|  |  |
| --- | --- |
| **Policy Title** | **Information Security Policy** |
| **Responsible Executive** | Vice President of Information Technology and CIO Jay Dominick |
| **Responsible Office** | Office of Information Technology, Operations and Planning |
| **Endorsed by** | Information Security Policy Committee |
| **Contact** | IT Security Officer, Anthony Scaturro; (609) 258-4611 |
| **Effective Date** | May 21, 2004 |
| **Last Update** | November 10, 2009 |

   
A [printer-friendly version](http://www.princeton.edu/oit/it-policies/it-security-policy/Documents/Information_Security_Policy.pdf) (.pdf) of the Information Security Policy is available.

**I.     Policy Statement**

Princeton University possesses information that is sensitive and valuable, e.g., [personally identifiable information](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp0000503ecd50000001f1a12a0c), financial data, building plans, research, and other information considered sensitive. Some information is protected by [federal and state laws](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp00005077334100000143ae511d) or [contractual obligations](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp0000507733410000014394511d) that prohibit its unauthorized use or disclosure. The exposure of sensitive information to unauthorized individuals could cause irreparable harm to the University or members of the University community, and could also subject the University to fines or other government sanctions. Additionally, if University information were tampered with or made unavailable, it could impair the University's ability to do business. The University therefore requires all employees to diligently protect information as appropriate for its [sensitivity level](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity).

**Failure to comply with this policy may subject you to disciplinary measures.  For University employees, failure to comply could result in termination.**

**II.    Policy**

* [Summary of responsibilities](http://www.princeton.edu/oit/it-policies/it-security-policy/#Responsibilities)
* [Information collections and guardians](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians)
* [Information sensitivity levels](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity)
* [Personally Identifiable Information (PII)](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp0000503ecd50000001f1a12a0c)
* [Directory information](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp0000503ecd50000001f1a62a0c)
* [Requirements for computers used to conduct University business](http://www.princeton.edu/oit/it-policies/it-security-policy/#ComputerRequirements)
* [Managing confidential information](http://www.princeton.edu/oit/it-policies/it-security-policy/#ConfidentialInfo)
* [Contractual obligations](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp0000507733410000014394511d)
* [Federal and state laws mandating information protection](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp00005077334100000143ae511d)

**Summary of responsibilities**

**All employees and contractors**

1. You may only access information needed to perform your legitimate duties as a University employee and only when authorized by the appropriate [Information Guardian](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians) or designee. ([University Information Guardians and contacts](http://www.princeton.edu/oit/it-policies/it-security-policy/information-guardians/))
2. You are expected to ascertain and understand the [sensitivity level](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity) of information to which you have access through training, other resources or by consultation with your manager or the [Information Guardian](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians).
3. You may not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by the [Information Guardian](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians) within the scope of your professional activities.
4. You must understand and comply with the University's requirements related to [personally identifiable information](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp0000503ecd50000001f1a12a0c) (PII) .
5. You must adhere to University's [requirements for protecting any computer used to conduct University business](http://www.princeton.edu/oit/it-policies/it-security-policy/#ComputerRequirements) for any computers used to transact University business regardless of the [sensitivity level](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity) of the information held on that system.
6. You must protect the confidentiality, integrity and availability of the University's information as appropriate for the information's [sensitivity level](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity) wherever the information is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.
7. Information deemed Confidential or Highly Confidential under this policy must be handled in accordance with the University's [requirements for protecting Confidential and Highly Confidential information](http://www.princeton.edu/oit/it-policies/it-security-policy/#ConfidentialInfo).
8. You must safeguard any physical key, ID card or computer/network account that allows you to access University information. This includes creating difficult-to-guess computer passwords.
9. You must destroy or render unusable any confidential or highly confidential information contained in any physical document (e.g., memos, reports, microfilm, microfiche) or any electronic, magnetic or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape, diskette) before it is discarded.
10. You must report any activities that you suspect may compromise sensitive information to your supervisor or to the University IT Security Officer.
11. Your obligation to protect sensitive information continues after you leave the University.
12. While many [federal and state laws](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp00005077334100000143ae511d) 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, anyone who receives such compulsory requests should contact the Office of the General Counsel before taking any action.
13. If you are performing work in an office that handles information subject to specific security regulations, you will be required to acknowledge that you have read, understand and agree to comply with the terms of this policy annually.

**Managers and supervisors**

In addition to complying with the requirements listed above for all employees and contractors, managers and supervisors must:

1. Ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the [Information Guardian](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians) and designees, and that those procedures are followed.
2. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.
3. Ensure that each staff member understands his or her information security-related responsibilities.

