



# **Information Security Policy**

**May 21, 2004  
(Updated April 7, 2008)**

## ***Modifications to the Original Document***

- April 7, 2008 – The “PRINCETON UNIVERSITY INTERNAL” classification was removed from the document footer.
- April 7, 2008 – Two additional Confidential Information Agreement templates were added to the end of the document. The original policy document only included one Confidential Information Addendum specifically designed for financial information protected by the Gramm-Leach-Bliley Act. The two Confidential Information Agreements that have been added to this document have been in common use at the University for the past few years and were designed to protect general University information under two circumstances: (1) where information is being transferred to an external service provider, and (2) where an external service provider or “vendor” has been contracted to support University-based applications and systems.

## ***Table of Contents***

<b>Goal of the Information Security Program .....</b>	<b>1</b>
<b>Purpose of Information Security Policy .....</b>	<b>1</b>
<b>Summary of Personal Responsibilities.....</b>	<b>2</b>
<b>General Principles .....</b>	<b>2</b>
Accountability .....	2
Information Collections and the Responsibilities of Information Guardians.....	2
Responsibilities of Office Heads and Chairs.....	3
User Responsibilities.....	4
Protecting Information Wherever It Is Located .....	4
Diligence Concerning Information Associated with “Identity Theft” .....	4
Limitations on Sharing Personally Identifying Information .....	5
Methods of Distributing Public Information Associated with Individuals .....	6
Exchanging Information via E-Mail or Other Network Facilities .....	6
Discarding Information .....	7
Valid Uses of Aggregate Information.....	7
Subpoenas .....	7
Reporting of Security Breaches or Suspicious Activity .....	7
Awareness Prior to Obtaining Access to Confidential Information .....	8
Additional Requirements for Technology Managers .....	8
<b>Appendix A - Personally Identifying Information That Is Generally Considered Public.....</b>	<b>10</b>
Information about Current and Former Students .....	10
Information about Parents, Guardians and Sponsors .....	11
Information about Faculty and Staff.....	11

<b>Appendix B - Potentially Applicable Laws</b> .....	<b>12</b>
Computer Fraud and Abuse Act (CFAA) .....	12
Electronic Communications Privacy Act (ECPA) .....	12
The Family Educational Rights and Privacy Act (FERPA).....	12
Health Insurance Portability and Accountability Act (HIPAA).....	13
The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (GLBA)) .....	13
The Technology, Education, and Copyright Harmonization Act (TEACH Act).....	13
State Laws .....	14
Subpoenas and Other Compulsory Requests .....	14
Vendor Agreements .....	14
<b>Appendix C – Table of Information Guardians and Designated Contacts</b> .....	<b>15</b>
<b>Appendix D – How Information Guardians Assess Security Requirements</b> .....	<b>18</b>
<b>Appendix E – Summary of End User Responsibilities</b> .....	<b>20</b>
<b>Appendix F – Confidential Information Addendum (Non-Disclosure) for Information     Covered by the Gramm-Leach-Bliley Act</b> .....	<b>22</b>
<b>Appendix G – Confidential Information Agreement (Non-Disclosure) for Data Transferred     to an External Service Provider</b> .....	<b>26</b>
<b>Appendix H – Confidential Information Agreement (Non-Disclosure) for Vendor Support,     either On-Site or via Remote Access</b> .....	<b>30</b>

# Information Security Policy

## ***Goal of the Information Security Program***

The goal of the Information Security Program is to ensure that the...

- Confidentiality,
- Integrity and
- Availability

Of each piece of information owned by or entrusted to Princeton University is protected in a manner that is consistent with...

- The value attributed to it by the University,
- The risk the University is willing to accept and
- The cost the University is willing to pay (in dollars and convenience)

Wherever it resides, i.e.:

- On printed media (e.g., forms, reports, microfilm, microfiche, books),
- On computers,
- On networks,
- On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD),
- In physical storage environments (e.g., offices, filing cabinets, drawers),
- In a person's memory, etc.

## ***Purpose of Information Security Policy***

The purpose of this document is to define the principles to which all University faculty, staff and students must adhere when handling information owned by or entrusted to Princeton University in any form. The principles cover the following areas:

- Defining the confidentiality, integrity and availability requirements for information used to support the University's objectives,
- Ensuring that those requirements are effectively communicated to individuals who come in contact with such information, and
- Using, managing and distributing such information – in any form, electronic or physical - in a manner that is consistent with those requirements.

This policy describes in general terms the Information Security Policy of the University, which is also embodied in various policies developed by the guardians of specific information.

## ***Summary of Personal Responsibilities***

While much of this policy document focuses on our legal obligations and the process of determining and communicating the sensitivity of information owned by or entrusted to the University, it also contains a number of requirements to which anyone who handles such information must adhere. In summary:

- You are responsible for your use or misuse of confidential information.
- You must not in any way divulge, copy, release, sell, loan, review, alter or destroy any information except as properly authorized within the scope of your professional activities.
- You must take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
- You must safeguard any physical key, ID card or computer/network account that allows you to access confidential information. This includes creating computer passwords that are difficult to guess.
- You must render unusable confidential information held on any physical document or computer storage medium (e.g., diskette, CD, magnetic tape, hard disk) that is being discarded.
- You must report any activities that you suspect may compromise confidential information to your immediate supervisor or to the University IT Security Officer.

