Effective Date: **February 1, 2010** Revised: **April 12, 2023**

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Data Access Management Policy

RESPONSIBLE OFFICE

Information Security

This policy supersedes the previous versions entitled "Data Management Guide"

REVISED: APRIL 2023 (BY CSIS GOVERNANCE)

Purpose and Overview

University Data is information that is related to Boston University's activities and is created, maintained, or processed by Boston University. University Data is a vital asset that must be available to employees who have a legitimate administrative need for it. However, the use of University Data for anything other than approved University purposes is prohibited by University policy and, in many instances, by law.

This document defines the roles and responsibilities with respect to managing access to University Data meeting the criteria defined in the Scope section.

Scope

This policy applies to access to University Data classified as Confidential or Restricted Use that is maintained by the University or a party acting on the University's behalf, hereafter called "Subject Data".

This policy does not apply to:

- Data or records that are personal property of a member of the University community, research data, or data created and/or kept by individual employees or affiliates for their own use;
- University Data that has been de-identified such that it may be classified as Internal or Public, as determined by the Data Trustee (see below);
- Situations in which the University is legally compelled to provide access to information;
- Data classified as Internal or Public. Access to these data types is determined at the discretion of the office that creates, maintains, or processes it; and
- Data for which a more restrictive set of policies and procedures are used, such as HIPAA data.

Official Roles and Responsibilities

A. Data Executive

The Data Executive is the executive or head of a University department that creates, maintains or processes Subject Data. A Data Executive is responsible for approving access to Subject Data, but may delegate such responsibility to Data Trustee(s). The Data Executive is responsible for establishing the criteria for sharing Subject Data.

The Data Executive shall ensure that their department is reminded of this policy annually.

The Data Executive may designate at least two and no more than four Data Trustees to help approve access requests and conduct access reviews. The Data Executive is responsible for ensuring that the Data Trustees receive the relevant training provided by Information Security.

B. University Leadership and Technology Providers

University Leadership is the management of any department that needs access to Subject Data or maintains records on behalf of a Data Executive. Technology Providers are subset of

University Leadership whose units provide electronic applications and systems to enable the use and storage of Subject Data.

University Leadership is responsible for appointing Departmental Security Administrators as needed to fulfill the requirements of this policy. University Leadership is responsible for ensuring their unit's knowledge of and compliance with this policy.

University Leadership and Technology Providers are responsible for appointing Data Custodians as needed to fulfill the requirements of this policy. They are responsible for ensuring Custodians understand their responsibilities under this policy.

C. Data Trustee

Data Trustees are responsible for:

- Ensuring and monitoring the accuracy, integrity, and privacy of Subject Data;
- Granting or denying access to the Subject Data;
- Performing regular audits to ensure approvals for access to Subject Data remain valid and appropriate.

Data Trustees are responsible for reviewing requests for access to Subject Data and responding within three business days. The required elements of an approval are described in the Documentation of Approvals section. Data Trustees should grant access to Subject Data only to individuals, Project developers or Project teams with a demonstrable legitimate administrative need for the Subject Data, in accordance with guidelines set by the Data Executive, and a plan for compliance with University policy and applicable law. The Data Trustee should approve access to only the minimum amount of Subject Data for minimum amount of time that is necessary to meet the requester's needs. If applicable to the technology, the Data Trustee may specify types of access (read-only, read-write).

Data Trustees may create pre-approvals for certain roles to have access to data if they wish. Birthright privileges are authorizations given to individuals when their account is first created or assigned a specific affiliation ("student", "faculty", e.g.) as defined in the Identity and Access Management Policy. Access rights being granted automatically when an individual is assigned a specific affiliation is an example of a pre-approval. Any constraints of the pre-approval should be clearly documented and communicated to the appropriate Data Custodian(s) and

Information Security. These privileges should periodically be reviewed by Data Trustees and Information Security.

