Ohio | Opportunities for Ohioans with Disabilities

Title:	**Audit and Accountability Policy**
Policy #:	**60-ITG-08**
Legal Reference:	ORC §3304.15, §3304.16, §149.43, §1347.15; NIST 800-53; DAS IT-13, DAS
Effective Date:	February 13, 2023
Approved:	Kevin L. Miller, Director
Origin:	Division of Information Technology
Supersedes:	N/A
History:	N/A
Review/ Implementation	Begin Review – 09/09/24 Implement Revisions By – 03/10/25

I. AUTHORITY

This policy, and if necessary subsequent procedures, are issued in compliance with Ohio Revised Code (ORC) §3304.15 and §3304.16 which establishes the power and authority of the Opportunities for Ohioans with Disabilities (OOD) and its Executive Director to develop all necessary rules, policy, and procedure in furtherance of its statutory duties.

II. PURPOSE

The purpose of this policy is to define information system audit and accountability requirements that will assist in assessing the adequacy of system controls, ensuring compliance with established policies and procedures, and uniquely tracing the actions of system users in accordance with appropriate federal (e.g., Code of Federal Regulations [CFR]) and state law (i.e., Ohio Revised Code [ORC], Ohio Administrative Code [OAC]), Governor directives and executive orders, other governing agency (e.g., DAS, OBM) policy or guidance, and/or Director expectations.

III. APPLICABILITY

This policy applies to all OOD Division of Information Technology (IT) employees and contractors and if applicable, any other OOD system/service owner.

IV. DEFINITIONS

Refer to “Information Technology Definitions” 60-ITG-99.A.

V. POLICY

A. General

1. OOD-managed information systems shall be configured to produce, store, and retain audit records for specific systems, applications, networks, and user or system process activities.

2. Procedures are provided in Section V. for the implementation and management of audit and accountability controls.

    a. Procedures shall be reviewed annually and updated as necessary.

B. Audit Records and Auditable Events

1. OOD-managed information systems shall be configured to generate an audit record for pre-defined auditable events in order to adequately support after-the-fact security incident investigations.

    a. Auditable Events (AU-2) – The selection of auditable events which require continuous auditing or audit in response to specific situations detailed in DAS IT Standard DAS-ITS-2100-12-A, "Auditable Events" shall be based upon the results of the following assessments:

        i. a data classification assessment that is conducted in accordance with DAS's statewide policy "Data Classification" (IT-13);

        ii. a risk assessment conducted in accordance with OOD Policy "IT Risk Assessment" (60-ITG-06); and

        iii. a Privacy Impact Assessment conducted in accordance with ORC 1347.15.

    b. Auditable Events Review – Auditable events and review frequencies shall be documented. The documentation shall be evaluated on an annual basis, when a system undergoes a major data-related change, or when there is a change in a law or State security change and updated as necessary.

    c. Minimum Event Audit Requirements – At a minimum, event audit requirements shall include recording the date, timestamp, logon/logoff and failed access attempts for operating systems, databases, and applications.

    d. Systems Audit Requirements – Any system performing privileged functions, including changes in the status of auditable events, shall generate pre-defined audit records and shall be audited.

        i. Changes to an audit system shall only be made by authorized individuals and may include adjustments to capture more or less information to comply with investigation requirements, as well as modifications that would facilitate audit reduction, analysis, and reporting.

    e. Legal Audit Requirements for Systems – Systems shall have the capability to meet any legal requirements for logging and other accounting of user or system process activities in order for an audit to be performed.

i. Systems maintaining confidential personal information (CPI) within the scope of ORC 1347.15 shall have a mechanism for recording access by OOD employees (e.g., the recording mechanism may include application logging access or passing the employee's identifier to the database using a monitoring tool).

f. Content of Audit Records (AU-3) – Information systems shall have the capability to include specific information in audit records. Audit records shall contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the identity of any user or system process associated with the event and the event outcome.

i. Centralized Management of Audit Record Content – Audit records and audit logs generated shall be forwarded to a centralized audit management system.