## ***General Principles***

### **Accountability**

All information gathered and maintained by employees of Princeton University for the purpose of conducting University business is considered institutional information and, as such, each individual who uses, stores, processes, transfers, administers and/or maintains this information is responsible and held accountable for its appropriate use.

### **Information Collections and the Responsibilities of Information Guardians**

University-held information must be protected against unauthorized exposure, tampering, loss and destruction, wherever it is found, in a manner that is consistent with applicable federal and state laws (see Appendix B), and with the information's significance to the University and any individual whose information is collected. Achieving this objective requires that University information be segregated into logical collections (e.g., medical records, employee benefit data, payroll data, undergraduate student records, graduate student records, personal data regarding alumni, financial records), and that each collection be associated with an individual known as an "Information Guardian" who must:

- Define the collection's requirements for confidentiality, integrity and availability (see Appendix D for requirement classifications),
- Convey the collection's requirements in writing to the managers of departments that will have access to the collection,
- Work with Office Heads and Chairs to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information).

The guardian of a logical information collection is typically the head of the department on whose behalf the information is collected or that is most closely associated with such information. A list of Information Guardians and their designated contacts may be found in Appendix C.

Each Information Guardian may designate one or more individuals on his or her staff to perform the above duties. However, the Information Guardian retains ultimate responsibility for their actions.

## **Responsibilities of Office Heads and Chairs**

Office Heads and Chairs are required to:

- Understand the security-related requirements for the information collections used within their respective departments by working with the appropriate Information Guardians and their designates.
- Develop procedures that support the objectives for confidentiality, integrity and availability defined by the Information Guardians and designates, and ensure that those procedures are followed.
- Effectively communicate any restrictions to those who use, administer, process, store or transfer the information in any form, physical or electronic.
- Ensure that each staff member understands his or her information security-related responsibilities and acknowledges that he or she understands and intends to comply with those requirements by having them review the "Protection of Confidential Information – Summary of Responsibilities" document contained in Appendix E.
- Report any evidence that information has been compromised or any suspicious activity that could potentially expose, corrupt or destroy information to the University IT Security Officer.

## **User Responsibilities**

### ***Protecting Information Wherever It Is Located***

Each individual who has access to information owned by or entrusted to the University is expected to know and understand its security requirements and to take measures to protect the information in a manner that is consistent with the requirements defined by its Information Guardian, wherever the information is located, i.e.,

- On printed media (e.g., forms, reports, microfilm, microfiche, books),
- On computers,
- On networks (data and voice),
- On magnetic or optical storage media (e.g., hard drive, diskette, tape, CD),
- In physical storage environments (e.g., offices, filing cabinets, drawers),
- In a person's memory, etc.

If an authorized user is not aware of the security requirements for information to which he or she has access, he or she must provide that information with maximum protection until its requirements can be ascertained.

Any individual who has been given a physical key, ID card or logical identifier (e.g., computer or network account) that enables him or her to access information is responsible for all activities performed by anyone using that key or identifier. Therefore, each individual must be diligent in protecting his or her physical keys and ID cards against theft, and his or her computer and network accounts against unauthorized use. Passwords created for computer and network accounts should be difficult to guess (see "Password Policy" document for guidelines). Furthermore, passwords should never be shared or recorded and stored in a location that is easily accessible by others. Stolen keys and ID cards, and computer and network accounts suspected of being compromised should be reported to the appropriate authorities immediately.

The assignment of a single network or system account to a group of individuals sharing the same password is highly discouraged and may only occur in cases where there is no reasonable, technical alternative.

### ***Diligence Concerning Information Associated with "Identity Theft"***

Identity theft is a serious and growing problem in our society. Anyone who can obtain certain pieces of information about an individual can open credit cards, take out loans, create forged documents or steal assets in the individual's name.

Being sensitive to the identity theft threat, the University requires that extra precaution be taken when collecting, using and storing non-public "personally identifiable" information, such as:

- Social Security Number,
- Date of birth,
- Place of birth,
- Mother's maiden name,
- Credit card numbers,
- Bank account numbers,
- Income tax records, and
- Drivers license numbers.

Collection and use of any of the above pieces of information should be limited to situations where there is legitimate business need and **no reasonable alternative**. Managers must ensure that their employees understand the need to safeguard this information, and that adequate procedures are in place to minimize this risk. Access to such information may only be granted to authorized individuals on a need to know basis.

### ***Limitations on Sharing Personally Identifying Information***

All non-public information gathered and maintained by employees of Princeton University, for the purpose of conducting University business, that personally identifies any living or deceased individual – names and other personal information pertaining to individual students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries, etc. – is considered “confidential” unless otherwise specified by this document or by the appropriate Information Guardian or designate. Such information associated with an individual may only be shared with:

- The individual with respect to whom the information is maintained,
- Persons designated in writing by that individual,
- University employees and representatives (included selected volunteers) who need access to such information for legitimate University business or to support the processing of such information, and who are authorized by the appropriate Information Guardian or designate,
- Governmental agencies to which the University has a legal obligation to provide such information,
- University-contracted organizations (e.g., health insurers, etc.) that:
  - Require such information to deliver their services on behalf of the University,
  - Are authorized by the appropriate Information Guardian, and
  - Are bound by appropriate, non-disclosure agreements. An organization receiving non-public financial information must execute a Confidential Information Agreement (See Appendices F, G and H).

The use of any personally identifying information collected and/or maintained by the University about any living or deceased individual – students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries, etc. – in hard copy or electronic form for any purpose that does not support the University’s objectives (e.g., political or commercial solicitations), is strictly prohibited.

