Effective Date: **March 1, 2020** Revised: **May 1, 2026**

**STANDARDS**

**EMPLOYMENT, INFORMATION MANAGEMENT, PRIVACY AND SECURITY**

# Data Center Security Standards

RESPONSIBLE OFFICE

**Information Services and Technology**

## Purpose

Information Security (InfoSec) is charged with helping to protect the University's data. This standard establishes the required safeguards at all data centers that provide services to the university broadly.

## Scope

This standard applies to all data centers that provide services to the university broadly. This includes space managed by external entities and rented or leased by the university to be used as data centers. For external managed data centers, Administrative Controls Standard #4 applies to BU staff with unescorted access to the data center, not the remote data center staff. Information Security can provide further guidance for negotiating agreements with external providers.

Units operating a data center to provide localized services should also comply with this standard to the extent practicable. If hosting NIST-compliant workloads, the data center must fully comply with this standard.

Cloud provided infrastructure, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) offerings should be evaluated during contracting to ensure the solutions are operated with similar levels of security. This review is required for any service that will host Restricted Use data.

# Standards

## Administrative Controls

1. The Data Center Service Owner shall develop, disseminate, and enforce procedures to implement this standard. This standard is reviewed annually by Information Security and the Data Center Service Owner.

2. Unescorted access to the Data Center is authorized by the Data Center Service Owner according to business need. To achieve separation of duties, the authorization from the Data Center Service Owner is implemented by a different office, such as Finance Administration or Public Safety. The Data Center Service Owner is responsible for providing timely access when requested, revoking access when notified of a change, and conducting periodic, at least annual, reviews to ensure accuracy of both the authorization and implementation of access controls. Information Security shall conduct

audits at least annually as well.

3. All physical media (e.g., hard drives, tapes, USB storage) must be inventoried by its owner, and when at end of life, physically destroyed by BU or an approved vendor. No failed media can be returned to a vendor without permission from Information Security, even if encrypted (Note: encrypted HIPAA data still requires a Business Associate Agreement with the vendor). Additionally, equipment removal must be approved by Data Center Service Owner.

4. All personnel with authorized, unescorted access to data centers must take initial and annual training that covers data center responsibilities. Completion of training is logged and audited.

5. Access by anyone who is not authorized for unescorted access is given a visitor badge that is documented in a log of access, and visitors must be escorted to the necessary rack/equipment. Logs of visitor access are reviewed by the Data Center Service Owner every quarter. Logs of visitor access are kept for at least one year.

## Physical and Technical Controls

1. Physical access to Data Centers is controlled by electronic locks using multifactor authentication. The Data Center Service Owner ensures that routine checks of physical security are conducted, including that all doors are kept secure and access controls are functioning properly. Keys are issued sparingly and are used for emergency access use only. Forced entry or holding doors open causes an alarm with immediate response requirements, and video surveillance records activity at entrances to data centers all hours of every day. Any issues are reported to appropriate responders, including the Incident Response Team (irt@bu.edu). This effort may be audited by Information Security.

2. Distribution and transmission lines are protected with conduit or cable trays, and access to networking closets and power equipment is controlled with keys or electronic locks. Emergency power shutoff is located within data centers to protect from unauthorized activation.

3. Power and environmental conditions are monitored, and deviations trigger an alert to

appropriate responders, such as Data Center Operations or Public Safety. Short-term power problems, such as surge or sag, are managed with Uninterrupted Power Supply (UPS) units or equivalent. Emergency lighting for exits and evacuation routes in facilities holding a data center automatically turn on for power outages.

4. Temperature and humidity are controlled with redundant systems, such as air conditioning units, in-rack cooling, or in-row cooling mechanisms.

5. Fire suppression systems are installed, operate without human presence, and are not dependent upon building power for operation. When activated, notification is sent to BU and emergency responders. Carbon Dioxide (CO2) canisters and other fire suppression systems are periodically tested.

