalf of the University.

Covered data and information for the purpose of this program includes constituent financial information required to be protected under the Gramm-Leach-Bliley Act (GLB Act), data required to be protected under the Family Education Rights and Privacy Act (FERPA), data required to be protected under the Health Information Privacy and Accountability Act (HIPAA), and data required to be protected by other Connecticut Law and other Federal Law, as appropriate.

Information Security Program is the title of this document and means the administrative, technical, or physical safeguards the University uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle constituent information.

Non-public personal information is defined as "personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available." (16 CFR Part 313.3(n)(1)). An example would be information that a student provides on the Free Application for Federal Student Aid (FAFSA).

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