### ***Methods of Distributing Public Information Associated with Individuals***

Some pieces of personally identifiable information are considered public information. These pieces of information are described in Appendix A. The following procedures describe how public information associated with individuals may be shared:

- Directory information, including name, class (students), office address and phone number (faculty and staff) and e-mail address, can be made generally available over the electronic University Web site. The appropriate Information Guardian may deem other elements of information as directory information as well. The campus address and phone number for any student may also be made available in this manner except for those students who have submitted a formal request to the University to keep such information confidential.

*Note – The Registrar and the Dean of the Graduate School maintain official University records of students who have expressly objected to such disclosure.*

- Other public information may be released in response to reasonable requests.

### ***Exchanging Information via E-Mail or Other Network Facilities***

Electronic mail (e-mail) may in some situations be considered an insecure mechanism for exchanging information. The privacy of information contained within e-mail messages can be exposed, especially when either the sender or any of the recipients are off-campus or utilize a wireless network connection. The use of mechanisms that exchange information in a readable form, such as “ftp”, “chat” and “instant messaging”, between on- and off-campus computers also places confidential information at risk.

If information, deemed by its Information Guardian as “confidential” or “highly confidential”, must be exchanged with an individual or entity off-campus using e-mail or any other network facility that transfers data, it must be encrypted using a hardware- or software-based mechanism approved by the Office of Information Technology.

All business-related e-mail containing “confidential” or “highly confidential” information sent to recipients who are not in the “princeton.edu” domain must include the following disclaimer:

*“This electronic communication, including any attached documents, may contain confidential and/or legally privileged information that is intended only for use by the recipient(s) named above. If you have received this communication in error, please notify the sender immediately and delete the communication and any attachments.”*

### ***Discarding Information***

Physical documents containing information that has been classified as “confidential” or “highly confidential” by their Information Guardians and/or designates must be shredded using a University approved device or shredding facility prior to being discarded.

Any computer hard drive or removable magnetic medium, such as a diskette, magnetic tape, Zip disk, etc., that has been used to hold any kind of “confidential” or “highly confidential” information must be electronically “scrubbed” using OIT-approved software prior to being discarded or being transferred to any individual or entity who is not authorized to view such information. On such media, the mere deletion of confidential data is not sufficient as deleted information is still accessible to individuals possessing any of a number of available software tools. Any non-erasable medium, such as a CD, optical disk, etc., that has been used to hold any kind of “confidential” or “highly confidential” information must be physically destroyed before being discarded.

The Facilities Department provides two strategies for shredding materials when the volume to be discarded requires their assistance. Information on office shredders is available from the Purchasing Department, which has equipment recommendations based on projected volume.

### ***Valid Uses of Aggregate Information***

Authorized users may analyze and aggregate institutional data. However, official, published reports that include such aggregate data may only be issued with the review and approval of the appropriate Information Guardian. Similarly, sharing those reports with individuals or organizations for which the reports are not primarily intended requires the permission of the individual or office primarily responsible for the report.

### ***Subpoenas***

Authorized users are reminded that the full range of information collected on any living or deceased individual – students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries, etc. – in hard copy or electronic form may be subpoenaed and entered into the public record of a court case. Appropriate discretion should therefore be exercised in the drafting of any document that will be stored in any University file.

Employees who receive investigative subpoenas, court orders and other compulsory requests from law enforcement agencies that require the disclosure of University held information should contact the Office of General Counsel before taking any action.

### ***Reporting of Security Breaches or Suspicious Activity***

Any member of the University staff who comes across any evidence of information being compromised or who detects any suspicious activity that could potentially expose, corrupt or destroy information must report such information to his or her immediate supervisor or to the University IT Security Officer. No one should take it upon himself or herself to investigate the matter further without the authorization of the University IT Security Officer or General Counsel.

### ***Awareness Prior to Obtaining Access to Confidential Information***

All individuals must review the “Protection of Confidential Information – Summary of Responsibilities” document contained in Appendix E before being given access to confidential information contained within the University’s computer systems, networks and physical facilities.

### **Additional Requirements for Technology Managers**

Technology managers are those individuals who manage computing and network environments where University information is stored, transmitted or processed, such as:

- Computer operating environments (e.g., UNIX, Windows, Macintosh, etc.),
- Database management environments (e.g., Oracle, Sybase, SQL Server, Access, etc.),
- Application environments (e.g., PeopleSoft, Data Mall, etc.),
- Network environments (e.g., electrical, optical, microwave and wireless networks, routers, switches, firewalls, etc.),
- Physical storage facilities (e.g., tape libraries, filing cabinets, etc.),

Technology managers are responsible for ensuring that specific data’s requirements for confidentiality, integrity and availability as defined by the appropriate Information Guardian are being satisfied within their environments. This includes the development of:

- A cohesive architectural policy,
- Product implementation and configuration standards,
- Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Information Guardians, and
- An effective strategy for protecting information against generic threats posed by computer hackers.

## ***Appendices***

## ***Appendix A - Personally Identifying Information That Is Generally Considered Public***

Notwithstanding the general policy of treating personally identifying information as “confidential”, the information listed below describes the circumstances under which certain limited types of personally identifying information may be generally considered by the University to be publicly accessible, except as otherwise noted. Other elements may only be considered public if defined as such by the appropriate Information Guardian.

