Effective Date: **May 1, 2026**

STANDARDS

EMPLOYMENT, INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Log Collection, Analysis, and Retention Standard

RESPONSIBLE OFFICE

Information Services and Technology

Purpose

Information Security (InfoSec) is charged with helping to protect the University's data. To appropriately protect the University, as well as ensure normal operations of IT services, applications, systems and required devices must appropriately generate, store, and make available logs that record significant events within the IT infrastructure. Security software, operating systems, and application log data as well as any other relevant logs are critical components in detecting, analyzing, preventing, and responding to information security incidents, including unauthorized data disclosures, on university systems.

The key objectives of this Standard are to:

- Describe the university's approach to computer security log management, including roles and responsibilities, proper handling of logs, and privacy considerations;
- Ensure appropriate log collection, monitoring, and analysis infrastructure is in place so

that cybersecurity incidents can be detected, investigated, and responded to in a timely and efficient manner;
- Ensure that appropriate log collection, analysis, and retention are in place to satisfy legal, regulatory, and contractual requirements including mandated reporting.

Scope

This standard applies to all university-managed devices connected to the university network containing non-public university information, and all applications handling non-public university information operated by or for the university.

This does not include personally owned devices unless they are used for handling Restricted Use data (which is discouraged as a practice) or have a research Data Use Agreement that requires a high level of data protection. Information Security can assist with research related questions.

Devices and applications not in compliance with this standard must complete the risk acceptance process or discontinue use of non-public university information.

Defined Terms

Security Log Data are a subset of all records of events created by security software, operating systems, and applications that are deemed critical elements in detecting, analyzing, preventing, and responding to cybersecurity incidents on university systems.

Security Log Data has some or all of the following properties or must be configured to collect the following properties:

1. It identifies identity and/or location data (including IP addresses) of significant security events including:

    a. successful or failed authentication or authorization activities

b. the escalation of privileges within an application or system, including impersonation of another individual or system account

2. It can identify anomalies in system or application behavior that threaten the confidentiality, integrity, or availability of university services and requires further investigation, including:

a. changes to system configuration, particularly related to identity and access management functions

b. execution of unusual commands for a user of this application or system

c. probing the system for vulnerabilities

This data does not generally include the contents of applications, messages, and filesystems except when included in a logged event beyond the control of the university. A more technical definition is provided in the standard below.

Roles and Responsibilities

Information Security

- Provides a Log Monitoring and Analytics service that will collect and analyze Security Log Data from all systems and applications that are in scope.
- May provide supplemental guidance on what types of logs should be sent or not sent, configuration of specific vendor log collection capabilities to ensure required information is available, available mechanisms for receiving them, and log retention issues. May also determine that certain types of logs should not be sent due to value or volume.
- Determines who may access aggregated logs within Log Monitoring and Analytics service for what purposes.
- Conducts investigative work related to Security Log Data and makes security-related recommendations to help mitigate risks discovered through log monitoring.

Device and Application Administrators

- Configures application and devices to submit log data according to this standard, which may also include researching the necessary options and capabilities to identify

appropriate logs and available mechanisms from our various vendors.
- Ensures the logging configuration is appropriate to any special legal, contractual, or regulatory requirements impacting their systems (HIPAA, PCI, Research Data Use Agreements).
- Seeks support from Information Security with questions about types of logs, available methods, and retention issues.
- Support investigative work related to Security Log Data. In particular, these individuals may be called upon to provide subject matter expertise on specific recorded events.

Individuals with Access to Security Log Data

- Individuals given access to Security Log Data on a device, in an application, or within the Log Monitoring and Analytics service must:
    - Use the data only for the purposes for which access has been authorized.
    - Abstain or prevent the sharing of data with anyone not otherwise authorized except as approved under the Access to Electronic Information Policy.

Standards

1. Requirement to record and forward Security Log Data

Security Log Data must be generated, recorded, and forwarded to the Log Monitoring and Analytics service to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. This must be implemented according to the following table.

- Systems and applications that cannot generate or forward logs and are required to do so must seek an exemption from Information Security.

Logging of Data by Multiuser systems and applications	Required	Required

Logging of Data by endpoint (Single User) systems and applications	Required	Recommended
Logging of Data by Non-User Devices (Internet of Things)	Required when possible	Required when possible

2. Requirement to retain Security Log Data

Security Log Data must be retained by the generating system or application according to the following table. The table specifies the minimum and maximum retention value.

- Systems and applications that cannot locally retain log data according to the following table and are required to do so per standard #1 must seek an exemption from Information Security.
- For systems that use log size-based retention rather than age-based retention, a good faith effort must be made to appropriately size the log file.
- Logs must be maintained in a format that allows them to be immediately available up to the minimum time requirement and available within 2 hours for as long as the log is maintained.
- Certain regulations like PCI may require logs to be retained for a longer period of time. Always comply with the most specific policy or standard applicable to your system or application.
- Retaining log data that contains personally identifiable information beyond the maximum retention is not permitted without an exemption from Information Security. Deidentified data used for statistical purposes may be retained for longer periods.
- Information Security may extract and retain log data related to cybersecurity incidents indefinitely and may share the extracts to resolve security incidents according to business need. These investigations must be consistent with the Cyber Incident Response Policy and Access to Electronic Information policy.

