System XX Logging and Monitoring Plan

Last Update: {Enter date procedure was approved}

**Procedure Owner:** {Enter procedure owner, typically business owner}

Contents

[Logging and Monitoring Plan Purpose 1](#_Toc162368178)

[On-Premises Systems 1](#_Toc162368179)

[Scope 2](#_Toc162368180)

[Logging Requirements 2](#_Toc162368181)

[Log Retention 3](#_Toc162368182)

[Logging System Configuration 4](#_Toc162368183)

[Log Correlation 4](#_Toc162368184)

[Monitoring 5](#_Toc162368185)

[SaaS Vendors 5](#_Toc162368186)

# Logging and Monitoring Plan Purpose

{Customize this} Many of the University’s systems house confidential data such as personal data (Category 3) or federally protected data such as student data (FERPA, Category 4). University personnel are tasked with due care to protect this data. An important part of data protection is to log {customize following items} application, system, database, and data access, then preserve those logs in case an investigation is needed. Logs must be sufficient to reconstruct events such as data corruption, data exfiltration, system tampering, malware installation and activity, configuration changes, and unauthorized user activities.

In addition to their collection, logs must be periodically reviewed to check for security violations. This may be done by manually inspecting logs or using automated tools. Logs may also be sent to a log management system and monitored using dashboard, reporting, and alerting features.

{Remove below if not relevant}

# Responsibilities

{add title, position, or name of person} serves as the system steward (business owner) and {add title, position, or name of person} serves as the system custodian (technical leads). They must ensure system logging practices meet University requirements.

## Scope

The scope of logs collected must be adequate to meet the logging plan’s purpose.

**The critical logs to be collected from this system are**: {Remove irrelevant items below}

Application logs {specify}.

Database logs {specify}.

System security logs.

Other system logs {specify}.

Web logs {specify}.

Virtualization platform logs {specify}.

Container (Kubernetes) logs {specify}.

Authentication logs {specify}.

Cloud activity audit logs {specify}.

{specify other}.

## Logging Requirements

{you can modify below, but do not remove compliance requirements}

The University logging strategy must comply with University, State, and federal requirements. The minimum requirements for logging should include:

* Login/log off events.
* Denied access requests to resources (invalid logical access attempts).
* System configuration changes.
* Creation or deletion of System objects (e.g., processes, user accounts).
* Use of privileged commands/functions (e.g., using sudo in a Linux System to restart the System).
* Actions taken by privileged user accounts (e.g., Using Administrator on a Windows, or using root on a Linux System).
* Any changes to the configuration of the logs themselves including initialization of logging, clearing of logs, and changes in retention settings.
* Any additional events, exceptions, or other user activities necessary to reconstruct unauthorized activities for a System.

Additionally, for applications housing confidential data:

* Access to confidential data (e.g., read, update, or delete events).

**Describe logs collected and indicate if any of the required logs will not be collected:**

{specify}

Requests to deviate from these requirements should done in writing using the [Exception to Policy](https://security.wwu.edu/files/2021-07/2021%2002%2008%20Exception%20to%20Policy_0.docx) form and approved by the Information Security Office.

## Log Retention

The schedules which logs should be retained and destroyed should follow the Washington State Agency and Western Washington University retention schedules. Table 1 has a summary of the retention schedules for some common logs.

*Table 1 - Log Retention Schedule*

|  |  |  |
| --- | --- | --- |
| Record Type | Full Description | Retention and Disposition Action |
| Audit Trails and System Usage Monitoring Records | Records that document the use of the University’s information technology and communication Systems to ensure security and appropriate use.  Records include, but are not limited to:   * Audit trails * Authorizations for and modifications to the configurations and settings of the University’s IT infrastructure (such as firewalls, routers, ports, network servers, etc.) * Log-in records * Security logs * System usage files * Internet activity logs (sites visited, downloads/uploads, video/audio streaming, etc.) * Fax and telephone logs.   Note:  Excludes records covered by Internet Browsing Records schedule | **Retain** for 1 year after date of activity then **Destroy** |
| Internet Browsing Records | Records routinely generated as part of internet browsing. Include, but are not limited to:   * Browsing history/saved passwords/web form information, etc. * Cache/temporary files * Cookies   Excludes internet activity log records covered by the Audit Trails and Systems Usage schedule | **Retain** until no longer needed for University business then **Destroy** |
| Authorization – Systems/Telecommunications Access | Records documenting the authorization of employees (including contractors and volunteers) to use University Systems/applications and telecommunication services. Includes, but is not limited to:   * User account creation/change requests * Network access authorization requests * Related correspondence/communications. | **Retain** for 7 years then **Destroy** |

Note that any federal regulations may override the schedules in Table 1.  The University Records Management Office provides information and support for record retention requirements. {customize}

**System Log Retention and Destruction Schedules**

The log retention and destruction schedules will be as follows:

|  |  |  |
| --- | --- | --- |
| Record Type | Full Description | Retention and Disposition Action |
| {specify} | {specify} | {specify} |

**Describe method to retain and dispose of records:**

{specify}

Any logs with confidential data should be disposed of using the guidelines in NIST publication [SP 800-88 Rev. 1, Guidelines for Media Sanitization](https://csrc.nist.gov/pubs/sp/800/88/r1/final).

## Logging System Configuration

Logs must be protected against tampering and unauthorized access.  In addition, they must have protection from common system failures.  To ensure logs are protected, the logs are configured to:ds`

* Synchronize with a University approved accurate time source.
* Have adequate storage space and alert on any disk space shortages.
* Log authorized and unauthorized access attempts.
* Require a privileged account (e.g., account with equivalent root, Power User, or Administrator privileges) to make changes to log settings.
* Record all privileged accounts.
* Record initialization and shutdown of logging.
* Protect the logging facilities and log information against tampering and unauthorized access.
* Record the creation, deletion, and modification of system objects.

**Describe logging system protections and indicate any deviations from the requirements:**

{specify}

Forwarding Logs to the University Security Information and Event Monitoring Solution (SIEM)

The University SIEM allows logs to be correlated between disparate sources. The following systems must be sent to the SIEM, but others may be sent upon approval of the University’s Information Security Office.

## Log Correlation

The University has a Security Information and Event Management System (SIEM) for correlating important logs and monitoring for anomalies.  The ISO manages the system and assists customers with setup. At a minimum, logs from the following system should be sent to the SIEM:

* Azure Active Directory
* Domain Controller logs
* RADIUS logs
* CAS logs
* Firewall & IDS/IPS logs
* DNS request logs
* DHCP logs (lease request, grant, and removal activities)
* University web server (https://wwu.edu) logs
* Microsoft 365 Defender logs
* Security logs from devices and endpoints in PCI-DSS scope
* Switch and router change logs
* Enterprise VPN logs

**Indicate what logs will be forwarded to the University SIEM:**

{specify}

## Monitoring

A log monitoring plan should be developed to ensure logs are being inspected for security and if desired, operational problems.

**Describe log monitoring plan:**

{Remove below if not relevant}

# SaaS Vendors

Our Software as a Service vendors are required to collect, analyze, and monitor application audit logs and any other critical logs necessary to secure their environment.  Their practices should be equivalent to University on-premises systems. Vendors’ logging practices should be reviewed during the application security design review. In addition, system stewards and system custodians should understand if they need direct access to logs, and if the vendor provides a mechanism to access those logs.

**Describe vendor logging processes and any notable deviations from University expectations.**

{specify}

**Describe what direct access the University may need to SaaS logs (if any).**

{specify}

# Change Log

|  |  |  |
| --- | --- | --- |
| Date | Author Name | Change Description |
| xx | xx | Original procedure |