### **Information about Current and Former Students**

While the Family Educational Rights and Privacy Act (FERPA) generally prohibits the public disclosure of information regarding current and former students that was collected during their enrollment (see Appendix B - Potentially Applicable Laws), FERPA does allow for the public disclosure of certain “Directory Information” that may be shared with the general public, **provided that the given student has not expressly objected to such disclosure.**

*Note – The Registrar and the Dean of the Graduate School maintain official University records of students who have expressly objected to such disclosure.*

The University considers the following to be “Directory Information” that may be shared with the general public:

- Name,
- Local address,
- Local telephone number,
- E-mail address,
- Photo,
- Dates of attendance,
- Major field of study,
- Participation in officially recognized activities, organizations and athletic teams,
- Weight and height of members of athletic teams,
- Degrees and awards,
- Academic institution attended immediately prior to Princeton University.

There are additional data elements, identified within FERPA as being available for public disclosure, which the University has decided to keep confidential or internal as a matter of policy. The following elements must be treated as “confidential”:

- Date of birth,
- Place of birth.

The following must be treated as “internal”:

- Home address,
- Home telephone number.

## **Information about Parents, Guardians and Sponsors**

The following information about parents, guardians and sponsors is considered to be public:

- Name,
- Address (home and local),
- Relationship to student.

## **Information about Faculty and Staff**

The following information about current and former staff and faculty is considered to be public:

- Name,
- Dates of his or her affiliation with the University,
- Office address and phone number,
- E-mail address,
- Title and/or job function.

## ***Appendix B - Potentially Applicable Laws***

As summarized below, a number of federal and state laws may also apply to information collected and maintained by University employees. Please direct questions regarding the applicability of these laws and other potential legal issues to the Office of General Counsel.

### **Computer Fraud and Abuse Act (CFAA)**

Enacted in 1984 (and revised in 1994), the CFAA criminalizes unauthorized access to a “protected computer” with the intent to defraud, obtain any information of value or cause damage to the computer. Under the CFAA, a “protected computer” is defined as a computer that is used in interstate or foreign commerce or communication or that is used by or for a financial institution or the government of the United States. For example, the act of “hacking” into a secure web site from an out-of-state computer may violate the CFAA.

### **Electronic Communications Privacy Act (ECPA)**

Enacted in 1986, the ECPA broadly prohibits (and makes criminal) the unauthorized use or interception of the contents or substance of wire, oral or electronic communications. In addition, the ECPA prohibits unauthorized access to or disclosure of electronically stored communications or information. Such prohibitions may apply to University employees who willfully exceed the scope of their duties or authorizations by accessing certain databases housed within the University system. The ECPA does not, however, prohibit the University from monitoring network usage levels and patterns in order to ensure the proper functioning of its information systems.

### **The Family Educational Rights and Privacy Act (FERPA).**

Enacted in 1974, FERPA (also known as the Buckley Amendment) affords students (or parents if the student is a minor) certain rights with respect to the student’s “education records.” As defined under FERPA, the term “education records” encompasses a broad range of materials and information such as disciplinary, financial and academic records established during a given student’s enrollment and maintained in a variety of University databases and other filing arrangements. In particular, FERPA provides that “education records” and personally identifiable information contained therein may not be released or disclosed (including disclosure by word of mouth) without the written consent of the student (or parents, as the case may be). Violations of FERPA may result not only from the unauthorized disclosure of education records but also from the failure to exercise due care in protecting such records against unauthorized access from outsiders. However, even in the absence of express student (or parental) consent, FERPA permits disclosure of education records to University employees who have a legitimate interest in the student and to outside parties in a variety of circumstances, such as those where public health or safety are at issue.

## **Health Insurance Portability and Accountability Act (HIPAA)**

Enacted in 1996, HIPAA sets national privacy standards for the protection of certain types of health information to the extent such information is electronically transmitted by health plans, health care clearinghouses, and health care providers. The University is subject to HIPAA as a provider of employee group health plans. Accordingly, with respect to such health plans, the University has (a) adopted written privacy procedures describing who has access to protected health information, how such information will be used, and when it may be disclosed; (b) required business associates to protect the privacy of such health information; (c) trained employees in the applicable privacy policies and procedures; and (d) designated a Privacy Officer to be responsible for ensuring that such policies and procedures are followed. HIPAA may also apply to certain research activities such as the collection and use of personally identifying health information from patient populations in clinical settings. Further information regarding compliance with HIPAA is available through the University's Privacy Officer in Risk Management.

## **The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act (GLBA))**

Enacted in 1999, the GLBA requires financial institutions to carefully protect customers' financial information. Universities are "financial institutions" by virtue of their loan servicing and therefore must comply with GLBA provisions. The GLBA has two relevant components: (1) "safeguarding" rules and (2) privacy rules. All personally identifiable financial information from students, parents, and employees must be safeguarded against foreseeable risks of disclosure, intrusion and systems failure. The University has designated information security program managers in the business units that handle financial information, identified risks to the security of financial information, and is developing security programs to protect against risks. As the privacy standards of GLBA must be followed for all non-student financial information, the University is developing a privacy policy to comply with GLBA and will make required privacy notifications to non-student customers whose financial information is obtained. More information is available on the Federal Trade Commission web site:

<http://www.ftc.gov/privacy/glbact/index.html>

## **The Technology, Education, and Copyright Harmonization Act (TEACH Act)**

Enacted in 2002, the TEACH Act relaxes certain copyright restrictions so that accredited, non-profit colleges and universities may use multimedia content for instructional purposes in technology-mediated settings. However, the TEACH Act carries a number of security requirements designed to ensure that digitally transmitted content will be accessible only to students who are properly enrolled in a given course.