g. Audit Storage Capacity (AU-4) – A sufficient amount of information system storage capacity shall be allocated for audit records and audit logs. Information systems shall be configured to reduce the likelihood of exceeding storage capacity for these items.

h. Response to Audit Processing Failures (AU-5) – Information systems shall provide the capability to generate information system alerts and send them to the appropriate personnel in the event of an audit failure or audit storage capacity being reached. In the event of an audit processing failure, the system shall shutdown or provide limited functionality, based on the outcome of the risk assessment conducted in accordance with OOD Policy "IT Risk Assessment" (60-ITG-06).

i. Audit Review, Analysis and Reporting (AU-6) – Information system audit records shall be regularly reviewed and analyzed to identify unauthorized, inappropriate, unusual, or suspicious activity. Such activity shall be investigated and reported to the appropriate officials, in accordance with OOD Policy "IT Security Incident Response" (60-ITG-05) and agency incident response procedures.

i. Frequency of Review and Analysis: As a minimum, audit records shall be reviewed and analyzed at least weekly by the system owner for inappropriate, unusual, or suspicious activity, and reporting shall be directed to the appropriate contacts.

a) Inappropriate, unusual, or suspicious activity includes, but is not limited to:

1) Excessive system usage (e.g., record searches, file retrievals, etc.)

2) System usage outside of the agency's business hours

3) System usage on weekends and holidays

4) Connections to agency systems from locations outside of Ohio

5) Excessive logins (or attempted logins)

b) Findings of inappropriate, unusual, or suspicious activity will be immediately provided to OOD's Chief Information Office (CIO) and Chief Information Security Officer (CISO). Other relevant parties may also be contacted, including:

1) system/service owner(s);
2) IT subject matter experts (SME);
3) OOD IT Management;
4) OIT and OISP; and
5) OOD Executive Leadership.

ii. Risk Escalation – If there is an increased risk to operating systems, databases or applications, review and analysis shall be performed more frequently.

iii. Integrate Alert Processes – Audit review, analysis and reporting processes shall be integrated to support investigations and subsequent responses to suspicious activities.

iv. Correlate Audit Repositories – Audit records shall be analyzed and correlated across different repositories to gain agency situational awareness.

v. Agency Coordination – During the configuration of security audit functions, OOD IT shall work with other divisions/bureaus within the agency to guide the selection of auditable events and ensure mutual support.

j. Audit Reduction and Report Generation (AU-7) – The centralized audit management system shall automatically process audit records for situations of interest based upon selectable criteria. The system shall also summarize the auditable events.

k. Timestamps (AU-8) – Audit records shall employ timestamps for use in audit record generation. Timestamps of audit records shall be generated using internal system clocks that are synchronized to a recognized network time protocol source.

l. Audit Information Protection (AU-9) – Audit information and audit tools shall be protected from unauthorized access, modification, and deletion.

i. Audit records and logs shall be protected from unauthorized modification, access, or deletion while online and during offline storage:

a) Only authorized system administrators, and the designated security personnel for the information system, are permitted access to audit records, logs and audit tools.

b) Audit records and logs containing sensitive data, such as CPI or PII, shall be encrypted.

ii. A monthly review of audit records, logs and access shall be performed to detect any instances of unauthorized access, modification, or deletion.

m. Nonrepudiation (AU-10) – Information systems' audit records and logs protect against an individual falsely denying having performed a particular action.

n. Audit Record Retention (AU-11) – Audit records and logs shall be retained to provide support for after-the-fact investigations of security incidents and to meet regulatory and record retention requirements.

o. Audit Generation (AU-12) – The information system provides audit record generation capability for the auditable events defined in Section B.1.a. Audit records shall be generated for the events defined in this section with the content defined in Section B.1.b. System/service owners shall select which events are to be audited.

