Effective Date: **May 1, 2026**

STANDARDS

Cyber Risk Management Standard

Purpose

The purpose of this standard is to establish a consistent framework for managing identified cyber risk. Cyber risk management is the overt act of accepting, mitigating, or transferring risks identified in a Cyber Risk Assessment. This requires an accountable party, the Risk Owner, to acknowledge the existence of the risk and make a formal statement about what the university should do about the risk by selecting between:

- **Risk Acceptance**, which may require additional approvers, depending on the severity of the risk.
- **Risk Mitigation**, which will require the Risk Owner to oversee remediation activities on a time scale agreeable to Information Security.

Once a risk to an asset, system, service, or process has been identified and evaluated by the Risk Assessment Standard, the designated Risk Owner must determine how we will respond to the risk. This standard outlines the options for responding and the timetable under which these decisions must be made.

Scope

This standard applies to all university departments, schools, and personnel responsible for managing or making decisions about information systems, applications, and data. It covers all areas of cyber risk, including software, hardware, and network architecture, on all forms of electronic devices that store, process, or transmit University Data.

Defined Terms

Risk: An assessment of the risk of continuing to operate with an identified vulnerability in an asset, system, service, or process after all compensating controls are considered. The risk may change over time as changes in threats and controls occur, including those outside of the asset, system, service, or process.

Risk Assessment: A document containing one or more identified risks.

Risk Acceptance: A risk management strategy where an organization or individual acknowledges the existence of a specific risk and chooses not to take any immediate action to mitigate or transfer it. Risk Acceptance should be time-bound, forcing periodic reassessment.

Risk Mitigation: A risk management strategy where actions are taken to reduce the likelihood or impact of a specific risk to an acceptable level. It is important to note that mitigation does not have to entirely resolve the risk, it may just reduce the likelihood or impact to achieve a lower risk severity.

Roles and Responsibilities

Risk Owner: The individual most directly accountable for remediation of the risk. This may be a service owner, project sponsor, business owner, unit lead, or other individual who would commit resources to correct an identified risk.

Risk Approver: A person authorized to accept the risks on behalf of the university. While the Risk Owner always has this role, multiple approvers may be necessary for some severities of risk.

BU Information Security: Overseen by the Chief Information Security Officer, this group is responsible for ensuring the identified risks are clearly communicated and triaged according to this standard in a timely fashion.

Standards

1. All decisions must align with the university's mission, risk appetite, and regulatory obligations. A Risk Owner should seek advice of Information Security, senior leadership, and counsel as necessary.

2. The Risk Owner will determine if the risk shall be accepted or mitigated.

3. The Risk Owner will make the determination within two weeks of being notified of the risk.

4. If a risk will be mitigated, the mitigation work must be completed within a timeframe commensurate with the risk.

	System contains University Data	**System does NOT contain Univers (e.g. Pre-production)**
Critical Risk	Within 5 days	Within 2 weeks
High Risk	Within 2 weeks	Within 4 weeks
Moderate Risk	Within 4 weeks	Within 90 days
Low Risk	Within 90 days	Within 180 days

5. The Risk Owner is responsible for ensuring that the mitigation is complete within the proposed timeframe. If a risk cannot be mitigated within the time frame, the risk should be accepted.

6. A secondary approval is required from a different individual based on the risk severity to accept or transfer a risk.

7. A risk that can be mitigated in the specified time frame does not require a secondary approval.

8. If multiple risks are grouped into one assessment document, any required secondary approver is based on the highest severity risk.

a. Low Risk: Unit lead or Chief Information Security Officer (CISO)

b. Moderate Risk: Unit lead and Chief Information Security Officer (CISO)

c. High Risk: Unit Dean or Vice President; and Chief Information Officer (CIO)

d. Critical Risk: Unit Dean or Vice President; and Chief Information Officer (CIO)

9. Information Security will ensure that risk management decisions are made and approved within two weeks.

10. Risk Management decisions must be reviewed annually or when there is a significant change in the system, process, or threat landscape.

11. All risk management decisions will be documented, along with any required approvals, in Information Security's Cyber Risk Register.

12. The outcomes of the cybersecurity risk management strategy are regularly reviewed by the Chief Information Security Officer to inform and adjust the organization's cybersecurity strategy.

13. The cybersecurity strategy is periodically reviewed and adjusted to ensure effective, efficient, and comprehensive coverage of organizational requirements and risks.

Procedures

Registration of Risk

All completed Risk Assessments are documented in Information Security's Cyber Risk Register. Each risk within an Assessment will have an assigned risk severity. Information Security shall notify the Risk Owner when a new Risk Assessment is recorded.

Review and Disposition of Risk

The Risk Owner shall review each risk and determine if:

- **The risk should be accepted.** The cost/benefit analysis of this risk suggests that the time or expense required to mitigate the risk is greater than the risk itself, or the risk will take longer to mitigate than the permitted time to mitigate the risk. Risk Acceptance should be time-bound, forcing periodic reassessment.
- **The risk should be mitigated.** The risk owner will work with the necessary staff to mitigate the risk per the timetable.

Approval of Decision

The Risk Owner shall always make the initial determination of how a risk will be managed. The determination will include a statement about why the option was chosen.

Secondary Approval

A secondary approval is required from a different individual based on the risk severity to accept or transfer a risk. Information Security shall assist in routing the approval form to the appropriate approvals.

Review and Monitoring

Risk Management decisions must be reviewed annually or when there is a significant change in the system, process, or threat landscape.

Escalation and Remediation

Information Security will ensure that risk management decisions are made and approved within two weeks or shall escalate the risk to management.

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 Cyber Risk Management Standard	IS&T Policy and Standards Review Commi

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
GV.RM-01		Risk management objectives are established and agreed to by stakeholders
GV.PO-01		Policy for managing cybersecurity risks is established based c context, cybersecurity strategy, and priorities and is communic enforced

GV.PO-02		Policy for managing cybersecurity risks is reviewed, updated, and enforced to reflect changes in requirements, threats, tech organizational mission
GV.OV-01		Cybersecurity risk management strategy outcomes are review adjust strategy and direction
GV.OV-02		The cybersecurity risk management strategy is reviewed and a ensure coverage of organizational requirements and risks
GV.OV-03		Organizational cybersecurity risk management performance is reviewed for adjustments needed
ID.RA-06		Risk responses are chosen, prioritized, planned, tracked, and
ID.RA-07		Changes and exceptions are managed, assessed for risk impa and tracked

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 Cyber Risk Management Standard was enacted May 2026.