PRINCETON UNIVERSITY

Information Security Policy

Policy Title	Information Security Policy
Responsible Executive	Vice President for Information Technology and CIO, Jay Dominick
Responsible Office	Office of Information Technology, Information Security Office
Endorsed by	Data Governance Steering Committee, approved by ECC 11/5/2015
Contact	Chief Information Security Officer, David Sherry
Effective Date	First version: May 21, 2004; current major revision: November 5, 2015
Last Update	March 18, 2016

I. Policy Statement

The purpose of this policy is to provide a security framework that will ensure the protection of University Information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. University Information may be verbal, digital, and/or hardcopy, individually-controlled or shared, stand-alone or networked, used for administration, research, teaching, or other purposes. Standards and procedures related to this Information Security Policy will be developed and published separately.

Failure to comply with this policy may subject you to disciplinary action and to potential penalties described in Section 1.1.7 of *Rights, Rules, Responsibilities*.

II. Who Is Affected By This Policy

The Information Security Policy applies to all University faculty and staff, as well as to students acting on behalf of Princeton University through service on University bodies such as task forces, councils and committees (for example, the Faculty-Student Committee on Discipline). This policy also applies to all other individuals and entities granted use of University Information, including, but not limited to, contractors, temporary employees, and volunteers.

III. Definitions

Authorization – the function of establishing an individual's privilege levels to access and/or handle information.

Availability – ensuring that information is ready and suitable for use.

Confidentiality – ensuring that information is kept in strict privacy.

Integrity – ensuring the accuracy, completeness, and consistency of information.

Unauthorized access – looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need.

University Information – information that Princeton University collects, possesses, or has access to, regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

IV. Policy

Princeton University appropriately secures its information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture.

A. Classification Levels

All University Information is classified into one of four levels based on its sensitivity and the risks associated with disclosure. The classification level determines the security protections that must be used for the information.

When combining information, the classification level of the resulting information must be re-evaluated independently of the source information's classification to manage risks.

Additional requirements for the protection of information in each classification level are identified in the Princeton Information Protection Standards and Procedures.

The classifications levels are:

1. Restricted

The following University Information is classified as Restricted:

- Social security number
- Bank account number
- Driver's license number
- State identity card number
- Credit card number
- Protected health information (as defined by HIPAA)

State and Federal laws require that unauthorized access to certain Restricted information must be reported to the appropriate agency or agencies. **All reporting of this nature to external parties must be done by or in consultation with the Office of the General Counsel (see: Office of General Counsel/Privacy/Information Technology).**

Sharing of Restricted information within the University may be permissible if necessary to meet the University's legitimate business needs. Except as otherwise required by law (or for purposes of sharing between law enforcement entities), no Restricted information may be disclosed to parties outside the University, including contractors, without the proposed recipient's prior written agreement (i) to take appropriate measures to safeguard the confidentiality of the Restricted information; (ii) not to disclose the Restricted information to any other party for any purpose absent the University's prior written consent or a valid court order or subpoena; and (iii) to notify the University in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of Restricted information within the University must comply with University policies including *Rights, Rules and Responsibilities* and Acceptable Use Policy for Princeton University Information Technology and Digital Resources.

2. Confidential

University Information is classified as Confidential if it falls outside the Restricted classification, but is not intended to be shared freely within or outside the University due to its sensitive nature and/or contractual or legal obligations. Examples of Confidential Information include all non-Restricted information contained in personnel files, misconduct and law enforcement investigation records, internal financial data, donor records, and education records (as defined by FERPA).

Sharing of Confidential information may be permissible if necessary to meet the University's legitimate business needs. Unless disclosure is required by law (or for purposes of sharing between law enforcement entities), when disclosing Confidential information to parties outside the University, the proposed recipient must agree (i) to take appropriate measures to safeguard the confidentiality of the information:(ii) not to disclose the information to any other party for any purpose absent the University's prior written consent or a valid court order or subpoena; and (iii) to notify the University in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of Confidential information within the University must comply with University policies including *Rights, Rules and Responsibilities* and Acceptable Use Policy for Princeton University Information Technology and Digital Resources.

3. Unrestricted Within Princeton (UWP)

University Information is classified as Unrestricted Within Princeton (UWP) if it falls outside the Restricted and Confidential classifications, but is not intended to be freely shared outside the University. One example is the Faculty Facebook.

The presumption is that UWP information will remain within Princeton University. However, this information may be shared outside of Princeton if necessary to meet the University's legitimate business needs, and the proposed recipient agrees not to re-disclose the information without the University's consent.

4. Publicly Available

University Information is classified as Publicly Available if it is intended to be made available to anyone inside and outside of Princeton University.

B. Protection, Handling, and Classification of Information

1. Based on its classification, University Information must be appropriately protected from unauthorized access, loss and damage. Specific security requirements for each classification can be found in the Princeton Information Protection Standards and Procedures.
2. Handling of University Information from any source other than Princeton University may require compliance with both this policy and the requirements of the individual or entity that created, provided or controls the information. If you have concerns about your ability to comply, consult the relevant senior executive and the Office of the General Counsel.
3. When deemed appropriate, the level of classification may be increased or additional security requirements imposed beyond what is required by the Information Security Policy and Princeton Information Protection Standards and Procedures.

V. Responsibilities

All Princeton University faculty, staff, students (when acting on behalf of the University through service on University bodies), and others granted use of University Information are expected to:

- Understand the information classification levels defined in the Information Security Policy.
- As appropriate, classify the information for which one is responsible accordingly.
- Access information only as needed to meet legitimate business needs.
- Not divulge, copy, release, sell, loan, alter or destroy any University Information without a valid business purpose and/or authorization.
- Protect the confidentiality, integrity and availability of University Information in a manner consistent with the information's classification level and type.
- Handle information in accordance with the Princeton Information Protection Standards and Procedures and any other applicable University standard or policy.
- Safeguard any physical key, ID card, computer account, or network account that allows one to access University Information.
- Discard media containing Princeton University information in a manner consistent with the information’s classification level, type, and any applicable University retention requirement. This includes information contained in any hard copy document (such as a memo or report) or in any electronic, magnetic or optical storage medium (such as a memory stick, CD, hard disk, magnetic tape, or disk).

- Contact the Office of the General Counsel prior to disclosing information generated by that Office or prior to responding to any litigation or law enforcement subpoenas, court orders, and other information requests from private litigants and government agencies.
- Contact the appropriate University office prior to responding to requests for information from regulatory agencies, inspectors, examiners, and/or auditors.

VI. Related Princeton Policies, Procedures, Standards, and Templates

Rights, Rules, Responsibilities

Acceptable Use Policy for Princeton University Information Technology and Digital Resources

University Policy for Accepting and Handling Credit and Debit Card Payments

Policy on Export Controls

Research Data Security Guidelines [http://www.princeton.edu/ria/human-research-protection/data/]

Red Flags Procedures Under Princeton University's Identity Theft Prevention Program

Procedure for Responding to a Possible Exposure of Sensitive University Data

Princeton Information Protection Standards and Procedures [http://protectourinfo.princeton.edu]

Confidentiality Information Agreement Template

VII. Policy Review

At a minimum, the Information Security Policy will be reviewed every 24 months.