Information Security Policy


Effective Date: February 12, 2010

Policy Statement

Boston University recognizes that in certain instances it must collect, store and use Sensitive Information relating to its students, employees and individuals associated with the University such as Social Security Numbers, drivers' license numbers and financial account numbers. The University is dedicated to collecting, handling, storing and using Sensitive Information properly and securely.

Reason for Policy / Implication Statement

Boston University is committed to collecting, handling, storing and using Sensitive Information properly and securely. This Policy establishes an Information Security Program to create administrative, technical and physical safeguards for the protection of Sensitive Information throughout the University. The purpose of this Program is to comply with applicable laws and to:

1. Provide a framework for comprehensive stewardship of Sensitive Information;
2. Increase awareness of the confidential nature of Social Security Numbers and other Sensitive Information;
3. Eliminate unnecessary collection and use of Sensitive Information;
4. Protect against anticipated threats or hazards to the security or integrity of Sensitive Information; and
5. Protect against unauthorized access to or use of Sensitive Information in a manner that creates a substantial risk of identity theft or fraud.

University Roles Affected By Policy

Any member of the University community, including all faculty, staff and students, who has access to University records that contain information covered by this Policy must comply with this Policy.
Definitions

**Breach of Security:** the unauthorized acquisition or use of Sensitive Information that creates a substantial risk of identity theft or other harm. This definition includes the unauthorized acquisition or use of encrypted electronic Sensitive Information where the confidential process or key has been compromised.

**Electronic:** relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

**Employee:** includes all Boston University faculty, staff and students, whether compensated or not, as well as volunteers, trainees, visiting researchers, or any other individual who provides services in collaboration with or under the control of Boston University faculty staff, or students and who, in connection with such services, has access to University records that contain Sensitive Information.

**Encryption:** transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key.

**Record:** any material upon which written, drawn, spoken, visual or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics that contain Sensitive Information. The term Record includes both paper and electronic files.

**Sensitive Information:** Information that has been determined by the Information Security Program Director to require privacy and security controls.

Responsibilities

The University Information Security Program Director is responsible for the administration of this Policy and the Information Security Program across departments and units that maintain Records in any format. The University Information Security Program Director shall oversee, with the assistance of the Information Security Program Committee, the administration of this Policy, including developing procedures concerning the review, oversight and governance of this Policy, and including any necessary training. Each unit manager or department head is responsible for administering this Policy within his or her unit or department consistent with the Information Security Guidelines and other procedures developed by the Director, the Committee, or appropriate University officials. University Employees may request, collect, store or use Sensitive Information only as permitted by this Policy, applicable Information Security Guidelines and practices required by his or her unit or department.
I. Information Security Program Director and Committee

A. University Information Security Program Director

The University Information Security Program Director shall be determined by the President, or the President’s designated representative, and shall be initially the Senior Associate Vice President for Financial Affairs. The Director shall, in consultation with the Security Committee, maintain a list of categories of information that will be included within the definition of Sensitive Information and prescribe appropriate levels of protection, as set forth below. The Director may consult with the Information Security Program Committee and charge that Committee with responsibilities concerning the administration and review of this Policy.

The Director may assign responsibility for developing more specific Information Security Guidelines to appropriate central University offices with responsibility for and expertise concerning the collection, use, storage and disposal of particular types of Sensitive Information. The Director shall provide a mechanism for reporting any suspected Breach of Security and shall respond to any reported Breach of Security as outlined below.

B. University Information Security Program Committee

The University’s Information Security Program Director shall convene an Information Security Program Committee to assist with the administration of this Policy and to help ensure compliance. In addition, the Committee may advise University offices charged with the development of Information Security Guidelines and review Information Security Guidelines. The Committee may include representatives from the offices of Financial Affairs, Information Services & Technology, Student Affairs, Development, Human Resources, Internal Audit, Research Compliance, General Counsel; and any other school, college, office or department as the Director, in consultation with the Executive Vice President and Provosts, deems appropriate.

C. Information Security Guidelines

The Information Security Program Director, in consultation with appropriate members of the Information Security Program Committee, shall identify central departments within the University that have responsibility for and expertise concerning the collection, use, storage and disposal of Sensitive Information and, as appropriate, shall charge those offices with development of specific Information Security Guidelines. The Information Security Guidelines shall specify administrative, technical and physical safeguards for the protection
of Sensitive Information. The Committee may review and the Director shall approve Information Security Guidelines.

D. Training

The Director or the Director’s designee, together with the Committee, shall develop a training program for Employees who will have access to Sensitive Information. The Director, in consultation with Human Resources and the Office of the Provost, will ensure that new Employees with access to Sensitive Information complete the training program concerning the University’s Information Security Program.

E. Vendors and Service Providers

The Director or the Director’s designee, together with the Committee, shall, as appropriate, maintain a list of University vendors, service providers or any other third-party to whom the University provides Sensitive Information. The Director or the Director’s designee, together with the Committee, will confirm that units and departments have taken reasonable steps to ensure that those vendors, service providers and third-parties are applying protective security measures to the Sensitive Information that are at least as stringent as those required by law. The Director shall require disclosure of vendors, service providers or any other third-party to whom the University provides other types of Sensitive Information, as appropriate.

F. Program Review

At least annually the Director, together with the Committee, shall review the Information Security Program and the Information Security Guidelines. During the course of the review, the Director and the Committee shall review any Breach of Security that occurred, including the results of any investigation and the University’s response to any Breach, as well as any internal or external risks to security identified by any unit or department or any other source. After the conclusion of the annual review, a summary report will be provided to the President, Executive Vice President and Provosts, or their designees.

II. Security Breach Response Team

The Director shall review any suspected Breach of Security together with representatives from Information Services & Technology and the Boston University Police Department, if appropriate, and the Office of the General Counsel. If the Director concludes that a Breach of Security has occurred, the Director shall convene a Security Breach Response Team to assess any reported Breach of Security and manage the University’s response. The Response Team may include representatives from the offices of the Executive Vice President, Information Services & Technology, Human Resources, Boston
University Police Department, Government and Community Affairs, Internal Audit, Marketing and Communications, Office of the General Counsel, and any other office, department, school or college as the Information Security Program Director, in consultation with the Executive Vice President and the Provosts, deems appropriate. The Security Breach Response Team will coordinate an investigation of the Breach, as appropriate, and the University’s response.

After the conclusion of any investigation, the Response Team may make recommendations concerning the University’s Information Security Program and the Information Security Guidelines. The Director and the Committee shall review any recommendations of the Response Team. A copy of the recommendations and any summary report of the investigation will be provided to the President, Executive Vice President and Provosts, or their designees.

**Related Documents & Policies**

- List of Personal Information
- Personal Information Protection Program
- FERPA Policy (http://www.bu.edu/reg/ferpa/ferpa-policy.html)
- HIPAA Policy (http://www.bumc.bu.edu/hipaa/)

**Contacts**

Christopher Goss  
Assistant to the Executive Vice President  
Boston University  
One Silber Way  
Boston, MA 02215  
(617) 353-6500  
cgoss@bu.edu