Effective Date: **May 1, 2026**

STANDARDS

EMPLOYMENT, INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Vulnerability Management Standard

RESPONSIBLE OFFICE

Information Services and Technology

Purpose

BU Information Security (InfoSec) is charged with helping to protect the University's data. Vulnerability Management is a process of identifying, evaluating, and mitigating security weaknesses in computer systems, networks, and applications to reduce the likelihood of cyberattacks and data breaches. Common vulnerability management tools consist of vulnerability scanners, patch management tools, and reporting and validation tools.

Scope

This standard applies to all devices connected to the university network.

Devices not in compliance with this policy must complete the risk acceptance process or be isolated in a way that prevents any potential exploitation, including being entirely disconnected from the network.

Standards

Vulnerability Management Program

The Chief Information Security Officer shall implement a Vulnerability Management Program that will provide:

- A vulnerability scanning service
- A patch management service
- A penetration test, at least once annually

The Chief Information Security Officer shall charter a Vulnerability Advisory Board (VAB) to: implement the Vulnerability Management Program; review and evaluate patch and vulnerability scan data; assign priorities to vulnerabilities; and coordinate remediation efforts.

Vulnerability Scanning and Announcements

Information Security will provide a Vulnerability Management program with the capability to continuously scan devices connected to the university network. Results will be provided to responsible device owners and administrators in a timely fashion.

Service Owners should subscribe to mailing lists, support groups, and other information sources to remain aware of vulnerabilities in their products. Information Security will make an effort to highlight critical vulnerabilities that come to their attention to appropriate Service Owners, but cannot monitor every possible vendor or know everyone who is using a particular product.

Required Access for Scanning

Vulnerability scans are significantly more accurate when they have access to the device operating system. To minimize risk to the device, use of an agent is preferred over direct authentication to the system. The use of one of these methods is required for all devices administered by faculty or staff for the benefit of the university.

Personally owned devices which primarily function as endpoint devices for their owner's use, or devices managed by other non-university entities (such as devices brought on-campus by vendors and guests), must comply with the program but are not required to provide access for scanning unless accessing or storing Restricted Use information, or being used in a research study with specific compliance requirements.

Patch Management

A patch management service will be provided to assist with the patching of servers and university managed endpoints. Administrators of endpoint devices not managed by the university must ensure their devices remain up to date in accordance with this standard. Device, Service, and Application owners/administrators are responsible for maintaining the currency of applications and devices and applications that cannot be patched by one of these methods.

Timeline for Remediation

Per the Minimum Security Standards, all devices connected to the university network are expected to be running currently supported operating systems, patched, and maintained regularly. This is an ongoing responsibility of device owners and administrators. All vulnerabilities, regardless of severity, need to be remediated within 60 days of becoming known to the university.

When new vulnerabilities are discovered, the Vulnerability Advisory Board will issue guidance on timelines for applying updates based on the difficulty of exploiting the vulnerability and the availability of fixes and compensating controls.

Penetration Testing

Information Security shall conduct penetration tests at least annually to validate the efficacy of the vulnerability management program and approved compensating controls in reducing risk. At least one test shall include identified critical or high-risk devices to test risk exposure. Findings from the penetration test will be remediated in the same manner as the routine vulnerability scans.

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.

Version History

Notes	Approver	D

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 CSF version 1 and 800-171 revision 2.

CSF Control	800.171 Control	Control
ID.RA-1 PR.IP-12 DE.CM-8 RS.MI-3	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems applications are identified.
ID.RA-1 PR.IP-12 RS.MI-3	3.11.3	Remediate vulnerabilities in accordance with risk assessments.

CSF Control	800.171 Control	Control
ID.RA-1 ID.RA-2 ID.RA-3	3.12.1	Periodically assess the security controls in organizational system determine if the controls are effective in their application.
PR.IP-12 RS.MI-3	3.12.2	Develop and implement plans of action designed to correct defici reduce or eliminate vulnerabilities in organizational systems.
ID.RA-1 ID.RA-2 ID.RA-3 PR.IP-12 DE.CM-4 RS.MI-3	3.14.1	Identify, report, and correct system flaws in a timely manner.

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 [this webpage]
  - Data Lifecycle Management Standard
  - Minimum Security Standards
  - 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)

History

This

Related BU Policies, Procedures, and Standards

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

History

This Vulnerability Management Policy became the the Vulnerability Management Standard - May 2026.

Management, Information Technology Use, Access, and Security, Privacy and Security
Keywords: patch management, scanning, Vulnerabilities, vulnerability, vulnerability management, Vulnerability Management Program, Vulnerability Management Standard