*ITC / ORG Name Here*

version 1.0

August 2021

***Audit and Accountability Policy***

## Document Review History

|  |  |  |
| --- | --- | --- |
| Date | Version | Reviewers |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Document Change History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Filename/Version | Author | Revision Description |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Document Review History i](#_Toc484683708)

[Document Change History i](#_Toc484683709)

[Introduction 1](#_Toc484683710)

[Background 1](#_Toc484683711)

[Purpose 1](#_Toc484683712)

[Scope and Applicability 1](#_Toc484683713)

[Audit and Accountability Policies 1](#_Toc484683714)

[Audit Events 1](#_Toc484683715)

[Content of Audit Records 2](#_Toc484683716)

[Audit Storage Capacity 2](#_Toc484683717)

[Response to Audit Processing Failures 2](#_Toc484683718)

[Audit Review, Analysis, and Reporting 2](#_Toc484683719)

[Audit Reduction and Report Generation 2](#_Toc484683720)

[Time Stamps 3](#_Toc484683721)

[Protection of Audit Information 3](#_Toc484683722)

[Audit Record Retention 3](#_Toc484683723)

[Audit Generation 3](#_Toc484683724)

[Procedures 4](#_Toc484683725)

[Resources 4](#_Toc484683726)

[Roles and Responsibilities 4](#_Toc484683727)

[Train Personnel 4](#_Toc484683728)

[Follow Up 4](#_Toc484683729)

[Compliance 4](#_Toc484683730)

[Documentation Compliance Review 5](#_Toc484683731)

[Security Officer Documentation Compliance Review 5](#_Toc484683732)

[Acronyms/Definitions 5](#_Toc484683733)

[References 6](#_Toc484683734)

[Forms (If applicable) 7](#_Toc484683735)

# Introduction

## Background

This policy is authorized and in use by {ORG Name}, hereafter referred to as (Org abbreviated Name) as defined in the definition page of this document, and it applies to personnel, as defined in the definition page of this document. The confidentiality, integrity, and availability of information stored within the information systems of {ORG ABBREVIATED NAME} must be protected in order to comply with federal and state law, governing policies, and to preserve our reputation as a caretaker of sensitive information. Audit and accountability controls are in place to ensure that {ORG ABBREVIATED NAME’s} information systems record the appropriate information to support the investigation of after-the-fact computer security incidents.

## Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information stored within the information systems managed, authorized, and in use by {ORG ABBREVIATED NAME} by defining the information system requirements for audit record generation, content, and retention.

## Scope and Applicability

This policy applies to information systems in use by {ORG ABBREVIATED NAME}.

Exceptions

Please see Appendix “A” for organizational specific exceptions.

# Audit and Accountability Policies

## Audit Storage Capacity (AU-4)

{ORG ABBREVIATED NAME} shall allocate audit record storage capacity in accordance with{{ORG ABBREVIATED NAME}-defined parameters and policies.

## Audit Review, Analysis, and Reporting (AU-6)

ORG ABBREVIATED NAME} IT Staff shall review and analyze information system audit records quarterly for indications of inappropriate or unusual activity and report findings to ORG ABBREVIATED NAME} Security Officer.

{ORG ABBREVIATED NAME} IT Staff shall employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

{ORG ABBREVIATED NAME Logging Management} shall analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

## Audit Reduction and Report Generation (AU-7)

The information system provides an audit reduction and report generation capability that:

* Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents
* Does not alter the original content or time ordering of audit records.

The information system provides the capability to process audit records for events of interest based on ORG ABBREVIATED NAME}-defined criteria.

## Audit Generation (AU-12)

The information system shall provide audit record generation capability for auditable events on mission critical information system components, allow ORG ABBREVIATED NAME} IT Staff to select which auditable events are to be audited by specific components of the information system, and generate audit records for the events.

## Monitoring for information Disclosure (AU-13)

The organization monitors [Assignment: organization-defined open source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information.

## Cross –Organization Auditing (AU-16)

The organization employs [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.

# Procedures

## Resources

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Business System Owner | Determines the information system is capable. |
| CISO | * Validate compliance on a {Time Period} basis.
* Authorize access to management of audit functionality.
 |
| HR | Provide policy during new hire process and informs personnel of changes. |
| Logging Management | * Coordinates security audit function with other organizational entities.
* Provides a rationale for auditable events that is adequate to support after-the-fact investigations.
* Reviews and updates list of audited events.
* Reviews and analyzes information system audit records.
* Employ automated mechanisms to integrate audit review, analysis, and reporting processes.
* Analyze and correlate audit records across different repositories.
 |
|  |  |
|  |  |

## Train Personnel

Personnel are informed by a ORG ABBREVIATED NAME} Human Resources representative of this policy during the new-hire process and are incrementally informed when the policy changes.

## Follow Up

The products of this policy must be reviewed at least annually, and when the {ORG ABBREVIATED NAME’s} review indicates that updates are required.

## Compliance

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Documentation Compliance Review

All roles identified above must maintain documented proof of compliance for portions of this policy that are applicable to their responsibilities.

## Security Officer Documentation Compliance Review

The ORG ABBREVIATED NAME} Executive Director will validate compliance with this policy on an annual basis.

# Acronyms/Definitions

|  |  |
| --- | --- |
| Acronym/Term | Definition |
| CISO | Chief Information Security Officer |
| HR | Human Resources |
| MC ORG ABBREVIATED NAME | Management Council of the Ohio Education Computer Network |
| ORG ABBREVIATED NAME | Ohio Education Computer Network |
| Personnel | Employees, contractors, consultants, temporary workers, and other workers. |
|  |  |
|  |  |
|  |  |
|  |  |

# References

# Forms (If applicable)