For requests by Project developers and Project teams, the Data Trustee must also confirm that the developers or team are coordinating with Information Security. Only Information Security may determine whether a solution complies with the Minimum Security Standards and such determination is in its sole discretion. The Data Trustee may request that Information Security confirm that this assessment has been completed and what risks were identified, if any. The Data Trustee shall not conduct their own assessment of the security of a proposed solution but may specify requirements, particularly regarding access controls.

After the Data Trustee has approved a requestor's access to Subject Data, changes to the system or to the manner in which Subject Data will be presented must be reviewed by Information Security, but do not require Data Trustee re-approval unless Information Security requests it.

The Data Trustee should carry out audits, not less than one time per year, to ensure approvals for access to Subject Data remain valid and appropriate.

Data Trustees are responsible for reviewing requests for access to Subject Data, whether the data will remain in the original data source or be copied to a new repository. Access to Subject Data copied to a new repository remains within the jurisdiction of the original Data Trustee.

D. Departmental Security Administrators (DSA)

The University Leadership of any department that needs access to Subject Data may designate up to four Departmental Security Administrators (DSAs). DSAs will act as liaisons between their University department and Information Security and oversee data security responsibilities at the department level. A new DSA's manager should ensure the new DSA receives the appropriate training from Information Security.

DSA responsibilities include:

- Identifying the department's need to store or access centrally maintained Subject Data sources and applications;
- Communicating requests for access to central financial, human resources systems (e.g.,

SAP), and student information systems (e.g., Mainframe). Before submitting a request for access, the DSA will confirm with the requestor's manager that the requestor has a legitimate administrative reason for needing access to the Subject Data;
- Conducting regular reviews (not less than one time per year, and to the extent possible) of access lists and requesting removal of access to Subject Data when no longer needed; and
- Communicating with Information Security in the event of any unauthorized disclosure, modification, or loss of Subject Data.

E. Individuals

Individuals may access, use or store Subject Data with authorization from the appropriate Data Trustee. Requests for authorization should be made through the requester's Data Security Administrator (DSA).

Individuals who are authorized by a Data Trustee to access, use or store Subject Data must use the data only in a manner consistent with approved university purposes. Individuals are not authorized to share Subject Data with others who do not have approval to access that same data until explicitly authorized as part of the request for access. Individuals must access Subject Data using devices that comply with the Minimum Security Standards for the appropriate data type (see Data Classification Policy) and follow any instructions or restrictions imposed by the Data Trustee. If an individual is authorized to provide information to an external vendor, the individual must work with Information Security to ensure the vendor will conform to the Minimum Security Standards.

F. Data Custodian

University Leadership or the Technology Provider of a mechanism to use or store Subject Data shall appoint Data Custodian(s). Data Custodians are the persons primarily responsible for maintaining the accuracy of access controls for Subject Data. Managers of Custodians are responsible for transitioning the responsibilities as staff turns over.

Data Custodian responsibilities include:

- Assisting individuals, Project developers and Project teams with identifying how to best access the Subject Data required for their work;

- Providing access to Subject Data, as approved by the Data Trustee and retaining a record of such approval;
- Removing access to Subject Data when requested by a DSA, Data Trustee, Data Executive, or the person to whom a requestor reports; and
- Supporting regular reviews of access lists by Data Trustees and DSAs, and removing access to Subject Data when no longer needed.

G. Information Security

Information Security's responsibilities include:

- With advice from the Office of the General Counsel, communicating changes in law that impact responsibilities of the University Leadership, Technology Providers, Data Executives, Data Trustees, DSAs and/or Data Custodians;
- Maintaining and publishing data management and protection standards, with appropriate input and approval from the Common Services and Information Security Governance Committee;
- Providing training to Data Executives, Data Trustees, Data Custodians, and DSAs on subjects relevant to compliance with this policy;
- Conducting an annual audit of the list of Data Trustees and DSAs to ensure the appropriate individuals have been identified;
- Maintaining the list of DSA responsibilities;
- Assisting with access requests from DSAs;
- Assisting individuals, Project developers and Project teams with submitting requests for access to Subject Data;
- Assisting with negotiations with third-party vendors who will use or store Subject Data to ensure minimum standards are agreed to;
- Responding to any reports of unauthorized disclosure, modification, or loss of Subject Data.

