Information Technology Services

WSU Information System Audit and Accountability Standard

Author(s): Steven Conover

Date: 06/12/2020

WASHINGTON STATE UNIVERSITY

Revision History

Version No.	Date	Description	Author
1.0	06/12/2020	Initial Release	Steve Conover

Contents

Standards References

Washington State OCIO 141.10.
6.1.4, 7.1 (1), 10.2 (1, 2, 3)

NIST 800-53
AU-2, AU-3, AU-5, AU-6, AU-8, AU-9

Information System Audit and Accountability Standard

System Security Event Logging Standard

Purpose:

The primary purpose of this standard is to comply with Federal and State laws, WSU policies, and industry best practices by identifying those security-relevant auditable events which, when collected and analyzed, can identify inappropriate, unusual, or suspicious activities.

The secondary purpose of this standard is to identify what type of security-relevant event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individual(s) or subject(s) associated with the event.

Scope:

This policy applies to all Institutional business units, workforce members, and institutional information systems that collect, store, process, share, or transmit Institutional Data.

Standard:

A security event is a change in the everyday operations of a network or information technology service that may have significance to the security of the system or data. Security events logs are used to help identify significant occurrences for system hardware or software. The log files are also known as audit records, audit trails, or event-logs.

Logs can be used to serve many functions, such as optimizing system and network performance, recording the actions of users, and providing data useful for investigating malicious activity. Log monitoring systems oversee network activity, inspect system events, and store user actions (e.g., renaming a file, opening an application) that occur inside the operating system.

- The following table details which security relevant events must be:
  - Capable of being logged (upon request),
  - Regularly logged (as part of normal information system operating procedures) and,
  - Audited
- Logs shall be monitored continuously and audit records are to be reviewed on a weekly basis and, during periods of heightened security, logs shall be reviewed on a daily basis.

Security Relevant Events

	Capable of Being Logged	Regularly Logged	Audited
Account Creation	X	X	X
Account Modification	X	X	
Account Renaming	X	X	
Account Disabling	X	X	
Account Deleting	X	X	X
Account Enabling	X	X	X
Successful Account Logon	X	X	
Failed Account Logon	X	X	

Account Lockout	X	X	X
Account Logoff	X	X	
Password Set	X	X	
Password Changing	X	X	X
Creation of Communication Sessions	X	X	X
Failed Execution of Privileged Functions	X	X	X
Execution of Privileged Functions	X	X	X
Connection Activities of Remote Users	X	X	
Access Restriction for Configuration Changes	X	X	X
Successful Configuration Changes	X	X	X
Modifying Audit Records	X	X	X
Deleting Audit Records	X	X	X
Device Identification and Authentication (Dynamic Lease Information)	X	X	
Nonlocal Maintenance & Diagnostic Session	X	X	X
Access to Physical Media Storage	X	X	
Identity of Internal Users Associated With Denied Communications	X	X	X

Software, Firmware, and Information Integrity Violations	X	X	X
Unauthorized Modification of Critical Security Files	X	X	X
Manual Overrides	X	X	X
Modifications to System Volume Files	X	X	X
Object Access	X		

NOTE:

In the event that an information system capable of automated logging of events incurs a logging failure, a record of the event shall be recorded on the central monitoring system which will send an email notification of the logging failure to the system administrator on record for the system being monitored.

Content of Audit Events

WSU requires that, to the extent technically feasible, the audit records generated by the information system must contain enough detail to determine what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Audit Records are to include, to the extent technically feasible:

- Time Stamp – The information system should be configured to use the WSU NTP time server, firenze.it.wsu.edu, and retrieve time information on a regular basis for servers and network devices so that timestamps in logs are consistent.
- WSU's NTP time server is configured to use UTC
- Source and Destination Addresses
- User/Process Identifiers
- Event Descriptions
- Success / Fail Indications
- Filenames Involved
- Access Control or Flow Control Rules Invoked
- Full Text Recording of Privileged Commands

Administrative:

The Office of the Chief Information Officer is responsible for the administration of, and the enforcement of compliance with this standard.

Definitions:

For further clarification on the terminology and definition of terms used within this document, please refer to this organization's published glossary of terms associated with this document.

Exceptions:

Exceptions to this policy shall be managed and maintained by the Office of the CIO, following the processes outlined by WSU BPPM: Configuration Management Policy and ITS Exceptions Process.

Review Cycle:

This standard is to be reviewed every three years or on an as-needed basis due to changes to technology environments, business operations, or regulatory environments.

Appendix A:

Acronyms

Acronym	Definition
CISO / CIO	Chief Information Security Officer / Chief Information Officer
ITS	Information Technology Services
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
UTC	Universal Time Coordinated
WSU	Washington State University

Terms

Term	Definition
Auditable Events	Those information system security-relevant events which, when collected, analyzed, and correlated, can identify inappropriate, unusual, or suspicious activities and support after-the-fact investigations of security incidents.
Privileged Functions / Commands	Functions and commands that can only be executed by a person or process that has access to system control, monitoring, or administration functions (e.g., system administrator, information system security officer, maintainer, system programmer).