V. PROCEDURES

A. General

1. These procedures will provide guidance for the implementation and management of audit controls defined in this policy and shall be acknowledged by all OOD IT employees and contractors tasked with supporting the audit functions of OOD used information systems.

   a. Auditable Events (AU-2) may include any action required by policies and procedures (e.g., OOD, OIT, DAS, OISP), applicable local, state, and federal laws; as well as industry directives, policies, regulations, and standards.

      i. Creation of Auditable Events – OOD IT shall ensure, or work with 3rd parties to ensure, auditable events are created in information systems used by OOD employees and contractors. This may include, but is not limited to:

         a) event timestamps (date and time);
         b) status and/or error codes;
         c) usernames/account names;
         d) device names;
         e) account creations;
         f) password changes; and
         g) successful and failed logons.

      ii. Auditable Events Review – OOD IT shall document auditable events and establish review frequencies in each system's Security Plan document. The documentation shall be evaluated on an annual basis and updated as necessary.

iii. Minimum Event Audit Requirements – OOD IT shall establish minimum event audit requirements to include recording the date, timestamp, logon/logoff and failed access attempts for operating systems, databases, and applications.

iv. Privileged Functions – OOD IT shall ensure that privileged functions, including changes in the status of auditable events, shall generate audit records and shall be audited.

v. Changes by Authorized Individuals – OOD IT shall put controls in place prevent unauthorized personnel from making changes to audit systems. Changes to audit systems will be documented in ServiceNow as a Change Request.

vi. Systems Capability and Auditable Events – OOD IT shall ensure that systems have the capability to meet any legal requirements for logging and other accounting of user activities.

b. Content of Audit Records (AU-3) – OOD IT shall engage data owners, and system service owners to ensure systems have the capability to include specific information in audit records. Audit records shall contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the identity of any user and system process associated with the event and the event outcome.

i. Centralized Management of Audit Record Content – OOD IT shall configure audit records and logs to be copied to a centralized audit management system (e.g., security information and event management [SIEM] system, Microsoft solutions).

c. Audit Storage Capacity (AU-4) – OOD IT shall ensure that a sufficient amount of storage is allocated for audit records and audit logs and shall configure information systems to reduce the likelihood of exceeding the storage capacity for these items.

d. Response to Audit Processing Failures (AU-5) – OOD IT shall ensure, or work with 3rd parties to ensure, information systems are created/deployed with the capability to generate information system alerts and notify appropriate personnel in the event of an audit failure or audit storage capacity being reached.

e. Audit Review, Analysis and Reporting (AU-6) – OOD IT shall regularly review information system audit records and audit logs and analyze them to identify unauthorized, inappropriate, unusual, or suspicious activity. Such activity shall be reported to OOD's Chief Information Officer (CIO) and Chief Information Security Officer (CISO), in accordance with OOD Policy "Incident Response" (60-ITG-05) and agency incident response procedures.

i. Frequency of Review and Analysis – At a minimum, audit records shall be reviewed and analyzed at least weekly by the system owner and OOT IT Security for inappropriate, unusual, and/or suspicious activity.

a) OOD systems containing sensitive data are considered high risk and should be audited more frequently.

b) Findings of inappropriate, unusual, or suspicious activity shall be immediately communicated, via email, to OOD's Chief Information Office (CIO) and Chief Information Security Officer (CISO), or designee(s).

c) OOD IT shall provide audit logs for OOD systems to facilitate internal investigations.

d) CIO and Chief Legal Counsel's approval is required prior to releasing audit findings to parties outside the agency.

f. Audit Information Protection (AU-9) – OOD IT shall configure audit processes in such a way as to be protected from unauthorized access and/or alteration. Any access to audit information/data shall be logged. Audit information (e.g., audit records, logs, reports) will be copied to another system such as a SIEM. Audit logs containing CPI will be encrypted.

B. Violation

An employee who violates this policy or its procedures may be subject to discipline up to and including removal.

FORMS AND ATTACHMENTS

- N/A

RESOURCES

- NIST 800-53
- DAS-ITS-2100-12-A – Auditable Events
- DAS Statewide Policy – IT-13 Data Classification
- OOD Policy 60-ITG-06 Risk Assessment
- OOD Policy 60-ITG-05 Incident Response

REVIEW

It is the responsibility of the Deputy Director, or designee, to review this policy, on or before, the date listed in the header and if applicable, make any necessary revisions. The Deputy Director, or designee, shall document the review as required in "Policy and Process" (10-ADM-01).