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

This standard uses the NIST SP 800-53 Rev. 5 framework as the guideline to establish control objectives to address a diverse set of security and privacy requirements. Not all controls within NIST SP 800-53 Rev. 5 may be selected for the Statewide baseline policies and standards. Agencies must categorize their data and identify the potential impact (high, moderate, or low), and select controls appropriately. This standard uses Table 3-1 in NIST SP 800-53B for the allocated impact levels (high, moderate, low) of controls and control enhancements. At a minimum, all low controls are selected, and certain moderate controls are selected. Agencies are to reflect their controls through the annual reporting process to DOA-DET.

Executive Branch Agencies are to develop policies, procedures, or processes for their own State information systems and system environments to protect State information, if applicable. 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. Agencies should consider the following for inclusion in their policies, procedures, or processes:

Event Logging (AU-2):

- Identifying the types of events that the system is capable of logging in support of the audit function;
- Coordinating 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;
- Specifying 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 will need to consider, specific to its own operations, which are not included in Appendix A. Each agency will need to identify what security events beyond those listed in Appendix A are necessary and appropriate in its environment.);
- Providing a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
- Annually reviewing and updating the event types selected for logging.

Content of Audit Records (AU-3):

- Ensuring 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; and
- Identity of any individuals, subjects, or objects/entities associated with the event.

Additional Audit Information (AU-3(1)):

- Generating 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).

Audit Log Storage Capacity (AU-4):

- Allocating 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):

- Alerting appropriate, Agency-defined personnel (or roles) in as close to real-time as possible in the event of an audit logging process failure; and
- Taking the appropriate Agency-defined actions to address the alert and failure.

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

- Reviewing and analyzing 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;
- Reporting findings to Agency-defined personnel (or roles); and
- Adjusting 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.

Automated Process Integration (AU-6(1)):

- Integrating audit record review, analysis, and reporting processes using Agency-defined automated mechanisms.

Correlate Audit Record Repositories (AU-6(3)):

- Analyzing and correlating 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):

- Providing and implementing 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; and
  - Does not alter the original content or time ordering of audit records.

Automatic Processing (AU-7(1)):

- Providing and implementing 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):

- Using internal system clocks to generate time stamps for audit records; and
- Recording 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):

- Protecting audit information and audit logging tools from unauthorized access, modification, and deletion; and
- Alerting Agency-defined personnel (or roles) upon detection of unauthorized access, modification, or deletion of audit information.

Access by Subset of Privileged Users (AU-9(4)):

- Authorizing 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):

- Retaining 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):

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

Definitions

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

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 Agencies Security Policies, Procedures or Standards follow the Executive Branch Agencies 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 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.

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
1.0	10/15/18	Submitted to and approved by the IT Executive Steering Committee	Reviewer: ITESC Author: DOA/DET	10/15/18
1.0	10/29/19	Reviewed with Agency Security Officers and feedback collected. Planning for making revisions.	Bureau of Security	10/29/19
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
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:

Alan Greenberg, CISO

DocuSigned by:
Alan Greenberg
7062227F849B429...

7/8/2022 | 1:55 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 groupaccount(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.