Effective Date: **July 1, 2013** Revised: **April 29, 2021**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Cybersecurity Training, Compliance, and Remediation

RESPONSIBLE OFFICE

Information Security

REVIEWED: APRIL 28, 2022 BY CSIS GOVERNANCE

This policy supersedes the previous versions of this policy entitled “Education, Compliance, and Remediation”

Purpose and Overview

The Information Security program has a critical role in ensuring the university community has a practical understanding of cybersecurity risks. Working within the Information Security Policy, Information Security promulgates the BU Data Protection Standards to provide guidance and direction for protecting data in this complex environment. To be effective, Information Security must communicate and provide training on cyber risks and the Standards, monitor for compliance, and remediate issues.

Scope

The Data Protection Standards, including all subparts, apply to all University Data, both physical and electronic, throughout Boston University. This policy defines the responsibilities of Information Security to train, monitor, and remediate cybersecurity issues across the university.

BU Information Security Responsibilities

To promote cybersecurity awareness and ensure policy compliance, Information Security will:

- Provide additional strategic direction and guidance to the University on cybersecurity topics, including meeting the Standards' requirements as needed.
- Provide training and consulting on cybersecurity and the Standards to the University community.
- Conduct cybersecurity policy 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 training programs designed to guide the University's efforts to protect Sensitive Information by increasing the 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. Cybersecurity Foundations

training, which includes the Data Protection Standards and additional information security policies, is provided on demand online to anyone within the BU community.

Compliance Monitoring

BU Information Security and IS&T will employ technologies and processes to monitor our cybersecurity risks. These technologies and processes fall into several general types:

- Vulnerability Management
  IS&T will conduct routine scans and audits of computing technologies connected to the university network for vulnerabilities which may indicate a lack of compliance with the Minimum Security Standards. When discovered, Information Security will notify the appropriate system owners.

- Scanning for *Restricted Use* Data
  IS&T will conduct electronic scans from time to time to locate *Restricted Use* data on University-owned systems. Once identified, Information Security will ensure that the controls protecting the data are sufficient under the Standards or work with appropriate individuals to properly secure or relocate the data.

- Incident Response
  Information Security maintains an incident response process that investigates cybersecurity events, including those that may indicate a breach of Sensitive Information. If Sensitive Information is discovered as part of such an investigation, Information Security shall remediate the exposure, including activation of the university's Data Breach Management Plan as needed.

- 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 or to take or recommend any action relating to information security 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 should work together and exchange information to support their respective functions.

Remediation Processes

When an issue with compliance with the Data Protection Standards is identified, Information Security will:

- Document the non-compliance.
- Alert the individual owner or system administrator to what was found
- Provide appropriate information regarding complying with the Data Protection Standards. Training will be offered where appropriate or desired.
- Offer consulting to help prevent future violations
- 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. If appropriate, access by the offending account overall or to a system or specific data may be suspended until a remediation plan is agreed to and enacted.

Legal Obligations

If IS&T learns of a data breach, the University will notify state or federal authorities or individuals affected by the data breach and take any other action that, in the University's judgment, is necessary to comply with its obligations.

Important

Failure to comply with the Data Protection Standards 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 (*This policy supersedes the previous versions entitled* "Data Management Guide")
  - Identity and Access Management
  - Data Lifecycle Management Policy (*This policy supersedes the previous versions entitled "*Data Protection Requirements")
  - Minimum Security Standards
  - Cybersecurity Training, Compliance, and Remediation Policy *[current webpage]*

BU Websites

- Information Services & Technology

BU Resources

- Additional Guidance on Data Protection Standards
  - 1.2.D.1 – Destruction of Paper Records and Non-Erasable Media -CD-ROMs, DVDs (Data Protection Standards Guidance)

- 1.2.D.2 – Destruction of Individual Files on Reusable Media (Data Protection Standards Guidance)
- 1.2.D.3 – Securely Erasing Entire Reusable Storage Devices (Data Protection Standards Guidance)
- 1.2.D.4 – Physically Destroying Reusable Storage Devices (Data Protection Standards Guidance)

Categories: Information Management, Privacy and Security Keywords: compliance review, Data Protection Standards, information security, information security responsibility, remediation program, remediation programs, security monitoring, sensitive data