Preface

This document outlines the plan to protect critical information and data, and to comply with Federal Law. To this end, the Division of Information Technology (DoIT), in alliance with University Counsel, proposes certain practices in the University information technology environment and institutional information security procedures. The main area to be impacted by these practices is DoIT. Other areas of the University that might be impacted include, but are not limited to: Enrollment Management, Student Life, Student Accounts and Registrar Services, Financial Aid, University Library, and many third-party contractors, including Higher One Card, Food Services and the Bookstore.

This document’s objectives are to:

- define the University's Information Security Plan,
- provide an outline to assure ongoing compliance with Federal regulations related to this Plan, and
- position the University for likely future privacy and security regulations.

Gramm Leach Bliley Requirements

Gramm Leach Bliley mandates that the University:

- appoint an Information Security Plan Coordinator (ISPC),
- conduct a risk assessment of possible security and privacy risks,
- institute a training program for employees that access covered data and information,
- oversee service providers and contracts, and
- evaluate the Information Security Plan and adjust as needed.

Information Security Plan Coordinator (ISPC)

Pace University has designated an Information Security Plan Coordinator (ISPC) who also serves as the University’s Compliance Officer. This person will work closely with University Counsel, the Director of DoIT’s Computer Systems Department, the University’s Chief Technology Officer, and the University’s Chief Information Officer, as well as all relevant Schools and Departments throughout the University.

---

1 The Financial Services Modernization Act of 1999 (also known as Gramm Leach Bliley (Gramm Leach Bliley) 15 U.S.C. §6801
The task of the ISPC includes helping relevant University offices in the following areas:

- identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information;
- evaluate the effectiveness of the current safeguards for controlling these risks; and
- design and implement a safeguards program, and regularly monitor and test this program.

**Risk Assessment and Safeguards**

The ISPC must work with all relevant areas of the University to identify potential and actual risks to security and privacy of information. This will be accomplished by:

- an annual data security review, with guidance from the Information Security Plan Coordinator conducted by each School or Department head, or their designee;
- identification of employees in their respective areas that work with covered data and information by the University’s Vice Presidents;
- a quarterly review of procedures, incidents, and responses will be conducted by the relevant departments of DoIT; and
- publication by DoIT of all relevant materials, except in those cases where publication may likely lead to breaches of security or privacy, for the purpose of educating the University community on network security and privacy issues. (DoIT will assure that these procedures and responses reflect those practiced at other benchmark Universities.)

Those responsible for the identification of internal and external risk assessment are the Directors of DoIT’s Network Services and Computer Systems Departments, the University’s Chief Technology Officer, the University’s Chief Information Officer, and the University Internal Auditor. However, all members of the University community are involved in risk assessment. DoIT and the University Internal Auditor will work in conjunction with relevant University offices to conduct regular risk assessments, including but not limited to the categories listed by Gramm Leach Bliley.

The Division of Information Technology (DoIT) will:

- Monitor the network connections of all computers on the University network to protect its security and integrity. For connections that have direct access to Management Information Systems containing information covered under Gramm Leach Bliley, DoIT will maintain physical location information for each workstation.

- Maintain records and procedures of patching activity. DoIT assures that patches for operating systems or software environments are reasonably current. DoIT will keep current on potential threats to the network and its data. Risk assessments conducted by the University Internal Auditor will conduct risk assessments and regularly update them.

- Develop and maintain, with input from relevant University departments, a data handbook including who is responsible for each covered data field in relevant software systems
(financial, student administration, development, etc.). DoIT and the relevant departments will conduct audits of activity (biannually at a minimum) and will report significant questionable activities.

- Work with relevant offices to develop and maintain a registry of those members of the University community who have access to covered data and information. DoIT, in cooperation with Human Resources, will work to keep this registry rigorously up to date.

- Develop a plan (for the future) to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected (now and in the future) from security risks.

- Assure the physical security of all servers and terminals which contain or have access to covered data and information. DoIT will work with other relevant areas of the University to develop guidelines for physical security of any covered servers in locations outside the central server area.

The University, under the direction of the ISPC, will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures which may expose the University to risks.

The University, under the direction of the ISPC, has begun the process of removing social security numbers as student identifiers. However, one of the largest security risks may be the possible non-standard practices concerning social security numbers, e.g., continued reliance by some University employees on the use of social security numbers. Social security numbers are considered protected information under both Gramm Leach Bliley and the Family Educational Rights and Privacy Act (FERPA). By necessity, student social security numbers still remain in the University student information system.

The University’s Department Director, Computer Systems Department, will conduct an assessment to determine:

- who has access to social security numbers,
- what systems continue to use the social security numbers, and
- in what instances are students being asked to provide a social security number.

This assessment will cover University employees as well as subcontractors such as the Bookstore, Food Services and consortiums.

It is recommended that relevant offices of the University decide whether more extensive background or reference checks or other forms of confirmation are prudent in the hiring process for certain new employees, for example employees handling confidential financial information.

2 20 U.S.C. § 1232g
3 Social Security Numbers are kept both for historical purposes and due to the requirements of 26 U.S.C. § 6050S, the tuition payment credit reporting requirements.
**Employee Training and Education**

Directors and supervisors are ultimately responsible for ensuring compliance with information security practices. However, the ISPC, DoIT and University Counsel will work in cooperation with Human Resources to develop training and education programs for all employees who have access to covered data.

The typical categories of employees are:

- professionals in information technology who have general access to all university data
- custodians of data as identified in the data handbook
- employees who use the data as part of their essential job duties

**Oversight of Service Providers and Contracts**

Gramm Leach Bliley requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Finance and Administration (Purchasing and Contracts), in cooperation with University Counsel, will develop and send form letters to all covered contractors requesting assurances of Gramm Leach Bliley compliance. While contracts entered into prior to June 24, 2003 are grandfathered until May 2004, University Counsel will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with Gramm Leach Bliley.

**Evaluation and Revision of the Information Security Plan**

The Information Security Plan will be subject to biannual review and adjustment as mandated by Gramm Leach Bliley (under the direction of the Information Security Plan Coordinator). Quarterly reviews will occur within DoIT as technology and evolving risks are constantly changing. Quarterly review of processes in other relevant offices of the University such as data access procedures and the training program will also occur regularly. Annual reevaluation of the plan itself, as well as the related data retention policy, should be conducted to assure ongoing compliance with existing and future laws and regulations.

**Definitions**

*Covered data and information* for the purpose of this plan includes student financial information required to be protected under the Gramm Leach Bliley Act (Gramm Leach Bliley). In addition to this coverage, which is required by Federal Law, Pace 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 Gramm Leach Bliley. 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 as defined in 12 CFR § 225.28. 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.

Questions concerning this or any other Information Technology Policy can be directed to doit@pace.edu.