Effective Date: **January 1, 2011** Revised: **May 1, 2026**

STANDARDS

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Minimum Security Standards

RESPONSIBLE OFFICE

Information Services and Technology

Purpose

Protecting University Data is a shared effort. Individuals with access to University Data are responsible for how they access, store, and process that data. They must use systems with security controls that match the classification level of the data they are handling. Individuals should consult with Information Services & Technology (IS&T) and their local IT support groups to determine the best way to access, store, and use their data, particularly for more sensitive data.

This document defines the minimum security standards required for any Electronic Device or Cloud Services (defined below) that may be used to access, store or process (input, output, transmit, receive, display, calculate, etc.).

Scope

The data handling protections outlined in this document apply to all Electronic Devices and

Cloud Services (defined below) used to access, store, or process information whether owned by Boston University (BU) or by a university employee or consultant and used to conduct university business. If you choose to use an Electronic Device you own (referred to herein as a "Personal Electronic Device"; for example, a home computer, smart phone, or tablet) to conduct university business, that Electronic Device is subject to these requirements. If you choose to use a Cloud Service that you have set up yourself (referred to as a "personal cloud service"; i.e., a service that has not been provisioned by the university), use of the service to conduct university business to BU is also subject to these requirements.

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 BU 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 National Institute of Standards and Technology Special Publication 800-171 (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

NOTE: Systems that handle Controlled Unclassified Information (CUI) must be reviewed by BU Information Security in order to confirm compliance with the required controls.

Defined Terms

“**University Data**” is information that is related to Boston University’s activities and is created, maintained, or processed by Boston University.

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

“**Cloud Services**” include any free or paid application, tool, or infrastructure made available by third parties wherein computing or storage resources are accessed via the Internet.

“**Electronic Device**” includes any device that is used to access, store or process data electronically. For example: a computer of any type (including a smart phone or tablet), a data storage device (including a USB device), a network device, a printer or copier that contains a storage device or that may be connected to a network.

“**Encryption**” is the process of converting human readable data (plain text) into data that cannot be read (cipher text) without knowledge of a specific secret (a key). There are two types of encryption referenced in this document: encryption in transit and encryption at rest. Encryption in transit refers to ensuring that all data sent over a network is encrypted, where encryption at rest refers to ensuring that all data written to disk or other permanent storage is encrypted. While the encryption process and outcome may be the same, the tools and methods for achieving each type of encryption are different.

Standards

Part I defines the cybersecurity roles related to security controls and each role’s responsibilities in adhering to this standard

Part II identifies baseline risk-based controls and systems management procedures that are required for all Electronic Devices working with Sensitive Data

Part III defines Cloud Services and their use cases and identifies the required controls when using these services

Part IV defines Personal Cloud Services and restrictions on their use with Sensitive Information

Part V defines Endpoint Devices and required controls to work with Sensitive Information

Part VI defines Non-Endpoint Devices and required controls to work with Sensitive Information

Part VII defines Internet of Things (IoT) Devices and required controls to work with Sensitive Information

Part I: Roles

Enterprise Services

IS&T is responsible for ensuring compliance of IS&T supported devices and services with this standard. IS&T will provide guidance about the approved data classifications for each device or service.

Schools, Colleges, Units and Departments

The University's schools, colleges, units, and departments are responsible for ensuring that the devices and services they provide to the community meet these minimum security standards, including providing guidance about the approved data classifications for each device or service.

Personal Responsibility

All Individuals with access to University Data are expected to be familiar with the Data Protection Standards to ensure understanding of how to handle Confidential or Restricted Use information properly.

If you use a personal Electronic Device or a personal cloud service, you are responsible for ensuring that your Electronic Device and/or personal cloud service meet the requirements below.

If you have questions, ask your supervisor, Departmental Security Administrator, IS&T, or BU Information Security.

Part II: Business Standards

Risk Based Controls

1. Kiosks and terminals intended for unauthenticated public use must not store any Sensitive Information.

2. Restricted Use data must only be stored on devices or cloud services that are approved for such use by BU Information Security.

3. Systems storing Confidential or Restricted Use data must be managed by a designated, qualified systems administrator who is capable of properly meeting the configuration requirements or deploying and confirming appropriate compensating controls.