All	**Minimum: 14 days** **Maximum: 90 days**	**Minimum: 14 days** **Maximum: 90 days**	**Minim** **Maxim**

3. Requirement to Detect Log System Failure

Device and Application Administrators must implement technical and administrative controls to ensure that logging remains active for all devices and applications. Any failure must be escalated for immediate attention. Unexplained failures must be reported to Information Security.

4. Requirement for timely logging of Security Log Data.

All Security Log Data should be recorded on the local system immediately.

Data forwarded to the Log Monitoring and Analytics service should reach the service within 5 minutes for Restricted Use devices and applications and within 30 minutes for other consumers of the Log Monitoring and Analytics service. Systems that are offline may not be able to comply with this requirement while offline but should commence sending all data once connected within these time parameters.

5. Requirements for Integrity of Security Log Data.

Security Log Data must be protected from unauthorized changes or deletion. Security Log Data repositories should only be writeable by the logging subsystem within the device or application. User data stored as part of log data must be sanitized, and Restricted Use data must be redacted or masked.

6. Access Control for Security Log Data.

Appropriate access controls must be implemented to ensure that only authorized individuals have access to Security Log Data.

- Security Log Data stored by the generating device or application must only be readable by individuals with a business need to access the data.

- Access to Security Log Data within the Log Monitoring and Analytics service will be provided based on business need and impact on privacy. Access decisions will be approved by the Director of Information Security with oversight from the Chief Information Security Officer.
- Use of these logs for purposes other than to protect the University, as well as ensure normal operations of IT services, applications and systems, such as academic or research purposes, must be approved by the Chief Information Security Officer. Depending on the circumstances, review by the Provost, Office of the General Counsel (OGC) and/or Institutional Review Board (IRB) may also be necessary.
- Release of log data to any party not normally authorized to read it shall adhere to the Access to Electronic Information Policy.

7. Technical Specification of Security Log Data

Logs must show the source, account, time, type, and location related to the event. Logging must be configured to record the following events when possible:

- Successful and unsuccessful logins and authentication;
- Authorization failures;
- Physical access authorizations, both success and failure;
- Password changes;
- Modification of security settings;
- Software installations;
- Mass file deletions/downloads;
- Group membership changes;
- System or network configuration changes;
- Access control changes;
- Access to or modification of data classified as Restricted Use;
- Privileged actions, such as those actions requiring administrator, sudo, or root access;
- Detection of suspicious or malicious activity from IT security systems, such as from an intrusion detection system or antivirus system.

8. Review of Logging Requirements

- Information Security will review the requirements of this standard at least annually and update as needed to ensure the objectives of this policy are met. Information Security may also generate guidelines between review cycles to clarify requirements.
- Device and Application Administrators should periodically review the standards to ensure ongoing compliance with the requirements.

9. Requirement to Review and Correlate Security Log Data

- Information Security shall configure the Log Monitoring and Analytics service to correlate Security Log Data and report on events requiring further analysis, reducing the overall volume of events for which review is required.
- Information Security shall analyze data within the Log Monitoring and Analytics service for indications of unlawful, unauthorized, suspicious, or unusual activity.
- Information Security shall escalate issues of concern, ensuring proper investigation and reporting.
- Device and Application Administrators may be called upon to help investigate or clarify how logs should be interpreted in the context of the system or application.

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 Log Collection, Analysis, and Retention Standard	IS&T Policy and Standards R

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
PR.AC-4	3.1.7	Prevent non-privileged users from executing privileged functions a capture the execution of such functions in audit logs.
PR.PT-1 DE.AE-2 DE.CM-3 DE.CM-7	3.3.1	Create and retain system audit logs and records to the extent nee to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity
PR.PT-1 DE.AE-2 DE.CM-3	3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.
PR.PT-1	3.3.3	Review and update logged events.
PR.PT-1	3.3.4	Alert in the event of an audit logging process failure.
PR.PT-1 DE.AE-2 DE.AE-3 RS.AN-1	3.3.5	Correlate audit record review, analysis, and reporting processes f investigation and response to indications of unlawful, unauthorize suspicious, or unusual activity.
PR.PT-1	3.3.6	Provide audit record reduction and report generation to support on demand analysis and reporting.
PR.PT-1	3.3.8	Protect audit information and audit logging tools from unauthorize access, modification, and deletion.

CSF Control	800.171 Control	Control
PR.PT-1	3.3.9	Limit management of audit logging functionality to a subset of privileged users.

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 Log Collection, Analysis, and Retention Standard was enacted May 2026.

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