Effective Date: **December 1, 2010** Revised: **May 1, 2026**

STANDARDS

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Data Classification Standard

RESPONSIBLE OFFICE

Information Services and Technology

Purpose

University Data is information generated by or for, owned by, or otherwise in the possession of Boston University that is related to the University's activities. University Data may exist in any format (i.e. electronic, paper) and includes, but is not limited to, all academic, administrative, and research data, as well as the computing infrastructure and program code that supports the business of Boston University. To effectively secure University Data, we must have a vocabulary that we can use to describe the data and quantify the amount of protection required.

Scope

This classification scheme is to be applied to all University Data, both physical and electronic, throughout Boston University. No data item is too small to be classified.

Overview

This standard defines four categories into which all University Data can be divided:

- Public
- Internal
- Confidential
- Restricted Use

Sensitive Data refers to all types of non-Public data (Internal, Confidential, and Restricted Use).

Data Protection

University Data that is classified as Public may be disclosed to any person regardless of their affiliation with the University. All other University Data is considered Sensitive Data and must be protected appropriately. This document provides definitions for and examples of each of the four categories. Other policies within the Data Protection Standards specify the security controls that are required for each category of data. Some key documents to reference are:

- Data Access Management Standard
- Data Lifecycle Management Standard
- Minimum Security Standards

Guidance for Classifying Data

Units and departments at the University have a multitude of types of documents and data. To the extent particular documents or data types are not explicitly addressed within this standard, however, guidance is available in the BU Data Sharing Guide. Working with BU Information Security and Data Enablement to ensure consistency across the university, Data Executives and Trustees in each business unit or department are responsible for data classifications in their areas. Consideration for classification includes the potential for harm to individuals or the University in the event of unintended disclosure, modification, or loss. When classifying data, each department should weigh the risk created by an unintended disclosure, modification or

loss against the need to encourage open discussion, improve efficiency and further the University's goals of the creation and dissemination of knowledge. Departments should be particularly mindful to protect sensitive personal information, such as Social Security Numbers, drivers' license numbers and financial account numbers, disclosure of which may create the risk of identity theft.

Some information could be classified differently at different times. For example, information that was once considered to be Confidential data may become Public data once it has been appropriately disclosed. Classifications that have been documented by BU Data Enablement are periodically reviewed for appropriate levelling. Everyone with access to University Data should exercise good judgment in handling sensitive information and seek guidance from management as needed.

A Note about Research

Boston University is committed to publishing the results of research to drive scientific theories and fuel technological innovation. Prior to any authorized publishing, research data is classified according to any applicable grant or data use agreement requirements. If there is no agreement governing use of the data, it is classified as Confidential unless it contains personally identifiable health information, in which case it is Restricted Use.

Standard

Classification Levels

Public

Public data is information that may be disclosed to any person regardless of their

affiliation with the University. The Public classification applies to data that do not require any level of protection from disclosure. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the University community and no steps need be taken to prevent its distribution.

Examples of Public data include: press releases, directory information (not subject to a Family Educational Rights and Privacy Act (FERPA) block), course catalogs, application and request forms, protected health information that has been de-identified consistent with the standards set forth under Health Insurance Portability and Accountability Act (HIPAA), and other general information that is openly shared. The type of information a department would choose to post on its website is a good example of Public data.

Internal

Internal data is information that is potentially sensitive and is not intended to be shared with the public. Internal data generally should not be disclosed outside of the University without the permission of the person or group that created the data. It is the responsibility of the Data Executive or Data Trustee to designate information as Internal where appropriate. If you have questions about whether information is Internal or how to treat Internal data, you should talk to your Departmental Security Administrator, dean or department head, or contact Data Enablement.

Examples of Internal data include: Some memos, correspondence, and meeting minutes; contact lists that contain information that is not publicly available; and procedural documentation that should remain private.

Confidential

Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or the business of Boston University. This classification also includes data that the University is required to keep confidential, either by law (e.g., FERPA) or under a confidentiality agreement with a third party, such as a research sponsor or vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or

transported. See the Minimum Security Standards for more details on protecting Sensitive Data.

Use or storage of University Data, particularly Confidential or Restricted Use data, on cloud services, mobile devices, or by third-party vendors is permitted only when those platforms or vendors have been approved by Information Security and meet applicable security standards. Data must be encrypted both at rest and in transit, and vendors must comply with contractual and regulatory obligations related to data protection.

