INFORMATION TECHNOLOGY SERVICES
George Mason University

ITS Logging Standards

Document Version Number:	2.1
Document Control Number:	ITS.ITSO-STD001
Last Updated:	12/8/2025
FOIA Exempt?	No

Process Owner:

- Cybersecurity Operations

NOTICE TO ALL USERS:

The Cybersecurity Operations office will pause the onboarding of new log sources from January 2026 to April 2026 as we will be actively working on migrating existing log sources and user content to a new SIEM tool. In the meantime, please notify us of your new log source by emailing itsoengineer@gmu.edu so we can add your request to our queue. We will reach out to you about the next steps upon completion of the SIEM migration.

PURPOSE:

Logging is a necessary measure for identifying, responding to, and preventing events such as operational problems, security incidents, policy violations, performance issues, and fraudulent activities. This document states the requirements for log details, log handling, and exceptions. It also defines the responsibilities of each key personnel.

SCOPE:

This document provides a framework for ensuring that critical system and application information is captured accurately as logs and forwarded to Information Technology Services (ITS) log repository for security monitoring, auditing, and troubleshooting purposes. It defines:

- what should be logged
- what should be monitored
- how to guarantee log delivery through local log retention policy
- how log data should be released or shared
- how to handle exceptions to this Standard

This standard applies to all ITS log sources, and others that IT Risk and Compliance (ITRC) have identified.

The document does not cover how to setup log forwarding agents as this is outlined in ITS procedures.

REQUIREMENTS:

1. Log Details and Classification

The level of log detail should be sufficient to address the following information:

- When the activity occurred
- Who performed the action and where the action originated
- What action was performed
- Result of the activity (success / failure)

Logging and monitoring are crucial for maintaining the integrity, confidentiality and availability of systems and applications. The Administrators will be responsible for determining the type of events that need to be logged and monitored based on the impact of those events on the confidentiality, integrity and availability of their systems and applications. The administrators should refer to the Appendix for a list of different log categories, fields to log, events to monitor, monitoring frequency and monitoring responsibility. Annual audits require logging and monitoring to occur in accordance with this Standard, the Appendix to this Standard, the IT Security Standard and all related documents listed within this Standard.

For further examples of log entries (e.g., firewall logs, operating system logs, etc.), please refer to Section 2 ("Introduction to Computer Security Log Management") of the NIST Special Publication 800-92, Guide to Computer Security Log Management. This document is available at: https://csrc.nist.gov/pubs/sp/800/92/final.

2. Log Handling
   a. Log Integrity

      Logs may be relevant in legal proceedings and must be protected against tampering, modification, destruction, and unauthorized access. Administrators must not erase, disable, or modify any logs outside of well-defined and documented log rotation procedures.

      i. Log Sensitivity

         Logs may contain restricted or confidential data and must be handled in a manner that is consistent with this sensitivity.

      ii. Chain of Custody

         As logs may be relevant to legal proceedings, it is important to have appropriate controls to maintain the chain of custody by sending logs in near real-time to the ITS Centralized Log Repository.

   b. Local Log Retention Periods

      Log data should be retained on the system long enough to guarantee delivery to the Centralized Log Repository. Administrators need to ensure that the logs are available locally on the system even if they stop being forwarded to the Centralized Log Repository during University Holidays. It is recommended to store critical server logs locally at least a day longer than your typical response time during weekends and University Holidays. Network devices have limited space for storing logs locally. Hence local log retention period would vary based on the type of device or appliance and the criticality of events being logged. For further guidance around local log retention requirements, please contact Cybersecurity Operations.

   c. Timestamping and Synchronization

All log records must contain a timestamp, including date, time and time zone. All systems generating logs must be in sync with ITS-approved Network Time Protocol (NTP) servers and be configured to use Eastern Time Zone with Daylight Savings (EDT.) If this is not possible, the timestamp should be in Coordinated Universal Time (UTC). For a list of ITS-approved NTP servers, please refer to the ITS Service Catalog.