4. Use authoritative data sources to minimize the number of copies of data, particularly Restricted Use data.

Systems Management

5. Procedures must be in place for securing downtime in accordance with the Vulnerability Management Standard to deploy critical security patches. Systems which cannot meet this requirement shall implement compensating controls specified by Information Security.

6. Powerful accounts such as administrator, super user, or root should be granted only to those with a documented need.

7. Accounts and access privileges should be removed in a timely fashion when an individual no longer has a need to access a system or application. A review cycle to reauthorize these accounts should be in place and followed.

Part III: Cloud Services

Cloud Services include any free or paid application, tool, or infrastructure made available by third parties wherein computing or storage resources are accessed via the Internet. The use of Cloud Services with University Data is governed by the Acceptable Use of Computing Services Policy, the Data Protection Standards, and other relevant University policies and procedures.

The following standards apply to the use of Cloud Services provided by or arranged for by, the University:

1. Services that will access, store or process Confidential or Restricted Use data must be evaluated by BU Information Security and the appropriate Data Trustee before use.

2. Cloud service offerings must define the roles and responsibilities of both the cloud service provider and the university during a breach investigation initiated by either party.

3. Cloud environments should be segregated (such as by subnet or AWS security groups) to separate test and production systems and data.

4. Isolate security services including firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), Log Management, and IAM from other services.

5. Limit administrative access to cloud infrastructure (IaaS) by requiring the use of a bastion host as a relay point for connecting into cloud instances.

6. Multifactor authentication is required wherever systems can support it. Compensating controls may be required by InfoSec where it is not available.

7. Secure Access Keys and Tokens should be rotated at least every 90 days.

8. Cloud Services must provide an exit strategy that enables the University to retain its

data and to remove or confirm destruction of all data from the cloud service.

9. The cloud provider must not mine or search University Data for purposes other than those approved by the University. This includes prohibiting the use of Artificial Intelligence (AI) Large Language Models (LLM) to train on University owned data or store query input and output data for a length of time not approved by BU Information Security.

10. Cloud providers that will store Confidential or Restricted Use data must document and contractually agree to implement strong physical access controls for their infrastructure and may be subject to audit by BU.

11. Cloud Services must define where they store data, including specific countries that data is, or could be, stored, replicated to, or routed through. Other countries may have requirements concerning access to data stored in or crossing their borders.

12. Cloud Services must implement access controls to ensure that data is not accessed by unauthorized users. For some Cloud Services this may include removing public/global read/view access.

13. The cloud provider must log all authentication attempts to provided services and be able to export the data if requested.

14. Restricted Use data must be encrypted at rest and while in transit; other data should be encrypted where reasonable to do so. This requirement applies to all storage devices, including removable media.

Part IV: Personal Cloud Services used for University Data

“Personal Cloud Service” is a subset of “Cloud Service” where the service is arranged for by an individual rather than the University, including the use of free software, services, and Artificial Intelligence (AI).

1. Confidential data should not be stored in Personal Cloud Services unless the service has been approved by Information Security and the appropriate Data Trustee.

2. Personal Cloud Services may not be used for Restricted Use data.

3. You must read and understand the terms of use, including whether the provider has access to your data and what it can do with the data. For example, the regular consumer version of Gmail scans your emails looking for keywords to better target advertising toward you, while the BU version of Gmail does not.

4. Understand how your data is protected, where (geographically) it is stored and how you might be able to get it back and erase the cloud copy in the event that you stop using the service.

5. Do not use your BU Kerberos password for Personal Cloud Services.

Part V: Endpoint Devices

An endpoint device is any hardware asset that connects directly to an organization's network or cloud services and serves as a primary interface for users or automated processes. Endpoint devices include, but are not limited to, workstations, laptops, mobile phones, tablets, thin clients, servers not housed in a secured data center, IoT devices, network-connected peripherals (e.g., printers, scanners), and remote computing devices. Because endpoints frequently process, store, or transmit organizational data, they represent critical control points for enforcing security policies, managing access, and detecting potential threats.

By comparison, a Non-Endpoint device (often referred to as a 'server') is intended to offer an application, storage, or other service. While it may be used directly by a human, such use is not the norm. In some cases, both sets of standards may apply, and the more stringent standard should be used.