## **State Laws**

In addition to the federal laws summarized above, there may be particular state laws that apply to the handling of confidential information. For example, state laws may govern the collection or use of information regarding children, consumers and other groups. Before establishing new practices with regard to the handling of confidential information, University employees are encouraged to consult the Office of General Counsel in order to determine whether specific New Jersey laws apply.

## **Subpoenas and Other Compulsory Requests**

Many of the federal and state laws described above create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies. Employees who receive such compulsory requests should contact the Office of General Counsel before taking any action.

## **Vendor Agreements**

When negotiating contracts with third party vendors, University employees should consider whether such vendors require access to University databases or to other filing systems containing confidential information. Agreements providing third party vendors with access to such information must ensure that the vendor is subject to obligations of confidentiality that will enable the University to comply with its own obligations under the applicable privacy laws. In addition, such vendors should be contractually obligated to implement data protection and security measures that are commensurate with the University's practices. By the same token, University employees must be careful not to disclose confidential information entrusted to their care by an outside party, especially when such information is governed by the terms of a confidentiality agreement or clause with that party.

## ***Appendix C – Table of Information Guardians and Designated Contacts***

As previously stated within this document, the guardian of a logical collection of information is typically the head of the department on whose behalf the information is collected or who is most closely associated with such information. For each assigned information collection, each Information Guardian or individual whom he or she designates is required to:

- Define the collection's requirements for confidentiality, integrity and availability (see Appendix D for requirement classifications),
- Convey the collection's requirements in writing to the managers of departments that will have access to the collection.
- Work with Office Heads and Chairs to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information),

Authorized users are required to understand the security-related requirements associated with the information with which they come into contact.

The table on following page lists information collections, their guardians and designated contacts:

## Table of Information Guardians and Designated Contacts

Information Collections Pertaining to ...	Information Guardian	Designated Contacts
<b><u>Students:</u></b>		
The physical or mental health of any University or Princeton Theological Seminary student.	Executive Director of Health Services	
Applicants – Undergraduates	Dean of Admissions	
Applicants – Graduates	Dean of the Graduate School	
Graduate Students	Dean of the Graduate School	
Undergraduate Students	Registrar	
<b><u>Faculty and Staff:</u></b>		
Work-related injuries for active employees or those on long- and short-term disability.	Executive Director of Health Services	
Applicants – Faculty and related staff	Dean of the Faculty	
Applicants – Staff (non-Dean of Faculty)	Vice President of Human Resources	
Current Faculty and their related staff	Dean of the Faculty	
Staff (non-Dean of Faculty)	Vice President of Human Resources	
Dependents and beneficiaries of Faculty and Staff	Vice President of Human Resources	
<b><u>Alumni and Donors:</u></b>		
Alumni (Personal Information)	Director of the Alumni Council	
Donors	Vice President for Development	

**Table of Information Guardians and Designated Contacts (continued)**

Information Collections Pertaining to ...	Information Guardian	Designated Contacts
<b><u>University Operations:</u></b>		
Academic/Administrative Departments	Head of the appropriate department	
Community Affairs	Vice President of Public Affairs	
Facilities	Vice President of Facilities	
Financial Matters	Treasurer	
<i>Information Security Program Managers for Non-Public Financial Information:</i>		
a. Loans & Receivables	Director/Bursar	Maria Bizzari
b. Undergraduate Financial Aid	Director	Robin Moscato
c. Graduate Financial Support	Assistant Dean	Sandy Mawhinney
d. University Mortgage Program	Mortgage Loan Officer	Lorrie McGough
Law Enforcement and Public Safety	Director of Public Safety	
Legal Matters	General Counsel	
Library Records	University Librarian	

## ***Appendix D – How Information Guardians Assess Security Requirements***

As stated previously, Information Guardians are responsible for assessing the security requirements for each of their assigned information collections across three areas of concern: confidentiality, integrity and availability. To facilitate the assessment process and ensure that these requirements are expressed in a consistent manner across the University, Information Guardians and designates will be required to categorize their information collections using the guidelines described in this section.

The **confidentiality** requirement for an information collection will be expressed in the following terms:

- “**Public**” information can be freely shared with individuals on or off campus without any further authorization by the appropriate Information Guardian or designate.
- “**Internal**” information can be freely shared with members of the University community. Sharing such information with individuals outside of the University community requires authorization by the appropriate Information Guardian or designate.
- “**Departmental**” information can be freely shared with members of the owning department. Sharing such information with individuals outside of the owning department requires authorization by the appropriate Information Guardian or designate.
- “**Confidential**” information can only be shared on a “need to know” basis with individuals who have been authorized by the appropriate Information Guardian or designate, either by their association with specific job functions or explicitly by name.
- “**Highly confidential**” information can only be shared on a “need to know” basis with a limited number of individuals who have been authorized by the appropriate Information Guardian or designate explicitly by name.