d. Log Review

The logs (events) shall be stored in the ITS Centralized Log Repository for automated processing and on-demand retrieval in searches and visualizations. Regular review of actionable events is required by Internal and External University audits. Log event monitoring guidelines and responsibilities of the System or Device Administrator, the Application Administrator and Cybersecurity Operations Analysts have been outlined in the Appendix to this document.

e. Release of Log Information

Disclosure of logs is governed by a number of state/federal regulations and industry standards. Handling of data classified by George Mason University is governed by all applicable University Policies. Processes for the release of logs that contain data that has been classified as Protected Data according to University Policy 1114 to persons or entities by any means must be reviewed by Cybersecurity Operations. A data-sharing agreement or other university-approved non-disclosure agreement must be completed by the system owner or their delegate prior to sharing classified data and be reviewed by Cybersecurity Operations. The following are examples of related regulations and industry standards:

- Federal Information Security Management Act of 2002 (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Sarbanes-Oxley Act (SOX) of 2002
- Payment Card Industry Data Security Standard (PCI DSS)
- Family Educational Rights and Privacy Act (FERPA)

COMPLIANCE:

Compliance with this Standard will be monitored by Cybersecurity Operations, ITRC, and auditors using evidence from ITS log repository, documentation of exceptions, and communication chains pertaining to release of log data

EXCEPTIONS:

While exceptions to these Standards weaken security posture, it is recognized that some exceptions may be necessary for reasons such as system resource limitations, performance impact, etc. For any deviation from these Standards, a request for exception must be submitted to ITRC.

DEFINITIONS AND ACRONYMS:

Terminology or Acronym	Definition
Administrator	Person(s) designated as directly responsible for the management of an IT system. For example, for a server, this would be the system administrator; for a database, the database administrator; for an application, the application administrator. Every log generation source must have one or more designated administrators who comply with this logging Standard.
Centralized log repository	The centralized log repository is the central repository for log data generated by systems. The centralized log repository is currently Splunk.
Centralized log repository Administrator	Person(s) designated as responsible for the administration of the centralized log repository. As such, this group has access to all logs in the centralized log repository. Any need for log correlation across log ownership boundaries will be coordinated with the centralized log repository administrator when approved byCybersecurity Operations. The log repository administrator is responsible for maintaining the documentation for log forwarding guides and procedures.
Cybersecurity Operations	Cybersecurity Operations is responsible for: • Providing processes for release of log information as specified in the Release of Information section of this standard; • Providing processes for log forwarding to the centralized log repository • Overall logging and monitoring security function
IT Risk and Compliance (ITRC)	The IT Risk & Compliance is responsible for: • Maintaining records of system eligibility for inclusion under, or exclusion from, the logging policy • Providing system risk assessments and system classifications for the purpose of determining log detail requirements
Log (Event)	A log is a system-generated record that provides information on an event or activity observed by that system. This data can be stored in one or more places, such as system logs, application logs, or appliance/device logs.
System Owner	The system owner is the direct supervisor of the administrator who is responsible for all the systems within that group or department. For example, the system owner is typically the manager in a department. If the department does not have a manager, the system owner would be the director in that department.

REVIEW SCHEDULE:

Annually

Titles and department names are subject to organizational changes.

INFORMATION TECHNOLOGY SERVICES
George Mason University

APPROVAL:

Title, Department Name	Name	Signature and Date
Chief Information Security Officer / Enterprise Cybersecurity	Matthew Dalton	Signed by: [signature] 12/17/2025 BFBBE97BAA404AA...
Vice President and Chief Information Officer / ITS	Charmaine Madison	Signed by: Charmaine Madison 12/17/2025 213112EC65F44A7...

