Program Statement

Boston University recognizes that in certain instances it must collect, store and use Social Security Numbers, drivers’ license numbers, financial account numbers and other sensitive information relating to its students, employees and individuals associated with the University. The University is dedicated to collecting, handling, storing and using that Information properly and securely. This Personal Information Protection Program is subject to the University’s Information Security Policy.

Definitions

The following definitions are taken principally from Massachusetts General Laws chapter 93H, section 1, and related regulations. These definitions are in addition to those outlined in the Boston University Information Security Policy.

Financial Account Number: any financial account number, including but not limited to bank account numbers, or credit or debit card numbers, with or without any required security code, access code, personal identification number or password that would permit access to a financial account. The BU ID is not a Financial Account Number.

Personal Information: Personal Information includes personally identifiable information as defined by the University Information Security Program Director and shall include an individual’s first name (or initial) and last name in combination with any one or more of the following:

- Social Security Number;
- Driver’s license number or other state-issued identification card number; or
- Financial Account Number, including credit or debit card numbers.

Procedures

I. Information Security Program Director and Committee

The University Information Security Program Director and the Information Security Program Committee shall administer this Program consistent with the University’s Information Security Policy. The Director may delegate
responsibilities concerning this Personal Information Protection Program, as appropriate.

In the event of any suspected Breach of Security concerning Personal Information, the Director shall respond as prescribed in the University’s Information Security Policy.

II. Units and Departments – Protection of Personal Information

Academic and administrative units or departments and all members of the University community may request, collect, store or use Personal Information only as permitted by this Program and applicable Information Security Guidelines. Units and departments may require within their own unit or department practices that are stricter than those set forth in this Policy or in the Information Security Guidelines. Each academic and administrative unit or department that requests, collects, stores or uses Personal Information must ensure that:

- Paper Records that contain Personal Information are stored in locked facilities, storage areas or containers;

- Electronic Records that contain Personal Information are stored and maintained on equipment and servers that are adequately secured and registered with Information Services & Technology and are transmitted only as permitted by applicable Information Security Guidelines;

- Only those Employees who have a legitimate business need to access Personal Information have access to paper and electronic Records that contain Personal Information;

- Temporary and casual employees do not have access to paper or electronic Records that contain Personal Information unless that temporary or casual employee has received approval from his or her supervisor, completed appropriate training and acknowledged this Program;

- Employees do not take Records that contain Personal Information out of the office without appropriate unit or departmental approval;

- Employees who have a legitimate business need to access electronic Records that contain Personal Information do so only through the Boston University-provided campus network or the University’s Virtual Private Network;
• Employee access to Personal Information is regularly monitored to ensure that only those Employees with a legitimate business need to access Personal Information are permitted to do so;

• Employees whose employment is terminated do not have physical or electronic access to any Records that contain Personal Information;

• Paper and electronic forms that ask individuals to provide Personal Information where there is no legitimate business need to request that information are, as requested by the Director, revised to eliminate those requests;

• Vendors or other individuals or entities outside of the University that are given access to Personal Information held by the unit or department have been disclosed to the Director;

• Records that contain Personal Information are destroyed as soon as there is no longer a business need to retain those Records, unless a longer retention period is specified by the University’s Record Retention Policy;

• Employees within the unit or department have taken approved University training concerning the University’s Information Security Program;

• Any suspected Breach of Security is reported to the Director immediately;

• Any identified internal or external risks to the security of Records that contain Personal Information are reported to the Director; and

• In consultation with Human Resources, appropriate disciplinary measures are imposed for violations of this Policy.