The **integrity/availability** requirement for an information collection will be expressed as follows:

- “**Non-critical**” if its unauthorized modification, loss or destruction would cause little more than temporary inconvenience to the user community and support staff, and incur limited recovery costs. Reasonable measures to protect information deemed “non-critical” include storing physical information in locked cabinets and/or office space, using standard access control mechanisms that prevent unauthorized individuals from updating computer-based information, and making regular backup copies.
- “**Critical**” if its unauthorized modification, loss, or destruction through malicious activity, accident or irresponsible management could potentially cause the University to:
  - Suffer significant financial loss or damage to its reputation,
  - Be out of compliance with legislative requirements,
  - Adversely impact its clients, or
  - Miss a legally mandated deadline.

In addition to the protective measures described for information deemed “non-critical”:

- “Critical” information must be verified either visually or against other sources on a regular basis, and
- A business continuity plan to recover “critical” information that has been lost or damaged must be developed, documented, deployed and tested annually.

## ***Appendix E – Summary of End User Responsibilities***

All individuals must review the following “Summary of Responsibilities” document before obtaining access to confidential information contained within the University’s computer systems, networks and physical facilities.

Office Heads and Chairs are responsible for ensuring that each of their staff members who have access to confidential information has reviewed the document and understands his or her responsibilities as they relate to the handling of confidential information.



## **Protection of Confidential Information – Summary of Responsibilities**

---

**Applicable to:** All Individuals with Access to Confidential Princeton University Information

**Effective Date:** May 21, 2004

---

The University maintains information that is sensitive and valuable, and is often protected by Federal and State laws that prohibit its unauthorized use or disclosure. This includes, but is not limited to:

- Personal information about faculty, staff, students, parents, alumni or donors (e.g., social security numbers, dates and places of birth, mother's maiden names, student records, employment records, disciplinary actions, credit card numbers, financial data, medical records, etc.)
- University business information (e.g., financial reports, internal reports and memos, contracts, strategic reports, surveys, etc.)
- Information about or provided by third parties (e.g., information covered by non-disclosure agreements, contracts, business plans, non-public financial data, computer programs, etc.)

The exposure of such information to unauthorized individuals could cause irreparable harm to the University or members of the University community. Thus, you are expected to diligently protect it:

- You may only access the information needed to perform your legitimate duties as a University employee and only after being authorized by the appropriate Information Guardian.
- You may not in any way divulge, copy, release, sell, loan, review, alter or destroy any information except as properly authorized within the scope of your professional activities.
- You must take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
- You must safeguard any physical key, ID card or computer/network account that allows you to access confidential information. This includes creating difficult-to-guess computer passwords.
- You must destroy or render unusable confidential information held on any physical document (e.g., memos, reports, microfilm, microfiche) or computer storage medium (e.g., diskette, CD, magnetic tape, hard disk) that is being discarded.
- You must report any activities that you suspect may compromise confidential information to your immediate supervisor or to the University IT Security Officer.
- Your obligation to protect confidential information does not cease after you leave the University.

Your failure to comply with the above requirements may subject you to disciplinary measures, up to and including termination of employment.

---

***Appendix F – Confidential Information Addendum  
(Non-Disclosure) for Information Covered by the  
Gramm-Leach-Bliley Act***

The form on the following page (or a comparable form approved by the Office of General Counsel) must be signed by an appropriate representative of any external organization before any member of that organization can be given access to University information that is protected by the Gramm-Leach-Bliley Act.



## Confidential Information Addendum for Information Covered by the Gramm-Leach-Bliley Act

This Addendum (“Addendum”) amends and is hereby incorporated into the existing agreement known as \_\_\_\_\_ (“Agreement”), entered into by and between \_\_\_\_\_ (hereinafter “Service Provider”) and Princeton University (hereinafter “Princeton”) on \_\_\_\_\_.

Princeton University and Service Provider mutually agree to modify the Agreement to incorporate the terms of this Addendum to comply with the requirements of the Gramm Leach Bliley Act (“GLB”) dealing with the confidentiality of customer information and the Safeguards Rule. If any conflict exists between the terms of the original Agreement and this Addendum, the terms of this Addendum shall govern.

1. Definitions:

- a. *Covered Data and Information* includes *Student Financial Information* (defined below) required to be protected under the Gramm Leach Bliley Act (GLB), as well as 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.
- b. *Student Financial Information* is that information that the university has obtained from a customer 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 C.F.R. §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.

2. Acknowledgment of Access to Covered Data and Information: Service Provider acknowledges that the Agreement allows the Service Provider access to Covered Data and Information. Specifically, access to the following categories of Covered Data and Information is anticipated under the Agreement:

---



---



---

3. Prohibition on Unauthorized Use or Disclosure of Covered Data and Information: Service Provider agrees to hold the covered data and information in strict confidence. Service Provider shall not use or disclose Covered Data and Information received from or on behalf of Princeton except as permitted or required by the Agreement or this Addendum, as required by law, or as otherwise authorized in writing by Princeton.

4. Safeguard Standard: Service Provider agrees that it will protect the Covered Data and Information it receives from or on behalf of Princeton according to commercially acceptable standards and no less rigorously than it protects its own confidential information.