Secure Endpoint devices must meet all of the following requirements:

1. Use an operating system (Windows, Mac OS, Linux, etc.) that is supported by a company who updates the operating system when security vulnerabilities are discovered. For mobile devices such as smart phones and tablets this includes not using devices for

which security controls have been intentionally subverted by the end user, such as a “jail broken” or “rooted” operating system.

2. Configure your systems and applications to receive and install updates automatically except where specific requirements prevent doing so.

a. Set up Windows Update or Mac Software Update to download and install automatically.

b. For mobile devices, use the native app store to download and install operating system and application updates automatically.

c. Unless device updates are being managed by an IT support group, configure devices to be updated within 2-3 days of a patch being released.

d. Where requirements prevent running fully updated software it may be necessary to deploy compensating controls. Consult with BU Information Security for these cases.

3. Always use a strong password and ensure your system requires authentication before it can be accessed. Password requirements can be referenced in the Authentication section of the Identity and Access Management standard.

4. Use biometric authentication (thumbprint, facial recognition, etc.) or set a strong PIN, passcode, password or pattern on mobile devices.

5. Create a non-administrative account for normal day-to-day activities to prevent unintended use of privilege, including by malware.

6. BU managed assets should be joined to the Active Directory.

7. BU managed assets should have an asset management agent installed and/or be enrolled in a Mobile Device Management (MDM) system. See the Asset Management Guide for more information.

8. Have your computer or mobile device lock the screen and require your password to

regain access if you are inactive for more than 15 minutes.

9. Ensure Endpoint Protection Software is installed and updated to protect your device from viruses, spyware, and other malicious behavior.

10. Information critical to the operation of the University shall be stored in an approved enterprise location (e.g. OneDrive) in addition to copies kept on a desktop, laptop, or mobile device.

11. Data backups should periodically be tested for validity and should be stored offline so the Operating System cannot modify them. Backups of Restricted Use data should use a solution that provides encryption in transit and at rest.

12. If connecting to a service from an off-campus location, ensure that the data is encrypted in transit by validating web URLs start with https:// and/or establishing a VPN or other secure network channel before accessing any Confidential or Restricted Use data.

13. Devices containing Sensitive Information must encrypt data at rest using native disk encryption functionality (for example, Bitlocker for Windows, FileVault for Mac or the native encryption on your smartphone or tablet). This requirement applies to all storage devices, including removable media.

14. For Electronic Devices that support it, make sure that you can remotely wipe the device.

15. All wireless connections must use strong encryption -WPA2 or equivalent or better- such as is offered by Boston University's 802.1x wireless network or by using a VPN over a wireless network.

Note: If you are using an Electronic Device that you cannot configure or for which you cannot confirm is securely configured (such as a public kiosk computer or a computer in a hotel, for example), that device should not be used to conduct BU business.

Part VI: Non-Endpoint Devices

This section contains detailed security requirements for all devices and services run or arranged for by the University, including but not limited to by IS&T.

1. Procured software that is used to store or process data, particularly Confidential or Restricted Use data, must be under vendor support. Non-supported software, including outdated operating systems, may not be used without an approved exception.

2. Systems should not require the intervention of a systems administrator on a per-machine basis to be updated. Use a tool that applies updates automatically. Absent a patch management program, security-related patches and updates must be applied to servers within 30 days. Vulnerabilities deemed 'critical' that are associated with known exploits must be patched as soon as possible.

3. Any default or vendor-supplied password must be changed to a non-default value that meets University minimum password complexity standards.

4. Firewalls should be used to protect Non-Endpoint Devices. If a network-based firewall is not an option, a local host-based firewall should be used. Firewalls should control/limit connections to and from the Non-Endpoint Device, permitting only what is necessary.

5. Data that is important to the operations of the University should be backed up to protect against loss. See the Record Retention Policy for details.

6. Sensitive Information should be encrypted in transit where it is reasonable to do so using VPN, SSL, or similar technologies. Encryption in transit should be used for Confidential data and is required for Restricted Use data.

7. All authentication attempts to operating systems and applications, both successful and failed, must be locally logged. These audit logs should be forwarded to an enterprise log repository where possible.

8. On multiuser devices, file system access controls should be implemented to ensure that data is not accessed by unauthorized users. Systems used to process or store Confidential or Restricted Use information should not host any unauthenticated service that allows access to browse the file system, such as anonymous ftp or directory indexing via a web server.

