STATE OF WISCONSIN
DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor
Kathy Blumenfeld, Secretary
Trina Zanow, Division Administrator
Effective Date: 08/01/2024

120 – 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

Based on NIST SP 800-53 Rev. 5, DET's Standards address a diverse set of security and privacy requirements. As a currently established baseline for implementation, DOA utilizes all low level, and selected moderate level controls in support of its security posture initiatives. Agencies shall categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately as defined by Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. Agencies shall update DET on the status of their baseline control implementation through the reporting and monitoring process.

Executive Branch Agencies shall develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. **Note:** Some agencies have specific regulatory requirements to follow that go above and beyond the requirements for other agencies. Implementation of the standard controls within this document can be (1) a common (inheritable) control, (2) a system-specific control, or (3) a hybrid control. The control implementation defines the scope of applicability for the control, the shared nature or inheritability of the control, and the responsibility for control development, implementation, assessment, and authorization.

This standard is divided into two sections of controls. **Section One** contains the minimum baseline controls that Executive Branch agencies shall implement. **Section Two** contains some of the common, regulatory controls agencies may be required to implement in addition to the baseline controls. Section Two is not all-inclusive. Each agency is responsible for identifying what other controls their agency may be required to implement beyond the scope of this standard.

SECTION ONE: BASELINE CONTROLS

Policy and Procedures (AU-1):

- Develop, document, and disseminate to appropriate agency personnel or roles:
    - An audit and accountability policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among agency entities, and compliance.
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
    - Procedures to facilitate the implementation of the audit and accountability policy

and the associated audit and accountability controls.

- Designate appropriate agency personnel to manage the development, documentation, and dissemination of the audit and accountability policy and procedures.
- Review and update the current audit and accountability:
  - Policy on an agency-defined frequency.
  - Procedures on an agency-defined frequency.

Event Logging (AU-2):

- Identify the types of events that the system is capable of logging in support of the audit function.
- Coordinate the event logging function with other agency/organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged.
- Specify the event types for logging within the system. (Note: Appendix A includes security events that are recommended to be logged for all systems. The security events in Appendix A are not all-inclusive. There may be additional events the agency needs to consider, specific to its own operations, which are not included in Appendix A. Each agency shall identify what security events beyond those listed in Appendix A are necessary and appropriate in its environment.).
- Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents.
- Review and update the event types selected for logging on an agency-defined frequency.

Content of Audit Records (AU-3):

- Ensure that audit records contain information that establishes the following:
  - What type of event occurred.
  - When the event occurred.
  - Where the event occurred.
  - Source of the event.
  - Outcome of the event.
  - Identity of any individuals, subjects, or objects/entities associated with the event.

Content of Audit Records | Additional Audit Information (AU-3(1)):

- Generate audit records containing any additional information that the agency deems as necessary and appropriate (i.e., access control or flow control rules invoked and individual identities of group account users).

Content of Audit Records | Limit Personally Identifiable Information Elements (AU-3(3)):

- Limit personally identifiable information contained in audit records to elements identified in the privacy risk assessment.

Audit Log Storage Capacity (AU-4):

- Allocate audit log storage capacity to accommodate audit log retention requirements. Audit log retention requirements are defined in AU-11.

Response to Audit Logging Process Failures (AU-5):

- Alert appropriate, personnel (or roles) in as close to real-time as possible in the event of an audit

logging process failure.
- Take the appropriate actions to address the alert and failure.

Audit Record Review, Analysis, and Reporting (AU-6):

- Review and analyze system audit records as close to real-time as possible for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity.
- Report findings to appropriate agency personnel or roles.
- Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Audit Record Review, Analysis, and Reporting | Automated Process Integration (AU-6(1)):

- Integrate audit record review, analysis, and reporting processes using automated mechanisms.

Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories (AU-6(3)):

- Analyze and correlate audit records across different repositories to gain situational awareness across all three levels of risk management (i.e., organizational level, mission/business process level, and information system level).

Audit Record Reduction and Report Generation (AU-7):

- Provide and implement an audit record reduction and report generation capability that:
  - Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents.
  - Does not alter the original content or time ordering of audit records.

Audit Record Reduction and Report Generation | Automatic Processing (AU-7(1)):

- Provide and implement the capability to process, sort, and search audit records for events of interest based on agency-defined fields within the audit records.

Time Stamps (AU-8):

- Use internal system clocks to generate time stamps for audit records.
- Record time stamps for audit records that are synchronized to the Department of Commerce (DOC) National Institute of Standards and Technology (NIST) Boulder Labs time source, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Protection of Audit Information (AU-9):

- Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
- Alert appropriate agency personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

Protection of Audit Information | Access by Subset of Privileged Users (AU-9(4)):

- Authorize access to management of audit logging functionality to only those individuals/roles with a specific need or business justification for access to the records.

Audit Record Retention (AU-11):

- Retain audit records for a time period consistent with records retention policies 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. Logs are to be maintained and readily available for a minimum of 90 days. Audit records are to be retained for one (1) year or longer, depending on regulatory requirements.

Audit Record Generation (AU-12):

- Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2.
- Allow limited personnel/roles to select the event types that are to be logged by specific components of the system.
- Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

SECTION TWO: REGULATORY CONTROLS

Executive Branch agencies shall implement the baseline controls listed in the previous section of this standard. Executive Branch agencies throughout the State of Wisconsin may also be subject to additional Federal, State, and/or Inter-agency regulatory requirements. It is each agency's responsibility to research and implement additional controls needed to meet regulatory compliance requirements and expectations outside of the State of Wisconsin baseline of controls.

Response to Audit Logging Process Failures | Storage Capacity Warning (AU-5(1)):

- Provide a warning to appropriate agency personnel or roles within an agency-defined time period when allocated audit log storage volume reaches an agency-defined percentage of repository maximum audit log storage capacity.

Protection of Audit Information | Store on Separate Physical Systems or Components (AU-9(2)):

- Store audit records for an agency-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

Definitions

Executive Branch Agency - State of Wisconsin legislatively defined Departments and all customers of DET services, equipment, and/or technologies. Agency or State Agency may be used interchangeably with Executive Branch Agency.

State information - Any information that is created, accessed, used, stored, or transmitted by an Executive Branch Agency.

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 the agency.

Exception Process

Exceptions to any Executive Branch Agency's Security Policies or Standards shall follow the Executive Branch Risk Exception Procedure.

Document History/Owner

This standard was developed as required by the State of Wisconsin Information Technology Security Policy Handbook, under the authority of Wis. Stat. § 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.

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 #	Revision or Review Date	Description of Change(s)	Reviewer/Author	Date Approved
2.0	11/03/20	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC/ITDC Author: DOA/DET/BOS	11/11/20
3.0	06/24/22	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: ITESC Author: DOA/DET	06/24/22
4.0	07/14/23	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	07/31/23
5.0	7/2/24	Reviewed with Agency Security Officers and IT Directors and changes were incorporated	Reviewer: WI ISAC and Enterprise IT Author: DOA/DET/BOS	7/30/24
NOTE: Keep only the origination and the last 10 years of update information. Only notate prior three revisions. Include only interim/final revision statuses.				

Authorized and approved by:

Troy Stairwalt, State of Wisconsin Chief Information Security Officer

	DocuSigned by: Troy Stairwalt DFEB606FC2524A8...	7/31/2024 | 4:05 PM CDT
Print/Type Title	Signature	Date

Appendix A

Security events that are **recommended** to 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).

Appendix A (Continued)

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

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

15. The audit trail shall capture configuration changes made to the system (e.g., operating system, application, and database) that have relevance to information security.

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.