Revised: **May 1, 2026**

STANDARDS

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Data Protection Standards Overview

RESPONSIBLE OFFICE

Information Security

Overview and Purpose

Boston University's Data Protection Standards are rules everyone at BU follows to keep personal and University information safe. These standards help prevent data breaches and cyber incidents, support teaching and research, and make sure BU meets legal requirements. By following these standards, we protect privacy, keep data accurate, and make sure University services run smoothly. All faculty, staff, students, and departments must follow these standards unless given special permission by BU Information Security.

What is a Data Protection Standard?

A Data Protection Standard is a specific set of rules that explains how to follow the University's broader information security policies. Policies explain the drivers: The "why" we do something. Standards clarify "what" needs to be done. Everyone must follow these standards when performing applicable work.

List of Data Protection Standards

This list shows how Boston University's Data Protection Standards help protect information, organized by the five key areas of the National Institute of Science and Technology (NIST) Cyber Security Framework (CSF).

Identify

Understand what information we have and what the risks to it are.

Data Classification Standard:

Defines how all University Data is categorized by sensitivity. This standard establishes four data classification levels – Public, Internal, Confidential, and Restricted Use – and provides definitions and examples for each.

Cyber Risk Assessment Standard:

Provides a structured methodology for evaluating cybersecurity risks, ensuring consistent assessment and prioritization of threats to Boston University systems and data.

Protect

Keep information safe from threats.

Cyber Risk Management Standard:

Outlines how identified cybersecurity risks are handled, assigns ownership, and guides decisions to mitigate, accept, or transfer risks.

Data Access Management Standard: Governs how access to sensitive University data is granted, managed, and reviewed. It defines formal roles and responsibilities for data governance – for example, appointing Data Trustees, Data Custodians, Departmental

Security Administrators (DSAs), and Data Executives in each department.

Data Access Management Standard:

Governs how access to sensitive University data is granted, managed, and reviewed. It defines formal roles and responsibilities for data governance – for example, appointing Data Trustees, Data Custodians, Departmental Security Administrators (DSAs), and Data Executives in each department.

Data Lifecycle Management Standard:

Defines requirements for protecting sensitive information at every stage—collection, storage, access, sharing, transmission, and destruction—across the University.

Identity and Access Management Standards:

Explains how BU creates, manages, and secures user accounts. It covers account setup and removal, password and authentication rules (like strong passwords and multi-factor authentication), and ensures people only have the access they need.

Minimum Security Standards:

Requires all devices and cloud services handling University data to follow baseline security practices—such as regular patching, encryption for sensitive data, strong passwords, and antivirus protection—to ensure the confidentiality, integrity, and availability of these systems.

Data Center Standards:

Mandates strong physical security, operational procedures, and environmental controls for facilities hosting University IT infrastructure, ensuring protection against intrusions and environmental threats.

Cybersecurity Training, Compliance, and Remediation Standard

:

Provides security training, monitors compliance, and assists with remediation to ensure policies are understood and followed.

Detect

Spot problems and threats quickly.

Vulnerability Management Standard:

Requires proactive identification and timely remediation of security vulnerabilities to reduce the risk of cyberattacks

Log Collection, Analysis, and Retention Standard:

Sets requirements for generating, storing, and analyzing system logs to support security operations and compliance.

Respond and Recovery

Act expediently when something goes wrong and get back to normal after an incident.

Cyber Incident Response Plan:

Generic: Provides a high-level plan for preparing and responding to generic cyber incidents, emphasizing a structured approach while allowing flexibility for specific situations. [This plan is not published. Contact Information Security for more information]

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related BU Policies, Procedures, and Standards

- Data Protection Standards Overview [this webpage]
  - Data Classification Standard
  - Data Access Management Standard
  - Identity and Access Management Standards
  - Data Lifecycle Management Standard
  - Minimum Security Standards
  - Cybersecurity Training, Compliance, and Remediation Standards
  - Cyber Risk Assessment Standard
  - Cyber Risk Management Standard
  - Data Center Security Standards
  - Vulnerability Management Standard
  - Log Collection, Analysis, and Retention Standard

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)

History

These Data Protection Standards became the Data Protection Standards Overview - May 2026

Categories: Data Protection Standards, Data Protection Standards, Information Management, Information Technology Use, Access, and Security, Privacy and Security Keywords: BU techWeb, data classification, information, information management, IS&T, privacy, security, techweb