REVISION HISTORY:

Date	Version Number	Department or Author	Brief Description of Changes
3/18/2019	1.0	IT Security Office / Nabiha Hasan	Initial Release
8/4/2020	1.1	IT Security Office / Nabiha Hasan	Minor revision - reformatting
9/15/2020	1.2	IT Security Office / Nabiha Hasan	Minor revision – updated Curtis McNay's title
3/2/2021	1.3	IT Security Office / Nabiha Hasan	Minor revision – mechanics, grammar and reference number correction
3/9/2023	1.4	IT Security Office / Nabiha Hasan	Annual review with minor revisions (reformatting and syntax)
3/11/2024	1.5	IT Security Office / Nabiha Hasan	Annual review without revisions.
6/20/2025	2.0	ITS / Matthew Dalton IT Security Office / Nabiha Hasan	Annual review with major revisions including content reformatted using the updated template.
12/8/2025	2.1	Cybersecurity Operations / Nabiha Hasan	Included note section and minor edits to appendix, updated departmental name from IT Security Office to Cybersecurity Operations.

RELATED DOCUMENTS/REFERENCES:

- Data Stewardship Policy (University Policy Number 1114)
- Information Technology Security Program (University Policy Number 1311)
- NIST Special Publication 800-92, Guide to Computer Security Log Management
- ITS.ITSO-PROC002_Log_Configuration_Procedure_for_UNIX_LINUX_Servers_v1.5final_Level3.pdf
- ITS.ITSO-PROC003_Log_Configuration_Procedure_for_Windows_Servers_v2.3final_Level3.pdf
- Logging Cheat Sheet - OWASP Cheat Sheet Series: https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.htmlhttps://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

Titles and department names are subject to organizational changes.

Appendix

Log Type	Events to Log	Required Fields	Events to monitor	Monitoring Frequency	Responsibility	Security Objective	Entity (User/System/Data)
Security Event	Malware detected / prevented Phishing reported / prevented / links clicked Suspicious file, process, code / library Known attack framework Potentially Unwanted Application (Attempted) Removal of security agents Confidence threshold met using ML Defense evasion Collection / discovery events IPS events	time (impacted) device IP DNS (optional) username (optional) signature action description category severity file hash (optional)	Trends in security tool alerts Network threat monitoring	Weekly	ITSO	CIA triad	User, System and Data
OS System	password changes service restarts / stop / starts host firewall changes system errors and warnings scheduled jobs hardware alerts system configuration changes user logins	time host name process name message username (optional) event type / code vendor product (optional)	Undocumented / unexpected changes unexpected stops and restarts of services/daemons logins outside of business hours location of logins for anomalies user lockout and failed actions system and hardware alerts new scheduled jobs added to system out of cycle password changes for regular users and service accounts	Weekly	System Administrators	Integrity and Availability	System and Data

Appendix

Enterprise Authentication and Multi-Factor Authentication	authentication success authentication failures authentication errors MFA success MFA failure MFA device registration MFA lookout	time source DNS / IP destination DNS / IP Description username / account name/ID result vendor product event message category destination port (optional) application name failure reason	attempts outside of business hours numerous attempts from one source reported fraud authentication events multiple sessions (simultaneous and after expiration) abnormal travel or authentication history	Weekly	ITSO for central authentication, cloud infrastructure, VPN, and local network. Application admins for applications Networking team for network device authentication for management.	Confidentiality and Integrity	User, System and Data
Network Traffic	allowed traffic blocked traffic	time source IP /zone / port destination IP / zone / port rule action application log (sub)type location bytes in / out translated IPs	abnormal outbound SSH connections traffic above/below baseline significant amount of blocked connections traffic matching threat intel/feeds	Weekly	ITSO	Integrity, Availability	System and Data
Network Device Syslog	device authentication system warnings and errors process/service state security/authorization messages configuration changes system alerts facility numbers responding to security objective (Integrity and Availability of the System)	time facility description / log subtype host / device name subsystem / process name application username (optional) source / destination IP (optional) severity	unexpected device reboots systems/process warnings or errors unexpected configuration changes authentication to administrative console outside business hours	Weekly	Networking Ops and Engineering	Integrity, Availability	System

