Effective Date: **March 1, 2011** Revised: **April 12, 2023**

POLICY

EMPLOYMENT, INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Data Lifecycle Management Policy

RESPONSIBLE OFFICE

Information Services and Technology

REVISED APRIL 2023 (BY CSIS GOVERNANCE)

This policy supersedes the previous versions entitled "Data Protection Requirements"

Purpose and Overview

The data lifecycle is the progression of stages in which a piece of information may exist between its original creation and final destruction. Boston University defines these phases as: Collecting, Storing, Accessing and Sharing, Transmitting, and Destroying.

This policy defines or references the requirements for protecting data at each stage of the lifecycle.

Scope

The data handling protections outlined in this document apply to all Sensitive Information, both *physical* and *electronic*, throughout all of Boston University.

Sensitive Information is University Data that is classified as *Internal*, *Confidential*, or *Restricted Use.* See the Data Classification Policy for definitions and examples of each of these classifications.

Public (non-Sensitive) Information does not require any level of protection from disclosure but appropriate precautions should be taken to protect original (source) documents from unauthorized modification.

Roles

Enterprise Services

IS&T is responsible for providing consulting and training concerning security, maintaining the security of the network and centrally provided services, and providing guidance about the approved data classifications for each service offered.

Schools, Colleges, Units, and Departments

The head of each of the university's schools, colleges, units, and departments ("Data Executive") is accountable for working with their designated Data Security Administrator(s) to ensure that their data is managed in compliance with this policy. Units are encouraged to take advantage of enterprise services available to support the requirements of this policy.

Individuals

All BU faculty and staff are expected to be familiar with and follow the Data Protection Standards to ensure proper understanding of how to handle Sensitive Information properly.

If you have questions, ask your supervisor, Departmental Security Administrator, or Information Security.

Data Lifecycle Phases and Requirements

Collecting

Collection of data should be minimized to the amount necessary to support the teaching, research, or administrative function the collection supports. As the sensitivity of the data element increases, the need to collect the element requires more scrutiny. The collection of Restricted Use data must be avoided whenever possible, and attention must be paid to the significant security and privacy protection requirements. Contact Information Security before engaging in any new collection of Restricted Use data.

Storing

- Store information in repositories that cannot be accessed by unauthorized individuals.
- Physical media should be stored in locked drawers and cabinets when not in use.
- Data should be encrypted at rest where reasonable to do so, preferably using technologies like whole disk encryption that is native to the operating system. Restricted Use data must always be encrypted at rest, and Endpoint Devices must use native disk encryption where available regardless of the types of data present.
- Limit the number of copies of data to the minimum possible and do not retain longer than needed.
- Portable media (CD-ROMs, USB keys) should not be used to store Restricted Use data. When required, the department must maintain an inventory of the media until it is erased and/or destroyed.

Accessing and Sharing

Apply the Principle of Least Privilege to all data: Grant access and share data only as needed for an individual or system to perform a required function. Increase scrutiny of these controls as the sensitivity of the data increases. Ensure processes are in place to immediately remove access upon change in affiliation of any individual.

Notes:

- Access to some Confidential data and all Restricted Use data requires approval of a Data Trustee in accordance with the Data Access Management Policy.
- Non-disclosure and other types of agreements (e.g., Data Use Agreement for research data, HIPAA Business Associate Agreement) may be necessary for certain types of data.
- Information may be shared with the subject of the record or with another party with the subject's approval, as appropriate.
- If you are uncertain if access should be granted or information should be shared, escalate the request to an appropriate supervisor or Data Trustee.

Transmitting

Transmission of Physical Media (Paper, CD-ROM, USB keys, etc.):

- Avoid printing Restricted Use data unless absolutely necessary.
- Use care when printing to ensure the paper copies are not left unattended on printers.
- Requirements for the creation of digital media are described in the Storing section of this document.
- Ensure mailings are addressed carefully and sent in sealed envelopes.

Electronic Transmission (Email, Fax, websites, cloud storage, etc.):

- Encryption should be used during transmission whenever possible. All Sensitive Information should be encrypted in transit where it is reasonable to do so using VPN, SSL, or similar technologies.
- Encryption in transit is strongly recommended for Confidential data and required for Restricted Use data.
- Avoid transmitting Restricted Use data via e-mail by sharing files or folders from BU cloud services instead, such as OneDrive, SharePoint, and Teams. Google Workspace Applications, including those provided through BU, should not be used with Restricted Use Data.
- Avoid faxing Restricted Use data unless necessary.

- Use care to ensure the paper copies are not left unattended when using fax machines.

Destroying

Destroy paper media using a cross-cut shredder or similar appropriate technology and then recycle or discard.

Printers, Computers and Mobile Devices may contain hard drives which must be properly erased prior to leaving BU control (returned to the vendor, sent to surplus, donated, disposed of, etc.). Dispose of drives using IS&T's Media Destruction service.

Notes:

- Review the university's Record Retention Policy and the information in this destruction section before disposing of records.
- Do not destroy records that are the subject of a litigation hold.

See also:

- Destruction of Paper Records and Non-Erasable Media (CD-ROMs, DVDs)
- Destruction of Individual Files on Reusable Media
- Securely Erasing Entire Reusable Storage Devices
- Physically Destroying Reusable Storage Devices

Exceptions

Information Security is authorized to grant exceptions to the requirements set forth in this document. Any exception granted will require a thorough review of the situation and the implementation of appropriate compensating controls.

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 *[current webpage]*
  - Minimum Security Standards
  - Cybersecurity Training, Compliance, and Remediation Policy (*This policy supersedes the previous versions entitled* "Education, Compliance, and Remediation")

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: Acceptable Use, Employment, Information Management, Information Technology Use, Access, and Security, Privacy and Security, Workplace Keywords: access, data, data collection, data destruction, data lifecycle, data protection, data storage, sharing data, transmitting data