5. Return or Destruction of Covered Data and Information: Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall:
  - a. Return to Princeton or, if return is not feasible, destroy all Covered Data and Information in whatever form or medium that Service Provider received from or created on behalf of Princeton. This provision shall also apply to all Covered Data and Information that is in the possession of subcontractors or agents of Service Provider. In such case, Service Provider shall retain no copies of such information, including any compilations derived from and allowing identification of Covered Data and Information. Service Provider shall complete such return or destruction as promptly as possible, but not less than thirty (30) days after the effective date of the conclusion of this Agreement. Within such thirty (30) day period, Service Provider shall certify in writing to Princeton that such return or destruction has been completed.
  - b. If Service Provider believes that the return or destruction of Covered Data and Information is not feasible, Service Provider shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction is not feasible, Service Provider shall extend the protections of this Addendum to Covered Data and Information received from or created on behalf of Princeton, and limit further uses and disclosures of such Covered Data and Information, for so long as Service Provider maintains the Covered Data and Information.
6. Term and Termination:
  - a. This Addendum shall take effect upon execution.
  - b. In addition to the rights of the parties established by the underlying Agreement, if Princeton reasonably determines in good faith that Service Provider has materially breached any of its obligations under this Addendum, Princeton, in its sole discretion, shall have the right to:
    - i. exercise any of its rights to reports, access and inspection under this Addendum; and/or
    - ii. require Service Provider to submit to a plan of monitoring and reporting, as Princeton may determine necessary to maintain compliance with this Addendum; and/or
    - iii. provide Service Provider with a fifteen (15) day period to cure the breach; and/or
    - iv. terminate the Agreement immediately if Service Provider has breached a material term of this Addendum and cure is not possible.
  - c. Before exercising any of these options, Princeton shall provide written notice to Service Provider describing the violation and the action it intends to take.
7. Subcontractors and Agents: If Service Provider provides any Covered Data and Information which was received from, or created for, Princeton to a subcontractor or agent, then Service Provider shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Service Provider by this Addendum.
8. Maintenance of the Security of Electronic Information: Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Covered Data and Information received from, or on behalf of, Princeton.
9. Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service Provider shall report to Princeton any use or disclosure of Covered Data and Information not authorized by this Addendum or in writing by Princeton. Service Provider shall make the report

to Princeton not less than one (1) business day after Service Provider learns of such use or disclosure. Service Provider's report shall identify:

- a. the nature of the unauthorized use or disclosure,
- b. the Covered Data and Information used or disclosed,
- c. who made the unauthorized use or received the unauthorized disclosure,
- d. what Service Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and
- e. what corrective action Service Provider has taken or shall take to prevent future similar unauthorized use or disclosure.

Service Provider shall provide such other information, including a written report, as reasonably requested by Princeton.

- 10. Indemnity. Service Provider shall defend and hold Princeton harmless from all claims, liabilities, damages, or judgments involving a third party, including Princeton's costs and attorney fees, which arise as a result of Service Provider's failure to meet any of its obligations under this Addendum.
- 11. Survival. The respective rights and obligations of Service Provider under Section 5 shall survive the termination of this Agreement

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf.

**PRINCETON UNIVERSITY**

**SERVICE PROVIDER:** \_\_\_\_\_

By: \_\_\_\_\_

By: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

***Appendix G – Confidential Information Agreement  
(Non-Disclosure) for Data Transferred to an  
External Service Provider***

The form on the following page (or a comparable form approved by the Office of General Counsel) must be signed by an appropriate representative of any external organization before any member of that organization can obtain non-public University information.



## Confidential Information Agreement for Data Transferred to an External Service Provider

This agreement is hereby entered into, by and between \_\_\_\_\_ (hereinafter "Service Provider") and Princeton University (hereinafter "Princeton") on \_\_\_\_\_. Princeton University and Service Provider mutually agree to the terms of this Agreement whereby Princeton will provide the following data and information:

\_\_\_\_\_

\_\_\_\_\_

to Service Provider for the following purposes:

\_\_\_\_\_

\_\_\_\_\_

Such data and information shall be provided to Service Provider for a defined period, starting upon the execution of this agreement and ending no later than \_\_\_\_\_. If any conflict exists between the terms of this agreement and any prior agreement, the terms of this agreement shall govern.

4. Definition:
  - a. *Covered Data and Information* will include all data and information provided by Princeton to Service Provider specifically for the aforementioned purposes as well as any data and information that Service Provider may derive from such data and information.
5. Acknowledgment of Access to Covered Data and Information: Service Provider acknowledges that the Agreement allows the Service Provider access to Covered Data and Information, and that Covered Data and Information will be used for testing and assessment purposes only.
6. Prohibition on Unauthorized Use or Disclosure of Covered Data and Information: Service Provider agrees to hold the Covered Data and Information in strict confidence. Service Provider shall not use or disclose Covered Data and Information received from or on behalf of Princeton except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by Princeton.
7. Safeguard Standard: Service Provider agrees that it will protect the Covered Data and Information it receives from or on behalf of Princeton according to commercially acceptable standards and no less rigorously than it protects its own Covered Data and Information.
8. Return or Destruction of Covered Data and Information: Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall:
  - a. Return to Princeton or, if return is not feasible, destroy all Covered Data and Information in whatever form or medium that Service Provider received from or created on behalf of Princeton. This provision shall also apply to all Covered Data and Information that is in the possession of subcontractors or agents of Service



shall make the report to Princeton not less than one (1) business day after Service Provider learns of such use or disclosure. Service Provider's report shall identify:

- f. The nature of the unauthorized use or disclosure,
- g. The Covered Data and Information used or disclosed,
- h. Who made the unauthorized use or received the unauthorized disclosure,
- i. What Service Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and
- j. What corrective action Service Provider has taken or shall take to prevent future similar unauthorized use or disclosure.

Service Provider shall provide such other information, including a written report, as reasonably requested by Princeton.