**Technology managers**

In addition to complying with the policy requirements defined for all employees and contractors, and managers and supervisors, those who manage computing and network environments that capture, store, process and/or transmit University information, are responsible for ensuring that the requirements for confidentiality, integrity and availability as defined by the appropriate [Information Guardian](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians) are being satisfied within their environments. This includes:

1. Understanding the [sensitivity level](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity) of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.
2. Developing, implementing, operating and maintaining a secure technology environment that includes:
   * 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 that adheres to industry-accepted "best practices" for the technology.
3. Ensuring that staff members understand the [sensitivity levels](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity) of the data being handled and the measures used to secure it.

**Information guardians**

In addition to complying with the requirements listed above, Information Guardians are responsible for:

1. Working with the University IT Security Officer and the Office of the General Counsel to understand the restrictions on the access and use of information as defined by [federal and state laws](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp00005077334100000143ae511d) and contractual obligations.
2. Segregating the information for which he or she is responsible into logical groupings, called [information collections](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians),
3. Defining the confidentiality, integrity and availability requirements ([sensitivity level](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity)) for each of his or her [information collections](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians).
4. Conveying in writing the [sensitivity level](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity) of each  [information collection](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians) for which he or she is responsible to the managers of departments that will have access to the collection,
5. Working with department managers to determine what users, groups, roles or job functions will be authorized to access the [information collection](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoCollectionsGuardians) and in what manner (e.g., who can view the information, who can update the information).

**Information collections and 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, the University's contractual obligations, and with the information’s significance to the University as well as any individual whose information is collected. Achieving this objective requires that:

* The information's [sensitivity level](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity) must be defined to convey what level of protection is expected to all employees/agents who are authorized to access the information.
* The individuals who should have access to sensitive information must be identified, either by role or by name.

For purposes of managing information, the University's various types of information must 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). Each collection must be "managed" by an individual known as an “Information Guardian,” who must:

* Define the collection’s [sensitivity level](http://www.princeton.edu/oit/it-policies/it-security-policy/#InfoSensitivity) consistent with this policy,
* Convey the collection’s requirements 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 an 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. 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.

(Princeton University [Information Guardians](http://www.princeton.edu/oit/it-policies/it-security-policy/information-guardians/) and contacts)

**Information sensitivity levels**

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 should categorize their information collections using the levels 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/designee.
* “**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/designee.
* “**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/designee.
* “**Confidential**” information can only be shared on a “need to know” basis with individuals who have been authorized by the appropriate Information Guardian/designee, either by job function or by name.
* “**Highly confidential**” information can only be shared on a “need to know” basis with a limited number of individuals who have been identified by the appropriate Information Guardian/ designee.

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

* Information is “**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.
* Information is “**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 legal/regulatory or contractual requirements,
  + Adversely impact its clients.
* Additional safeguards for "**Critical**" information:
  + “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.

**Personally Identifiable Information (PII)**

Personally Identifiable Information (or “PII,” as used in this Policy) is information that can be used (either alone or in combination with other information) to identify, contact or locate a unique person. Examples include (but are not limited to): name, social security number, address, birth date, telephone number, account numbers, etc.

All Personally Identifiable Information in the possession of Princeton University is considered Confidential unless:

1. The information is designated as “Directory Information” by the appropriate Information Guardian; or
2. The Information Guardian has otherwise authorized its disclosure.

The University requires that the following pieces of PII may not be collected, stored or used except in situations where there is legitimate business need and **no reasonable alternative**:

* 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.

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.

**Directory information**

All Personally Identifiable Information in the possession of Princeton University is considered Confidential unless designated as “Directory Information” by the appropriate Information Guardian or otherwise authorized to be disclosed.

**Directory information for current and former students**

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

Note: The Registrar maintains the record of students who have objected to such disclosure.

The relevant Information Guardians define the following to be “Directory Information” that may be shared:

* Name
* Address (While FERPA permits sharing address information, the Guardians require that it be treated as “Internal” and not disclosed absent compelling reason)
* 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.

**Information about parents or guardians**

The following information about parents/guardians is considered to be “Directory Information”:

* Name
* Address
* Relationship to student.

**Information about faculty and staff**

The following information about current and former staff and faculty is considered to be “Directory Information”:

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

For information about providing references for former employees or faculty, please contact Human Resources or the Dean of the Faculty office.