9. Servers storing significant quantities of Confidential data or any Restricted Use data should be kept in secure rooms with strong physical access controls. Multifactor physical access controls and video surveillance of these areas should be used.

10. Restricted Use data must be encrypted at rest; other data should be encrypted where reasonable to do so, preferably using technologies like whole disk encryption that is native to the operating system. This requirement applies to all storage devices, including removable media.

11. Reusable media (disk drives, removeable storage devices) must be securely erased or destroyed when removed from service. When Confidential or Restricted Use data is involved, failed media that is not encrypted (even if under warranty) cannot be returned to the manufacturer if it cannot be wiped. These drives must be destroyed via our Media Destruction service.

12. Systems should be routinely scanned for vulnerabilities and discovered vulnerabilities should be remediated in accordance with the

13. Network-accessible systems that contain Restricted Use information from multiple individuals should require two-factor identification where technically practicable, including access by individuals to their own data.

14. Endpoint Protection Software should be installed and tied to enterprise management and reporting utilities.

15. Services, network based or local to the system, that do not have an associated need should be disabled.

16. Non-Endpoint devices must be configured to sync time information (Network Time Protocol) from the BU Network Time Protocol (NTP) service operated by IS&T. If this

capability is present, it must be utilized.

17. If the device is used to store or process data that is important to University business, a disaster recovery and business continuity plan should be in place to recover and restore services.

18. Non-production systems (e.g. Dev, TEST) must not store production Restricted Use data unless security controls equivalent to the production environment are in place.

19. Authentication to devices or software should use approved enterprise authentication services (e.g. Active Directory, Kerberos, Shibboleth)

20. Use standard, repeatable processes to install operating systems and applications from trusted sources.

21. Systems and applications used by the University shall be configured to log security-related events which should be reviewed on a regular basis. See Log Collection, Analysis, and Retention Standard.

22. System events should be monitored and alerts sent in the event of log process failures.

23. Systems should terminate a user session after a defined period of inactivity.

24. System Administrators should follow IS&T Architectural Standards for the creation and maintenance of cryptographic keys for organizational systems.

Part VII: Internet of Things (IoT) Devices

Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communication networks. These devices differ in that they generally have a specific function, such as sensing temperature, and are not intended for general purpose computing. These devices have historically been challenging to secure so added attention is needed for these devices.

This section contains several security requirements for Internet of Things devices and services running on or arranged for by the University, including but not limited to by IS&T.

1. IoT Devices and their implementation architectures should be reviewed by BU Information Security prior to being installed on the Boston University network.

2. Once reviewed, IoT Devices should be placed on an isolated network approved for IoT Device(s).

3. IoT devices that require communication with other Boston University systems and networks must be placed behind a Boston University managed firewall for the purpose of monitoring and controlling network communication.

4. IoT devices with specialized communication requirements such as non-standard network address translation (NAT) or unique port and protocol requirements will require full architecture and engineering review prior to approval and installation.

5. Any default or vendor-supplied password must be changed to a non-default value that meets University minimum password complexity standards.

6. Systems should be routinely scanned for vulnerabilities and discovered vulnerabilities should be remediated in accordance with the Vulnerability Management Standard.

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
Initial Publication of Minimum Security Standards	Information Security and Business Continuity Gove Committee
Updated Standards	Information Security and Business Continuity Gove Committee
Revised Standards	Information Security and Business Continuity Gove Committee
Revised Standards	Information Security and Business Continuity Gove Committee
Revised Standards	Common Services and Information Security Goverr Committee
Revised Standards	Common Services and Information Security Goverr Committee
Revised Standards	Common Services and Information Security Goverr Committee
Reviewed, No Changes	Common Services and Information Security Goverr Committee
Revised Standards	Common Services and Information Security Goverr Committee

Notes	Approver
Revised Standards	Common Services and Information Security Governance Committee
Revised Standards	IS&T Policy and Standards Review Committee

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related BU Policies, Procedures, and Standards

- Data Protection Standards Overview
  - Data Classification Standard
  - Data Access Management Standard
  - Identity and Access Management Standards
  - Data Lifecycle Management Standard
  - Minimum Security Standards [this webpage]
  - 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)

Categories: Data Protection Standards, Data Protection Standards, Information Management, Information Technology Use, Access, and Security, Privacy and Security Keywords: Data Security Standards