H. Application Development

IS&T, through its Application Development or other groups, may develop new ways to use or store Subject Data (each, a "Project"). Upon request, the Data Trustee may grant Project teams access to Subject Data for the purpose of such Project. This authorization does not empower individual Project developers or members of the Project teams to grant others

access to Subject Data. Individual end users of the Subject Data must be approved as described above in Subsection (E) unless otherwise approved by the Data Trustee.

If a third party will create, maintain or process Subject Data on behalf of the University in connection with a Project, this must be specified in the Project developer's or Project team's request to the Data Trustee. The Project developer or Project team must require that the third party demonstrate compliance with the Minimum Security Standards for the data type and agree to follow restrictions imposed by the Data Trustee.

Documentation of Approvals

- Where reasonable to implement, approvals of requests to access Subject Data should capture the following information:
- The name and title of the Data Trustee or Executive approving the request
- The date of approval
- The individuals or Project developer or team authorized to access the Subject Data
- The university purpose for which the access has been approved
- Any explicit permissions or restrictions on how the data may be accessed or used
- Whether the requester is authorized to make a copy of the Subject Data
- The time period for which such access is authorized. Access for development projects should be for a limited duration.

Access Request Appeals

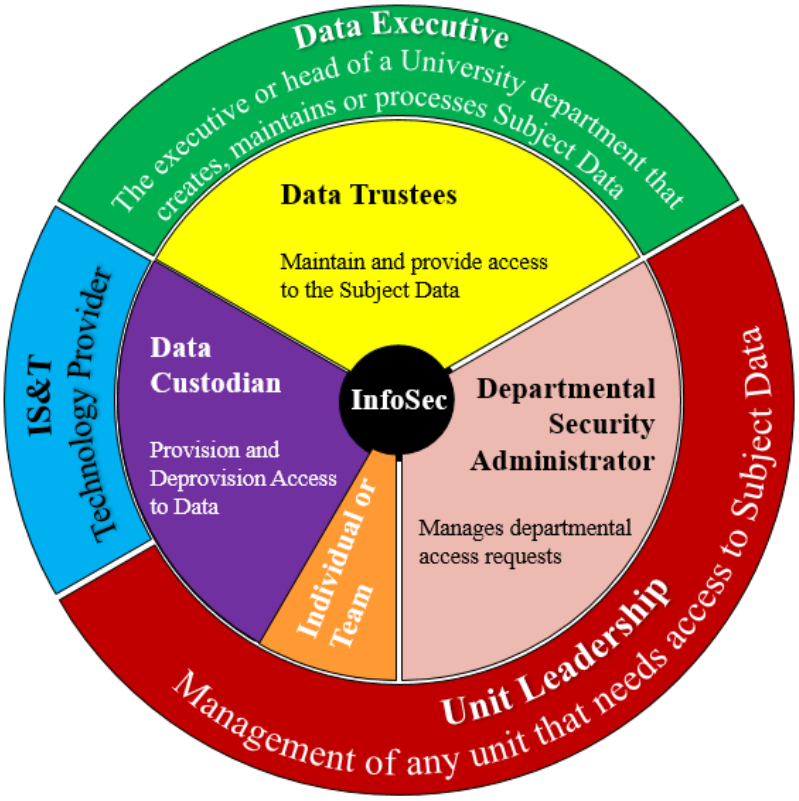
The requestor may appeal a Data Trustee's denial of access to Subject Data to the Data Executive.

Identifying Data Executive or Trustees

If you need assistance identifying a Data Executive or Data Trustee, please contact your DSA or Information Security. A list of Data Trustees is maintained on the IS&T Website ("TechWeb").

Reference Image for Role Relationships

To assist with understand the relationship between the roles defined in Official Roles and Responsibilities, the following diagram has been provided.



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 *[current webpage]*
  - 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 (*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)