Purpose and Overview

BU Personnel are responsible for the protection of sensitive data entrusted to the University. There are contracts and state and federal laws that require protection of certain types of data; the BU Data Protection Standards aim to provide simplified guidance and direction for compliance in this complex environment.

This document contains details regarding the Data Protection Standard’s education, compliance review and remediation programs.
Scope

The Data Protection Standards, including all subparts, apply to all University Data, both physical and electronic, throughout Boston University.

BU Information Security Responsibilities

One subpart of the Data Protection Standards, the Data Protection Requirements, describes the strong protections required for Restricted Use data. For example, Restricted Use data must be encrypted if emailed or otherwise electronically transmitted or when stored on portable electronic devices (see the Data Protection Requirements for full details).

In support of the Data Protection Standards, BU Information Security will:

- Provide strategic direction and guidance to the University for meeting the Standards’ requirements.
- Provide training and consulting on the Standards to the University community.
- Conduct Security Monitoring and Compliance Reviews as defined below.
- Alert individuals and organizations that are not complying with the Standards and provide additional training and consulting services to remediate issues.

Training Program

BU Information Security will conduct and/or coordinate proactive education and training outreach programs designed to help increase the BU community’s awareness of information security issues, including the requirements of the Data Protection Standards.

This training is general in nature, providing an overview of information security and the legal and regulatory context in which we operate. It is not intended to replace regulation-specific training that may be required of people conducting specific duties and needing specific information about those duties. For example, FERPA training is and remains the responsibility
of the Registrar’s Office.

BU Information Security will, on an annual basis, send a reminder by email to the Faculty and Staff of Boston University providing a summary of the provisions of the Data Protection Standards, including the monitoring provisions of this document, and including a link which can be reviewed for more details.

Security Monitoring and Compliance Reviews

BU Information Security and IS&T will employ technologies and processes to protect BU Information Resources. These technologies and processes fall into several general types:

- **Network Intrusion and Vulnerability Detection.** IS&T will perform ongoing, routine network security monitoring, including using technologies to detect and/or prevent network intrusion and to scan for and identify vulnerabilities or compromises to BU network resources. These systems and related processes may provide alerts to IS&T and/or the owners of affected systems. Once alerted, the IS&T Incident Response Team, local administrators, and/or the owner of the relevant system will be responsible for mitigating any security issues found, including the presence of unprotected sensitive data.

- **Scanning for Restricted Use Data.** IS&T will conduct electronic scans to locate Restricted Use data that resides on central servers not intended for such data. IS&T will make available programs that permit units, departments, individuals to scan their own systems to identify Restricted Use data.

- **Audits.** The network monitoring and scans described above supplement the University’s ongoing efforts to ensure the security and reliability of its information technology systems. They do not replace or affect the scope of other University audit requirements and do not affect Internal Audit’s authority to conduct any audit, including audits relating to information security, or to take or recommend any action as the result of an audit. Information Security activities are intended to educate the community about safely and securely conducting the University’s business.

The Information Security and Internal Audit functions at Boston University may support each other from time to time. Internal Audit may request that Information Security support its audit functions. Likewise, Information Security may alert Internal Audit if it discovers a material
information security issue.

These reviews do not typically focus on the content of the message or file itself but rather on summary information about the message(s) or file(s). In order to maintain confidentiality, such reviews will be conducted only by Information Security personnel authorized to perform such activities.

**Review and Remediation Processes**

**Automated Review Process**

When an automated system discovers non-compliance with the Data Protection Standards, the process will be as follows:

- The automated system will document the non-compliance.
- The automated system will alert the relevant individual owner or system administrator to what was found and will provide appropriate information regarding the Data Protection Standards and what options exist to address the issue.
- After receiving an alert, the individual owner or system administrator may contact BU Information Security for consulting to help prevent future violations. BU Information Security may review reports from the automated system for patterns of non-resolved events or other heuristics of concern and may conduct a manual review and/or escalate the issue, as described below.

**Manual Review Process**

Where automated systems cannot identify a contact person for an issue or cannot provide automated notification, or where an incident comes to the attention of BU Information Security in another way, a manual review may be necessary. The process will be as follows:

- BU Information Security will document the non-compliance.
- BU Information Security will alert the individual owner or system administrator to what was found and will provide appropriate information regarding the Data Protection Standards. BU Information Security will offer training where appropriate or desired.
- BU Information Security will offer consulting to help prevent future violations and will work with the individual or representative of the organization to establish a timeline for the
remediation based upon the severity of the risk, the business needs of the client, availability of appropriate technology and other appropriate considerations.

**Escalation Process**

Information Security may escalate issues through layers of management based on the severity of the non-compliance or the number of times non-compliance has been detected.

- In the event of a severe issue or upon the **second** incident of non-compliance (regardless of the severity) after the remediation period of the first is over, Information Security will notify the relevant individual’s manager or manager of the organization.
- In the event of a critical issue or upon the **third** incident of non-compliance (regardless of the severity) after the remediation period of the second is over, Information Security will contact the manager of the organization to discuss the issue and that this is the third such finding. The Dean, VP or administrative head of the organization will receive a copy of the message or may be contacted directly.
- If appropriate, the offending account or system may be suspended until Information Security has received a written summary of corrective actions, signed by the individual, manager, and appropriate Dean or VP.

**Legal Obligations**

If IS&T learns or is notified of a data breach that obligates the University to notify state or federal authorities or individuals affected by the data breach, the University will do so and will take any other action that, in the University’s judgment, is necessary to resolve the issue.

**Important**

Failure to comply with the [Data Protection Standards](http://www.bu.edu/policies/education-compliance-and-remediation/) may result in harm to individuals, organizations or Boston University. The unauthorized or unacceptable use of University Data, including the failure to comply with these standards, constitutes a violation of University policy and may subject the User to revocation of the privilege to use University Data or Information.
Technology or disciplinary action, up to and including termination of employment.

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related BU Policies, Procedures, and Guidelines

- Data Protection Standards
  - Data Classification Policy
  - Data Access Management Policy (superseded the previous Data Management Guide)
  - Identity and Access Management
  - Data Protection Requirements
  - Minimum Security Standards
  - Education, Compliance, and Remediation

BU Websites

- Information Services & Technology

BU Resources

- Additional Guidance on Data Protection Standards

Categories: Information Management, Privacy and Security Keywords: Data Protection Standards

This Document is available at: http://www.bu.edu/policies/education-compliance-and-remediation/