Appendix

Web Activity	event logs http methods service warnings and errors cookie requests WAF logs (if implemented)	time message log level username client IP page URL domain user agent string HTTP status HTTP method bytes received bytes transmitted	unexpected behavior or requests that should be considered malicious indicators of vulnerability exploitation high volume of requests from single source IP address suspicious file uploads via POST or PUT potential shell/script upload	Weekly	Web Application Admins (operationally) ITSO (during Incident Response)	Integrity and Availability	System and Data
Privileged User Activity	DUO administrative actions PIM activation Privileged AD account usage Superuser activity and sudo commands privileged network activity/commands application admin activity user provisioning/decommissioning all actions performed by orchestration/IaC tool user modifications group modifications	time operation type operation name user / privileged user old / new values action approve / deny command event code	unexpected or undocumented changes risky privileged commands data exfiltration activity outside normal business hours long sessions numerous configuration changes in a short time Duo administrative management changes unusual/unexpected logins to systems from orchestration servers users added to privileged groups/roles	Weekly	Applications monitored by application owners and admins Systems monitored by system owners and admins ITSO for Duo, Azure, PIM activations, Tier0 admin accounts, and other enterprise privilege activity. Networking teams for networking or infrastructure systems	Confidentiality, Integrity, and Availability	User, System and Data

Appendix

DHCP	DHCPDISCOVER DHCPREQUEST DHCPINFORM DHCPACK DHCPOFFER DHCPDECLINE DHCPNAK DHCPRELEASE	time action dhcp_server dhcp_type signature IP mac address device response	monitor for unauthorized devices on the network multiple dhcp request and ACKs for one device in a short time duplicate MAC addresses attempting to steal static addresses	Weekly	ITSO	Confidentiality, Integrity, and Availability	System
Physical Access Control	access to protected spaces changes to access controll list	time username building / office action	unexpected/undocumented changes unexpected access outside business hours logs for a door held open or ajar	Weekly	ITSO	Confidentiality and Integrity	System and Data
Network Access Control	vpn connection initiated vpn connection established vpn connection failed vpn connection ended access control policy changes	time username action description source IP destination IP device (translated) source IP (translated) port duration message id / type bytes in / bytes out	multiple failures / multiple locations unexpected users added to / removed from VPN groups VPN activity from compromised accounts Notably short / long VPN sessions	Weekly	ITSO: Failures, locations, session anomalies Networking Groups: VPN group changes, configuration changes on networking device(s)	Integrity and Availability	User and System
Database Audit Log	DBA authentications database user/group modifications database configuration changes changes made to sensitive tables dropping any table DBA adding/changing specific data in tables DBA manually deleting data in tables database warning and errors	time username OS user server name source database source host / IP Service Name action code dbid sql statement sql text sql bind values bind variables	direct logins outside of business hours unexpected/undocumented changes made to users, groups, databases, or other objects notable warmings or errors	Weekly	DBAs	Confidentiality, Integrity, and Availability	System and Data

Appendix

DNS	DNS protection tool logs DNS event logs DNS audit logs	time device query action source IP device name reply code / response code	trends in DNS traffic, requests, and/or responses queries with threat list matches unexpected/undocumented changes unexpected zone transfers monitor newly seen domains by DNS protection tool	Weekly	ITSO	Integrity and Availability	System
Backup Server Logs	logins to backup servers/systems copy/update/delete of backup files changes to backup configuration status of scheduled backups warmings or errors of scheduled jobs logins from backup systems to other servers (if authorized)	time message volume name clusters status severity event type object type backup client host name backup file set name (optional) duration incident ID (optional) authentication (central) job status user action	unexpected/undocumented changes to backup files or configurations logins outside of business hours logins to other systems warmings or errors actions that copy backup files	Weekly	Server administrators and Backup Application administrator	Confidentiality, Integrity, and Availability	System and data

Appendix

Security Scan Log	active scan results passive scan results plugin update audit records authentication to scanning infrastructure audit logs	time IP severity cvss score cve plugin ID / name / output description exploit available type last seen OS port / protocol (optional)	difference in scanned assets based on previous scan exploitation attempts of vulnerable systems multiple authentications in a day to the scanning infrastructure failed plugin feeds failed scans changes made to scan policy changes made to asset list user and group modifications	Weekly	ITSO	Confidentiality and Integrity	System and Data