**Requirements for any computer used to conduct University business**

In order to adequately protect University information systems from compromises, all computers used to conduct University business must be configured using security industry-sanctioned best practices that include but are not limited to the following:

* Configure and use computers in a manner that is compliant with the University's core technology policy, [Princeton University Information Technology Policy](http://www.princeton.edu/itpolicy/).
* Require all computer accounts to have strong passwords as defined by the [University's Password Composition Policy](http://www.princeton.edu/itsecurity/policies/password-policy/).
* Define accounts intended for day-to-day computer use as "general user accounts". Accounts that have administrative privileges must only be used for system setup and maintenance.
* Computers should be configured to "time out" after no more than 20 minutes of inactivity.
* Users should lock or log off their computers before leaving them unattended.
* Ensure that system and application security updates are applied as soon after being released by the vendor as possible;
* Ensure that anti-virus software is installed and is actively protecting the system;
* Limit the services running on University computers to those needed by the computer user to perform his or her assigned tasks;
* Ensure that any system is configured to keep a record of:
  + Who attempted to log into the system (successfully and unsuccessfully) and when,
  + When they logged out,
  + Administrative activity performed,
  + Unsuccessful attempts to access confidential and highly confidential files.

**Managing confidential and/or highly confidential information**

No one may access information that has been classified as Confidential and Highly Confidential without authorization by the appropriate Information Guardian. For information classified as Confidential, such authorization may be granted to individuals by name or to all individuals serving in a specific job function. For information classified as Highly Confidential, access must be authorized for each individual by name.

For information classified as Confidential or Highly Confidential, the following procedural and system-level controls must be in place:

* Access to a Confidential or Highly Confidential information collection may only be granted after receiving permission by the appropriate Information Guardian/designee authorizing such access. The authorization by the appropriate Information Guardian/designee must be documented either by physical or electronic form.
* Departmental procedures must be in place to ensure that all individuals who have access to Confidential or Highly Confidential information are aware of the sensitivity of the information to which they have access, understand their responsibilities to protect that information appropriately, and acknowledge their understanding and intent to comply with this policy.
* Tangible records (paper documents, microfilm, etc.) containing Confidential or Highly Confidential information must be:
  + stored in a locked cabinet or drawer when not in use with access limited to authorized individuals, and
  + physically shredded/destroyed when no longer needed.
* In addition to the [requirements for all computers used to conduct University business](http://www.princeton.edu/oit/it-policies/it-security-policy/#ComputerRequirements), computers that accept, capture, store, transmit or process information classified as Confidential or Highly Confidential must comply with the following requirements:
  + Any piece of Confidential or Highly confidential information that is transmitted across the network must be encrypted using an encryption product and methodology approved by the University IT Security Officer;
  + Laptops, other mobile and external storage devices must:
    - Have the information on their drives encrypted using an encryption product and methodology approved by the University IT Security Officer, except when domestic or international laws prohibit the use of encryption software.
    - Where technically feasible, only be usable by a limited number of specific users and system administrators explicitly authorized by the department that owns the laptop. Note - While traveling to most countries with our standard encryption software on your laptop or mobile device requires no action on your part, there are a few nations to which transporting encryption software without a proper license could violate domestic or international law. **When traveling to any country in this category, both the encryption software and all Confidential and Highly Confidential information must be removed from your system prior to your departure.** To determine whether any country on your itinerary falls into this category, please visit the University's [Travel website](http://www.princeton.edu/travel) and register your trip. For further detail about encryption export and import laws, see "[Important information when traveling internationally](http://www.princeton.edu/itsecurity/services/encryption/travel)."
* Computer servers must:
  + Be secured by a hardware firewall, approved by the University IT Security Officer, that only permits connections with authorized systems using approved protocols.
  + Require anyone who administers system or database software or implements or maintains application software to supplement his or her password with an additional method of authentication, e.g., token, biometric, certificate.

**Contractual obligations**

**Agreements protecting another entity’s information**

University employees are responsible for complying with the terms of contracts or agreements that may limit the ability to disclose confidential information belonging to (or collected on behalf of) another organization. Employees are expected to educate themselves about the limitations imposed on the information to which they have access, including contractual obligations. Some examples of these arrangements are:

* Non-disclosure agreements when research information developed by another institution is shared with the University
* Non-disclosure agreements where the external entity shares pre-release product information,
* End user licensing agreements associated with commercial software, shareware, freeware and other software,
* Contractual obligations with external entities requiring compliance with security standards for an industry or association. The credit and debit card industry requires that we comply with data security standards known as PCI-DSS. Offices that accept credit or debit cards for payment must be in compliance with the [University’s Policy for Handling Credit and Debit Card Payments](http://www.princeton.edu/itsecurity/policies/CreditDebitCardPolicy.pdf).

Additional resources are available at the University’s [Contracting website](http://www.princeton.edu/contracting), or contact the [Office of the General Counsel](http://www.princeton.edu/ogc) (258-2500).

**Agreements protecting University information**

When negotiating contracts with external entities, University employees should consider whether there are any alternatives to giving members of the other organization access to University databases or to other filing systems containing sensitive information.

