State of Wisconsin
Department of Administration
Division of Enterprise Technology
SECURITY

Effective Date: 1/1/2017

Audit and Accountability Standard

Purpose

The Audit and Accountability standard provides documentation of the requirements of the Audit and Accountability Policy, the Configuration Management Policy, the Maintenance Policy, and the System and Information and Integrity Policy.

Standard

Audit and log functions must be enabled on DET/State information systems and system environments to capture events that can be used to meet the requirements of security best practices and compliance needs outlined in the IT Security Policy Handbook and associated standards and procedures. The functions must include:

Log Generation

- Mainframes, servers, databases, and networking equipment must perform security log generation for all of its components (e.g., OS, service, application) (AU-2).
- All security events (Appendix A) must be logged and must be set to capture significant levels of detail to indicate activity (AU-3).
- The information system must maintain receiver/releaser credentials to ensure the "Chain of Custody" is not broken (AU-3).
- Logs and security events must be accessible and capable of being used for audit record generation (AU-12).
- The mobile device management servers must log security events for all mobile devices and the mobile device server (AU-2).

Log Storage and Disposal

- Systems that collect logs, whether local or consolidated, must maintain sufficient storage space to meet the minimum requirements for both readily available and retained logs. Storage planning must account for log bursts or increases in storage requirements that could reasonably be expected to result from system issues, including security (AU-4). When non-revolving log storage reaches 90% capacity, a warning must be issued.
- Log integrity for consolidated log infrastructure needs to be preserved, such as storing logs on write-once media or generating tracking digests for each log file.

Log Administration

- All hosts and networking equipment must issue alerts on security log processing failures, such as software/hardware errors, failures in the log capturing mechanisms, and log storage

capacity being reached or exceeded. All alerts must be as close to real time as possible (AU-5).

- Procedures must exist for managing unusual events. Response must be commensurate with system criticality, data sensitivity and regulatory requirements (AU-6).

Log Consolidation

Security-related information from all systems, with the exception of individual workstations, must be transferred to a consolidated log infrastructure. Systems running workstation operating systems which are used for shared services, such as shared file storage or web services must also satisfy these requirements.

All workstations must have the ability to transfer logs to a consolidated log infrastructure, if needed.

Log data must be transferred real-time from individual hosts to a consolidated log infrastructure. Where real-time transfer is not possible, data must be transferred from the individual hosts to a consolidated log infrastructure as quickly as the technology allows.

State agencies must establish processes for the establishment, operation and, as appropriate, integration of log management systems to ensure the protection of all original event log information (AU-7).

Log Access and Use

Log data must be initially analyzed as close to real time as possible (AU-6).

The information system shall be synchronized to the Department of Commerce (DOC) National Institute of Standards and Technology (NIST) Boulder Labs time source to ensure the integrity and correlation of the logs (AU-8).

Access to log management systems must be recorded and must be limited to individuals with a specific need for access to the records. Access to log data must be limited to the specific sets of data appropriate for the business need (AU-9).

All system and application logs shall be maintained in a form that cannot readily be viewed or altered by unauthorized persons. A process must be put in place to provide for log preservation requests, such as a legal requirement to prevent the alteration and destruction of particular log records (e.g., how the impacted logs must be marked, stored, and protected) (AU-10).

Because of the nature of the data contained in security logs (e.g., passwords, e-mail content), they are considered Personal, Private or Sensitive Information (PPSI) and must be protected.

Within the consolidated log infrastructure, logs must be maintained and readily available for a minimum of 90 days. DET shall retain audit records for one (1) year or as required by applicable

state and federal laws to provide support for after-the-fact investigations of security incidents and to meet regulatory audit record retention requirements. Based on Agency requirements, including audit or legal needs, logs may need to be retained for a longer period of time. DET shall retain audit records for Federal Tax Information (FTI) systems for seven years and DET shall retain audit records for CMS CARES systems for ten years (AU-11).

Log data must be securely disposed of (at both the system and the infrastructure level) in compliance with the Media Protection Standard.

The agency must employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries (AU-16).

Definitions

- Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies.
- DET/State information - Any information that is created, accessed, used, stored, or transmitted by an Agency and/or DET.
- DET/State information systems and system environments - All equipment or services used to input, store, process, transmit, and output information, including, but not limited to: network devices, servers, databases, printers, Internet, email, physical, virtual, cloud, and applications accessible to and/or managed by DET.

Compliance References

IRS Pub 1075
CIJIS Security Policy
CMS MARS-E
HIPAA Security Rule
NIST SP 800-53

Exception Process

Exceptions to this and all DET Security policies or procedures must follow the DET Exception Procedure.

Document History/Owner

This standard was developed as required by the Department of Administration, DET Information Technology Security Policy Handbook, under the authority of Wisconsin State Statute 16.971.

This standard is effective upon approval and publication until retired. Revisions and updates continue the effective date by documenting required changes over time.

Effective Date: 1/1/2017

Ownership for this standard is assigned to DOA, DET Bureau of Security. As such, the DOA, DET Bureau of Security is responsible for the maintenance, update(s), and review of this document annually before the anniversary of the effective date.

Version #	Approval, Revision, or Review Date	Description	Approver/Author, Title
.1	4/20/2016	Original Draft	Jeff Thompson Compliance Officer
.2	6/21/2016	Revisions and formatting	Tanya Choice Cybersecurity Compliance Consultant
.3	7/11/2016	Revisions and formatting	Tanya Choice Cybersecurity Compliance Consultant
1.0	10/26/16	Revision and final approval	Bill Nash Chief Information Security Officer

Authorized and Approved by:

Bill Nash — Bill Nash — 10/26/16

Print/Type — Signature — Date

Chief Information Security Officer

Division of Enterprise Technology-Bureau of Security

Effective Date: 1/1/2017

Appendix A - Security events that must be logged for all systems include but are not limited to (AU-2):

1. The audit trail shall capture all successful login and logoff attempts.
2. The audit trail shall capture all unsuccessful login and authorization attempts.
3. The audit trail shall capture all identification and authentication attempts.
4. The audit trail shall capture all actions, connections and requests performed by privileged users (a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator(s) and network administrator(s) who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the powers and access rights of existing users).
5. The audit trail shall capture all actions, connections and requests performed by privileged functions.
6. The audit trail shall capture all changes to logical access control authorities (e.g., rights, permissions).
7. The audit trail shall capture all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
8. The audit trail shall capture the creation, modification and deletion of objects including files, directories and user accounts.
9. The audit trail shall capture the creation, modification and deletion of user accounts and group accounts.
10. The audit trail shall capture the creation, modification and deletion of user account and group account privileges.
11. The audit trail shall capture: i) the date of the system event; ii) the time of the system event; iii) the type of system event initiated; and iv) the user account, system account, service or process responsible for initiating the system event.
12. The audit trail shall capture system start-up and shutdown functions.

13. The audit trail shall capture modifications to administrator account(s) and administrator group account(s) including: i) escalation of user account privileges commensurate with administrator-equivalent account(s); and ii) adding or deleting users from the administrator group account(s).

14. The audit trail shall capture the enabling or disabling of audit report generation services.

15. The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

16. The audit trail shall be protected from unauthorized access, use, deletion, or modification.

17. The audit trail shall be restricted to personnel routinely responsible for performing security audit functions.