Audit and Accountability

OVERVIEW

Auditing and logging are necessary for detecting significant auditable events and those that are relevant to the security of information systems, institutional data, and the environment in which they operate.

See *BPPM* 87.01 for definitions related to this section. See also the Audit and Accountability Standard on the IT website.

Purpose

Auditing and logging controls are required for compliance with state, federal, and industry information security and privacy policies, regulations, and standards.

Scope

This policy (*BPPM* 87.50) applies to all institutional business units, workforce members, and institutional information systems that collect, store, process, share, or transmit institutional data.

POLICY

Information owners are accountable for developing appropriate procedures for the implementation of this policy.

IMPORTANT: Information owners are to develop procedures to implement this policy (*BPPM* 87.50) in a reasonable amount of time, not to exceed 12 months after this policy goes into effect.

Event Identification

Information system owners must identity the events each information system is capable of logging and auditing, related to the information systems for which they are responsible.

Based on the information system environment and the security controls to be implemented, information system owners must determine:

- An appropriate list of events that are to be logged and audited within the information system; and
- The frequency the events are to be audited.

Audit Logs

Information systems must generate audit records for the events that have been determined to be audited, that contain information that is relevant to the recorded event.

Retention Requirement

Information system owners must transfer and/or store audit logs in a different system(s) from those generating the logs.

Audit and Accountability

Coordinating Functions

Information system owners are to coordinate their logging and auditing functions with central Information Technology Services (ITS), other University business units, and third parties who provide and/or require audit information, to support auditing and compliance needs.

NOTE: The central information technology departments are WSU ITS in Pullman, and ITS in Spokane, Tri-Cities, Vancouver, and Everett, collectively referred to as central ITS.

Audit Storage Capacity

Information systems must allocate the required audit record storage capacity in accordance with the appropriate institutional, state, federal, and industry policies, standards, laws, and regulations for retention.

Audit Processing Failure

In the event of an audit processing failure, a notification should be sent to the information system owner and other appropriate business unit personnel according to their roles. The action to take in case of an audit failure is to be identified based on:

- Risk associated with losing audit records;
- Severity of the system processing failure;
- Classification of the system and data;
- Regulatory requirements; and/or
- Other appropriate factors.

Audit Review

Business units must review and analyze information system audit records on a regular basis for unintended disclosure, unusual and/or malicious activity. Audit reviews are to be reported to the information system owner and other appropriate business unit personnel according to their roles.

Audit Records

Information system owners must provide the capability to process, sort, and search audit records, as well as generate reports in support of investigative, regulatory, and/or legal requirements.

Logging systems must generate audit records with time stamps that are synchronized with an approved accurate time source.

Protection

Information systems must be configured to protect audit information and audit logging tools from unauthorized access, modification, and deletion.

ENFORCEMENT

The Office of the Chief Information Officer (CIO) is responsible and has the authority for enforcing compliance with this policy.

Audit and Accountability

Violations

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable University or state policies and handbooks (e.g., the WSU *Faculty Manual*, the *Administrative Professional Handbook*, *WAC* 357-40 (civil service employees), applicable collective bargaining agreements, or the WSU Standards of Conduct for Students, *WAC* 504-26).

Exceptions

Exceptions to this policy are managed and maintained by the Office of the CIO, under the guidance of the University Chief Information Security Officer (CSIO).

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exception. Approvals for policy exceptions are effective for a specified period of time and must be reviewed by the Office of the CIO on a periodic basis.

MAINTENANCE

The Office of the CIO is to review this policy every three years or on an as-needed basis due to changes to technology environments, business operations, standards, or regulatory requirements.