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

POLICY

INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Minimum Security Standards

RESPONSIBLE OFFICE

Information Services and Technology

REVIEWED: APRIL 24, 2024 (BY CSIS GOVERNANCE)

Purpose and Overview

Protecting University Data is a shared effort. Individuals with access to University Data are responsible for accessing, storing, and processing data on systems that have appropriate security controls in place for the class of data. 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.) Sensitive Information (defined below) owned or used by Boston University.

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 Sensitive Information whether owned by Boston University (BU) or by a University employee or consultant and used to do 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 access, store or process Sensitive Information, 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 access, store or process Sensitive Information belonging to BU is also subject to these requirements.

The Payment Card Industry Data Security Standards (PCI-DSS) includes more stringent requirements for systems handling credit card data than described herein. If you are handling credit card data in any way, please contact Information Security to ensure that your systems meet the PCI-DSS requirements.

Systems that handle Protected Health Information (as defined under the Health Insurance Portability and Accountability Act (HIPAA)) are subject to HIPAA and must comply with all BU HIPAA Security and Privacy policies. If you are handling Protected Health Information in any way, please contact Information Security to ensure that your systems meet the HIPAA and policy requirements.

Systems that handle International Traffic in Arms Regulations (ITAR) or other export-controlled information may be subject to other requirements. You may not have or store information subject to ITAR without a Technology Control Plan that has been approved by Research Compliance. Contact Research Compliance for details.

Terminology

"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 electronic or paper form and includes, but is not limited to, all academic, administrative, and research data, as well as the computing infrastructure and program code that support the business 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.

“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.

Roles

Enterprise Services

IS&T is responsible for ensuring compliance of IS&T supported devices and services with this policy. IS&T will provide guidance about the approved data classifications for each 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 their communities, or the University meet these minimum security standards, including specifying whether services are appropriate for each class of data.

Personal Responsibility

All BU faculty and staff 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, or Information Security.

Business Standards

Risk Based Controls

- Kiosks and terminals intended for unauthenticated public use must not store any Sensitive Information.
- Restricted Use data must only be stored on devices or cloud services that are approved for such use by Information Security.
- 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.
- Use authoritative data sources to minimize the number of copies of data, particularly Restricted Use data.

Systems Management

- Procedures should be in place for securing downtime on short notice to deploy critical security patches, particularly for server systems.
- Powerful accounts such as administrator, super user, or root should be granted only to those with a documented need.
- 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.

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:

- Services that will access, store or process Confidential or Restricted Use data should be evaluated by Information Security and the appropriate Data Trustee before use.
- Cloud service offerings should define the roles and responsibilities of both the cloud service provider and the university during a breach investigation initiated by either party.
- Cloud environments should be segregated (such as by subnet or AWS security groups) to separate test and production systems and data.
- Isolate security services including firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), Log Management, and IAM from other services.
- Limit administrative access to cloud infrastructure (IaaS) by requiring the use of a bastion host as a relay point for connecting into cloud instances. Use multifactor authentication for administrative access wherever possible.
- Secure Access Keys and Tokens should be rotated at least every 90 days.
- Use multifactor authentication to cloud service provider management applications wherever possible.
- Cloud Services must provide an exit strategy that enables the University to retain its data and to remove all data from the cloud service.
- The cloud provider must not mine or search University Data for purposes other than those approved by the University.
- Cloud providers that will store Confidential or Restricted Use data must document and contractually agree to implement strong physical access controls for their infrastructure.
- The unit procuring the cloud services must understand where and how cloud services 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.
- 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.
- The cloud provider must log all authentication attempts to provided services and be able

to export the data if requested.

- Restricted Use data must be encrypted at rest and while in transit; other data should be encrypted where reasonable to do so.

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 for storing University Data, including the use of free services.

- Confidential data should not be stored in Personal Cloud Services unless the service has been approved by Information Security and the appropriate Data Trustee.
- Personal Cloud Services may not be used for Restricted Use data.
- 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.
- 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.
- Do not use your BU Kerberos password for Personal Cloud Services.

Endpoint Devices

An endpoint device is a system that is intended for direct human interaction. By comparison, a server is intended to offer an application, storage, or other service and 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:

- Use an operating system (Windows, Mac OS, supported versions of 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.

- Configure your system and applications to receive and install updates automatically except where specific requirements prevent doing so.
  - Set up Windows Update or Mac Software Update to download and install automatically.
  - For mobile devices, use the native app store to download and install operating system and application updates automatically.
  - 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.
  - Where requirements prevent running fully updated software it may be necessary to deploy compensating controls. Consult with Information Security for these cases.
- 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
- Use biometric authentication (thumbprint, facial recognition, etc.) or set a strong PIN (alphanumeric), passcode, password or pattern on mobile devices. Many protections and security features of your phone (for example, the native encryption capability of the iPhone) are not activated unless you have turned on this security feature.
- Create a non-administrative account on your computer to use for normal day-to-day activities. This account should be a regular user account and not an administrative or root account.
- BU managed systems should be joined to the Active Directory
- BU managed systems should be managed in KACE
- 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.
- Install Endpoint Protection Software to protect your device from viruses, spyware, and other malicious behavior.
- If you have information on your computer or mobile device that is important to the operation of the University, back up that data on a regular basis.
- 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.
- If connecting 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 via the network.
- 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).

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

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.

- 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 (e.g., Windows XP, Windows 7, Windows Server 2003, Windows Server 2008, CentOS 5, RedHat Enterprise Linux 5), should not be used. For already deployed systems that cannot be upgraded, compensating controls must be in place.
- 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.
- Any default or vendor-supplied password must be changed to a non-default value that meets University minimum password complexity standards.
- System/Device based firewalls should be used where it is reasonable to do so, are recommended for systems with Confidential data, and required for systems with Restricted Use data.
- Data that is important to the operations of the University should be backed up to protect against loss of use. See the University Record Retention Policy (FA-002) for details.
- 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.
- 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.

- 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.
- Servers storing significant quantities of Confidential data or any Restricted Use data should be kept in secure rooms with strong physical access controls. Two factor physical access controls and video surveillance of these areas should be considered.
- 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.
- Reusable media (disk drives) should be securely erased when removed from service. When 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.
- Systems should be routinely scanned for vulnerabilities and discovered vulnerabilities should be remediated swiftly.
- 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.
- Endpoint Protection Software should be installed and tied to enterprise management and reporting utilities.
- Network services that do not have an associated need should be disabled.
- Non-Endpoint devices should be configured to sync time information (Network Time Protocol) from an established, credible source.
- 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.
- Non-production systems (e.g. Dev, TEST) should not store production Restricted Use data unless security controls equivalent to the production environment are in place.
- Where possible, authentication to Non-Endpoint devices or software should be from approved enterprise authentication services (e.g. Active Directory, Kerberos, Shibboleth)

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 policy.

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 (*This policy supersedes the previous versions entitled* “Data Protection Requirements”)
    - Minimum Security Standards [current webpage]
    - 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: Information Management, Privacy and Security Keywords: Data Security Standards