Effective Date: **February 12, 2010** Revised: **April 12, 2023**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Information Security Policy

RESPONSIBLE OFFICE

Office of the Vice President Information Services and Technology

Reviewed: April 2023 (BY CSIS GOVERNANCE)

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 as well as certain types of research data. 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 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, fraud or other misuse of the data.

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 Sensitive 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, volunteers, trainees, visiting researchers, and any other individual who provides services to Boston University, whether compensated or not, 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 material.

Sensitive Information: Information that is designated as Restricted Use, Confidential or Internal Data under the Data Protection Standards.

Responsibilities

The University's Chief Information Security Officer 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's Chief Information Security Officer shall oversee, with the assistance of the Common Services and Information Security Committee (the "Committee"), the administration of this Policy, including developing procedures concerning the review, oversight and governance of this Policy, and including any necessary training. University Employees may request, collect, store or use Sensitive Information only as permitted by this Policy, the Data Protection Standards and practices required by his or her unit or department.

Every member of the University community should strive to minimize the collection, handling, storage and use of Sensitive Data. Only those who have a legitimate business need to access Sensitive Information should do so, and for as limited as time as possible. Minimize or eliminate the collection, handling, storage and use of Sensitive Data whenever and wherever possible.

Procedures

I. Information Security Program Director and Committee

A. University Chief Information Security Officer

The University's Chief Information Security Officer shall, in consultation with the Committee, maintain a list of categories of information that will be included within the definition of Sensitive Information and prescribe appropriate levels of protection in a series of procedures collectively known as the Data Protection Standards. The Chief Information Security Officer may consult with the Committee and charge the Committee with responsibilities concerning the administration and review of this Policy.

The Chief Information Security Officer 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 Common Services and Information Security Committee

The Chief Information Security Officer shall convene a Common Services and Information Security 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.

C. Data Protection Standards

The Chief Information Security Officer, in consultation with the Committee, shall identify categories of Sensitive Information and the appropriate safeguards required to protect each category. The Data Protection Standards shall specify administrative, technical and physical safeguards for the protection of Sensitive Information. The Committee may review, and the Chief Information Security Officer shall approve the Data Protection Standards.

D. Training

The Chief Information Security Officer or the Chief Information Security Officer ’s designee, together with the Committee, shall develop a training program for Employees who will have access to Sensitive Information.

E. Vendors and Service Providers

The Chief Information Security Officer or the Chief Information Security Officer ’s designee, together with the Committee, may recommend that University vendors, service providers or any other third-party to whom the University provides Sensitive Information be required to meet appropriate criteria or agree to appropriate contract terms before being granted access to Sensitive Data.

F. Program Review

At least annually the Chief Information Security Officer, together with the Committee, shall review the Information Security Program and the Data Protection Standards. During the course of the review, the Director and the Committee shall review any Breach of Security that is reported to outside authorities, including the results of any investigation and the University’s

response to any Breach.

II. Security Breach Response Team

The Chief Information Security Officer shall review any suspected Breach of Security of Sensitive Information as specified in the Data Breach Response and Management Plan.

Related Documents & Policies:

Data Protection Standards
Data Breach Response and Management Plan (maintained by Information Security)
FERPA Policy
HIPAA Policy

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related Policies

- Data Protection Standards
- Sensitive Data Incident Response
- FERPA Policy
- HIPPA Policies
  - HIPAA Policies for BU Health Plans Manual – Privacy and Security of Protected Health Information for BU Health Plans
  - HIPAA Policy Manual – Privacy and Security of Protected Health Information for BU Healthcare Provider Covered Components
- Listing of related BU TechWeb Policies
- Access to Electronic Information Policy
- Acceptable Use of Computing Services Policy

- Digital Privacy Statement
- Network Security Monitoring Policy

Related Procedure

- Policy Violation Notification Procedure

Categories: Information Management, Privacy and Security Keywords: breach, data protection, security, security breach response team, sensitive, sensitive information