Any unauthorized disclosure or loss of Confidential data must be immediately reported to the Information Services & Technology Service Desk via ithelp@bu.edu or 617-353-HELP (353-4357).

Examples of Confidential data include:

- Information covered by the Family Educational Rights and Privacy Act (FERPA), which requires protection of records for current and former students. This includes pictures of students kept for official purposes.
- Personally identifiable information entrusted to our care that is not otherwise categorized as Restricted Use data, such as information regarding applicants, alumni, donors, potential donors, or parents of current or former students, and information covered by the European Union's General Data Protection Regulation (GDPR).
- The Boston University ID Number, when stored with other identifiable information such as name or e-mail address.
- Information covered by the Gramm-Leach-Bliley Act (GLBA), which requires protection of certain financial records.
- Individual employment information, including salary, benefits, and performance appraisals for current, former, and prospective employees.
- Legally privileged information.
- Information that is the subject of a confidentiality agreement.
- Human subject research data with identifiers limited to dates, city, Zip Code; such as information that is the subject of a HIPAA Limited Data Set covered by a Data Use Agreement.

Restricted Use

Restricted Use data includes any information that BU has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner. In some cases, unauthorized disclosure or loss of this data would require the University to notify the affected individual and state or federal authorities. In some cases, modification of the data would require informing the affected individual. Restricted Use data may only be collected, stored, transmitted, processed, or used with authorization from the Chief Information Security Officer, and when handled in accordance with required security controls.

The University's obligations will depend on the particular data and the relevant contract or laws. The Minimum Security Standards sets a baseline for all Restricted Use data. Systems and processes protecting the following types of data need to meet that baseline:

- Personally identifiable health information
- Personally Identifiable Information (PII) covered under Massachusetts General Law chapter 93H and 201 CMR 17, including an individual's name plus the individual's Social Security Number, driver's license number, or a financial account number.
- Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens.
- An individual's biometric data (e.g., fingerprints, face scans, etc.) stored for identification or authentication purposes.
- "Criminal Background Data" that might be collected as part of an application form or a background check.

More stringent requirements exist for some types of Restricted Use data. Individuals working with the following types of data must follow the University policies governing those types of data and consult with Information Security to ensure they meet all of the requirements of their data type:

- Protected Health Information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA). See the university's HIPAA Policy for details.
- Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored.

- Controlled Unclassified Information required to be compliant with NIST 800.171
- Data required to be compliant with any NIST cybersecurity standards according to any agreement.
- Data controlled by U.S. Export Control Law such as the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). ITAR and EAR have additional requirements. See the Export Controls site for details.
- U.S. Government Classified Data

  Restricted Use data should be used only when no alternative exists and must be carefully protected. Any unauthorized disclosure, unauthorized modification, or loss of Restricted Use data must be reported to Information Services & Technology Service Desk via ithelp@bu.edu or 617-353-HELP (353-4357).

Resolving Conflicts between this Guideline and Other Regulations

Some data may be subject to specific protection requirements under a contract or grant, or according to a law or regulation not described here. In those circumstances, the most restrictive protection requirements should apply. If you have questions, contact Information Security.

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.

In addition, Information Security may publish directives aimed at clarifying the intent of a standard to aid in the interpretation of this standard.

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.

Version History

Notes	Approver	D
Initial Publication of Data Classification Guide	Information Security and Business Continuity Governance Committee	D
Updated Definitions	Information Security and Business Continuity Governance Committee	J
Updated and renamed Data Classification Policy	Information Security and Business Continuity Governance Committee	A
Updated Definitions	Common Services and Information Security Governance Committee	A
Reviewed, No Changes	Common Services and Information Security Governance Committee	A
Updated Definitions	Common Services and Information Security Governance Committee	A
Reviewed, No Changes	Common Services and Information Security Governance Committee	A
Updated Definitions	Common Services and Information Security Governance Committee	A
Reviewed, No Changes	Common Services and Information Security Governance Committee	A

Notes	Approver	D
Updated and renamed Data Classification Standard	IS&T Policy and Standards Review Committee	M

END OF POLICY TEXT

Categories: Data Protection Standards, Data Protection Standards, Information Management, Privacy and Security Keywords: classification of data, data classification, data protection, data protection standard, Data Protection Standards