- 15. Indemnity. Service Provider shall defend and hold Princeton harmless from all claims, liabilities, damages, or judgments involving a third party, including Princeton's costs and attorney fees, which arise as a result of Service Provider's failure to meet any of its obligations under this Agreement.
- 16. Survival. The respective rights and obligations of Service Provider under Section 5 shall survive the termination of this Agreement

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

**PRINCETON UNIVERSITY**

**SERVICE PROVIDER: \_\_\_\_\_**

By: \_\_\_\_\_

By: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Signature: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

***Appendix H – Confidential Information Agreement (Non-Disclosure) for Vendor Support, either On-Site or via Remote Access***

The form on the following page (or a comparable form approved by the Office of General Counsel) must be signed by an appropriate representative of any external organization before any member of that organization can gain access to University computer systems.



## Confidential Information Agreement – Vendor Remote or On-Site Support

This agreement is hereby entered into, by and between \_\_\_\_\_  
(hereinafter “Service Organization”) and Princeton University (hereinafter “Princeton”) on  
\_\_\_\_\_.

Princeton University and Service Organization mutually agree to the terms of this Agreement to govern the handling of Princeton data and information by any employee, subcontractor, agent or other individual affiliated with Service Organization (hereinafter “Service Provider”) to which he or she may have access during the course of any work done relating to the maintenance, support or testing of computer software and/or hardware used by Princeton.

If any conflict exists between the terms of this agreement and any prior agreement, the terms of this agreement shall govern.

1. Definitions:

The term Service Provider will refer to any employee, subcontractor, agent or other individual affiliated with Service Organization who has access to Princeton data and information.

The term *Covered Data and Information* will refer to any piece of Princeton data and information to which any Service Provider may have access during the course of his or her performing work relating to the maintenance, support or testing of computer software and/or hardware used by Princeton.

1. Acknowledgment of Access to Covered Data and Information: Service Organization acknowledges that the Agreement allows Service Providers to access Covered Data and Information, and that Covered Data and Information will be used for testing and assessment purposes only.
2. Prohibition on Unauthorized Use or Disclosure of Covered Data and Information: Service Organization agrees that Service Providers will hold the Covered Data and Information in strict confidence. Service Providers shall not use or disclose any piece of Covered Data and Information that may be accessed except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by Princeton.
3. Safeguard Standard: Service Organization agrees that Service Providers will protect the Covered Data and Information according to commercially acceptable standards and no less rigorously than it protects its own Covered Data and Information.
4. Handling of Covered Data and Information: Service Providers will take no intentional action to make a copy of any piece of Covered Data and Information onto any computer or media without prior authorization by manager of the Princeton department responsible for that data. In cases where information is copied onto any media, electronic, magnetic, optical, print, film or otherwise, such Covered Data and Information will be carefully guarded by all Service Providers against unauthorized exposure and, once the issue has been resolved, Service Providers will destroy all copies of Covered Data and Information

either through destructive erasure (magnetic and electronic media) or physical shredding (all other media, such as paper, CDs, DVDs, etc.).

5. Term and Termination:
  - a. This Agreement shall take effect upon execution.
  - b. In addition to the rights of the parties established by the underlying Agreement, if Princeton reasonably determines in good faith that any Service Provider has materially breached any of its obligations under this Agreement, Princeton, in its sole discretion, shall have the right to:
    - i. Exercise any of its rights to reports, access and inspection under this Agreement; and/or
    - ii. Require Service Organization to submit to a plan of monitoring and reporting, as Princeton may determine necessary to maintain compliance with this Agreement; and/or
    - iii. Provide Service Organization with a fifteen (15) day period to cure the breach; and/or
    - iv. Terminate the Agreement immediately if any Service Provider has breached a material term of this Agreement and cure is not possible.
  - c. Before exercising any of these options, Princeton shall provide written notice to Service Organization describing the violation and the action it intends to take.
6. Subcontractors and Agents: If a Service Provider provides any Covered Data and Information which was received from, or created for Princeton to a subcontractor or agent, then Service Organization shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Service Organization by this Agreement.
7. Maintenance of the Security of Electronic Information: Service Organization shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Covered Data and Information received from, or on behalf of, Princeton.
8. Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service Organization shall report to Princeton any use or disclosure of Covered Data and Information not authorized by this Agreement or in writing by Princeton. Service Organization shall make the report to Princeton not less than one (1) business day after Service Provider learns of such use or disclosure. Service Organization's report shall identify:
  - a. The nature of the unauthorized use or disclosure,
  - b. The Covered Data and Information used or disclosed,
  - c. Who made the unauthorized use or received the unauthorized disclosure,
  - d. What Service Organization has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and
  - e. What corrective action Service Organization has taken or shall take to prevent future similar unauthorized use or disclosure.

Service Organization shall provide such other information, including a written report, as reasonably requested by Princeton.

9. Indemnity. Service Organization shall defend and hold Princeton harmless from all claims, liabilities, damages, or judgments involving a third party, including Princeton's costs and attorney fees, which arise as a result of Service Organization's failure to meet any of its obligations under this Agreement.
10. Survival. The respective rights and obligations of Service Organization under Section 5 shall survive the termination of this Agreement

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf.

<b><u>PRINCETON UNIVERSITY</u></b>	<b>SERVICE ORGANIZATION:</b> _____
By: _____	By: _____
Title: _____	Title: _____
Signature: _____	Signature: _____
Date: _____	Date: _____