If such access is necessary, agreements that provide the outside entity with access must ensure that the employees/agents of the entity are required to maintain confidentiality consistent with the University’s obligations and interests. In addition, outside employees/agents should be contractually obligated to implement data protection and security measures that are commensurate with the University’s practices.

Additional resources are available at the University’s [Contracting website](http://www.princeton.edu/contracting), or contact the [Office of the General Counsel](http://www.princeton.edu/ogc) (258-2500).

**Federal and state laws mandating information protection**

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 the General Counsel.

**Key Statutes**

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

This law impacts every office and employee of the University who comes in contact with student records. All University employees are expected to be familiar with the requirements of FERPA and its application to their work. Enacted in 1974, FERPA (also known as the Buckley Amendment) affords students certain rights with respect to the student’s “education records.” As defined by FERPA, the term “education records” encompasses a broad range of materials and information such as disciplinary, financial and academic records created during a given student’s enrollment and maintained by the University, whether in paper form, in databases or other means of storage. In particular, FERPA provides that “education records” and personally identifiable information contained therein may not be disclosed without the written consent of the student. 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 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 imposes obligations on health plans, health care clearinghouses, and health care providers to protect health information when electronically transmitted. As a provider of self-insured group health plans, the University is subject to certain HIPAA requirements. Therefore, certain offices must take steps to appropriately manage contracts with business associates, complete training on applicable privacy policies and procedures and/or complete a confidentiality acknowledgement. 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, Director of Risk Management, or from the Office of the General Counsel.

**The “Red Flags Rule”**

The University’s loan programs are subject to the Federal Trade Commission’s (FTC) Red Flag Rule, which implements sections 114 and 315 of the Fair and Accurate Credit Transaction Act (FACT) of 2003. Compliance requires that the University take steps to protect the identity of those to whom it extends credit and that it develop and implement an identity theft program for new and existing accounts. Adherence is mandatory for “creditors or financial institutions that provide covered accounts”. In addition, the regulation requires users of consumer reports to develop reasonable policies and procedures to react to a notice of an address discrepancy or a fraud alert. This provision applies when credit or background checks are done on prospective employees or when credit checks are requested for new loan applicants or assessment of delinquent account holders. Further information is available from the University’s Identity Theft Prevention Coordinator.

**PCI-DSS**

To reduce their losses due to credit card fraud, five members of the payment card industry, Visa, Master Card, American Express, Discover and JCB, banded together to develop security standards for any organization that accepts, captures, stores, transmits and/or processes credit card information either manually or through an automated system. This set of standards is referred to as the Payment Card Industry’s Data Security Standard, or "PCI-DSS." PCI-DSS is enforced through the contracts that Princeton University, as a merchant account holder, has with our merchant bank, i.e., the financial institution that serves as a liaison between Princeton University merchants and the payment card companies. Penalties for non-compliance can include increased credit card transaction fees, a suspension of credit card privileges, and fines in cases where a credit or debit card account is compromised.

The [University Policy for Accepting and Handling Credit and Debit Card Payments](http://www.princeton.edu/itsecurity/policies/CreditDebitCardPolicy.pdf) was developed to ensure that University personnel who handle credit and/or debit card transactions understand their responsibilities in complying with PCI-DSS.

**Other Statutes and Restrictions**

**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 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 website](http://buseinss.ftc.gov/privacy-and-security/gramm-leach-bliley-act).

**The HITECH Act**

In February 2009, the American Recovery and Reinvestment Act of 2009 (“ARRA”) was enacted. Title XIII of the ARRA, The Health Information Technology for Economic and Clinical Health Act (“HITECH Act” or the “Act”), imposed new federal security breach notice requirements and added numerous new privacy and data security restrictions for covered entities and their business associates under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Princeton, as a sponsor of self-insured group health plans, has certain offices that are required to comply with HIPAA and therefore must comply with the HITECH Act. The HITECH Act created numerous modifications to the HIPAA Privacy and Security Regulations, such as further restricting permitted disclosures and requiring additional record-keeping for disclosures, as well as requiring changes to agreements with business associates. The Act also creates new federal security breach notice laws that apply to all personal information held by a health plan sponsor such as Princeton. These laws require notice to individuals, government agencies, and, in some cases, the media.

**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.

**Access to Information under Vendor Agreements**

When negotiating [contracts](http://www.princeton.edu/oit/it-policies/it-security-policy/#comp0000507733410000014394511d) 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.

**III.   Procedure**

There is no content for this section.

**IV.   Who is Affected by this Policy**

All Princeton University faculty, students, and staff are affected by this policy.

**V.    Definitions**

There is no content for this section.

**VI.   Related Policies**

[University Information Technology Policy](http://www.princeton.edu/itpolicy)

**VII.  Update Log**

May, 21, 2004:  Policy issued.

November 10, 2009:  Policy updated.