# 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 Boston 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 IS&T and BUMC IT Data Center Policy, | Tracy Schroeder, VP of IS&T |
| Initial Publication of Data Center Standard | IS&T Policy and Standards Review |

# Appendix A: NIST Cyber Security Framework and SP 800.171 Mapping

The following table maps the National Institute of Science and Technology (NIST, nist.gov) Cyber Security Framework (CSF) and Special Publication (SP) 800-171 controls to standards expressed in this document. Fully implementing this standard with associated procedures and evidence of adherence to those procedures would likely indicate that all the controls listed here are met. However, compliance must always be evaluated for the scope of the information system in question, and having a standard by itself does not guarantee compliance. This document references NIST 800-171 revision 2.

| CSF Control | 800.171 Control | Control |
| --- | --- | --- |

| | | |
|---|---|---|
| PR.AC-2 | 3.10.1 | Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. |
| PR.AC-2<br>DE.CM-2<br>DE.CM-7 | 3.10.2 | Protect and monitor the physical facility and support infrastructure for organizational systems. |
| PR.AC-2<br>DE.CM-2<br>DE.CM-7 | 3.10.3 | Escort visitors and monitor visitor activity. |
| PR.AC-2<br>DE.DP-3 | 3.10.4 | Maintain audit logs of physical access. |
| PR.AC-2 | 3.10.5 | Control and manage physical access devices. |

# Appendix B: NIST SP 800.53 Mapping

The following table maps the National Institute of Science and Technology (NIST, nist.gov) Special Publication (SP) 800-53 controls to standards expressed in this document. Fully implementing this standard with associated procedures and evidence of adherence to those procedures would likely indicate that all the controls listed here are met. However, compliance must always be evaluated for the scope of the information system in question, and having a standard by itself does not guarantee compliance. This document references 800-53 revision 4.

| CSF Control | 800.171 Control | Control |
|---|---|---|
| PR.IP-5 | PE-1 | The organization develops, documents, and disseminates a phys and environmental protection policy that addresses purpose, sco roles, responsibilities, management commitment, coordination an organizational entities, and compliance. |
| PR.AC-2 | PE-2 | The organization develops and maintains a list of individuals with authorized access to the facility where the system resides. |
| PR.DS-3 | CM-8 | |
| PR.DS-3 | PE-16 | The organization authorizes, monitors, and controls entry and exi points to the facility. |
| PR.AC-2<br>DE.CM-7 | PE-3 | The organization enforces physical access authorizations at entry points by verifying individual access authorization before granting access. |

| CSF Control | 800.171 Control | Control |
|---|---|---|
| PR.AC-2 DE.CM-7 | PE-8 | The organization controls temperature and humidity levels within facility to reduce the risk of damage to system components. |
| PR.AC-2 DE.CM-2 DE.CM-7DE.DP-3RS.AN-1 | PE-3 | The organization enforces physical access authorizations at entry points by verifying individual access authorization before granting access. |
| PR.AC-2 DE.CM-2 DE.CM-7DE.DP-3RS.AN-1 | PE-6 | The organization protects the facility and system from fire damag |
| PR.AC-2 DE.CM-2 DE.CM-7DE.DP-3RS.AN-1 | PE-6(1) | The organization monitors physical access to the facility where th system resides using physical intrusion alarms and surveillance equipment. |
| PR.AC-2 DE.CM-2 DE.CM-7DE.DP-3RS.AN-1 | PE-8 | The organization controls temperature and humidity levels within facility to reduce the risk of damage to system components. |
| PR.AC-2 | PE-4 | The organization controls physical access to system distribution a transmission lines using defined security measures to prevent unauthorized access, accidental damage, and tampering. These measures include locked wiring closets, conduit protection, and wiretapping sensors to safeguard unencrypted transmissions. |

| CSF Control | 800.171 Control | Control |
|---|---|---|
| PR.AC-2 | PE-9 | The organization protects power equipment and power cabling fr damage, theft, and unauthorized access. |
| PR.AC-2 | PE-10 | The organization provides the capability to shut off power to the system or individual system components in emergency situations |
| N/A | PE-11 | The organization develops and implements emergency exit proce |
| N/A | PE-12 | The organization provides emergency lighting for emergency exit other appropriate areas. |
| N/A | PE-14 | The organization controls temperature levels within the facility to reduce the risk of damage to system components. |
| N/A | PE-13 | The organization provides fire extinguishers and other fire suppre equipment at appropriate locations within the facility, and maintai equipment in good working condition. |
| N/A | PE-13(1) | The organization employs fire detection devices/systems for the information system that activate automatically and notify [Assignr organization-defined personnel or roles] and [Assignment: organi defined emergency responders] in the event of a fire. |
| N/A | PE-13(2) | The organization employs fire suppression devices/systems for th information system that provide automatic notification of any activ to Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]. |

| CSF Control | 800.171 Control | Control |
| --- | --- | --- |
| N/A | PE-13(3) | The organization employs an automatic fire suppression capabilit the information system when the facility is not staffed on a contin basis. |

END OF POLICY TEXT

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