***Security Assessment and Authorization Policy***

*ITC/ORG Name Here*

version 1.0

August 2021

## Document Review History

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

## Document Change History

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

**Contents**

[Document Review History 2](#_Toc83735470)

[Document Change History 2](#_Toc83735471)

[Introduction 4](#_Toc83735472)

[Background 4](#_Toc83735473)

[Purpose 4](#_Toc83735474)

[Scope and Applicability 4](#_Toc83735475)

[Security Assessment and Authorization Policies 4](#_Toc83735476)

[(CA-2) Security Assessments 4](#_Toc83735477)

[(CA-3) System Interconnections 5](#_Toc83735478)

[(CA-7) Continuous Monitoring 5](#_Toc83735479)

[(CA-9) Internal System Connections 5](#_Toc83735480)

[Procedures 6](#_Toc83735481)

[Resources 6](#_Toc83735482)

[Roles and Responsibilities 6](#_Toc83735483)

[Train Personnel 6](#_Toc83735484)

[Follow Up 6](#_Toc83735485)

[Compliance 6](#_Toc83735486)

[Documentation Compliance Review 6](#_Toc83735487)

[Security Officer Documentation Compliance Review 6](#_Toc83735488)

[Acronyms/Definitions 8](#_Toc83735489)

[References 9](#_Toc83735490)

[Forms (If applicable) 10](#_Toc83735491)

# Introduction

## Background

This policy is authorized and in use by {{ORG Name}and 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. Security assessment and authorization controls are in place to ensure that {{ORG ABBREVIATED NAME}’s} information system is regularly reviewed for compliance with security requirements.

## 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 specific controls required to assess the information systems.

## Scope and Applicability

This policy applies to the information systems held by {{ORG ABBREVIATED NAME}} and personnel involved in the assessment thereof.

Exceptions

Please see Appendix “A” for organizational specific exceptions.

# Security Assessment and Authorization Policies

## (CA-2) Security Assessments

The {Organization Security Group shall develop a security assessment plan that describes the scope of the assessment including:

ORG ABBREVIATED NAME}} Security officer will set security controls and control enhancements during the assessment.

OECN Security Group will develop assessment procedures to determine security control effectiveness.

## (CA-3) System Interconnections

The Security Officer authorizes connections from the information system to other information systems through the use of the Interconnection Security Agreements.

{ {ORG Abbreviated Name} Technology staff maintains documents for each interconnection, interface characteristics, security requirements, and the nature of the information communicated.

{ {ORG Abbreviated Name} Technology Staff reviews and updates Interconnection Security Agreements on an {annual} basis.

{{ORG ABBREVIATED NAME} Security Officer and Executive Director defines and determines which personnel should have security access to connect to external information systems.

## (CA-7) Continuous Monitoring

The security officer and IT Director develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

* establishing {ORG Abbreviated Name} -defined metrics to be monitored by {ORG Abbreviated Name} technology Staff establishes the frequency for monitoring and the assessment for supporting such monitoring on an annual basis.
* {performs ongoing security control assessments in accordance with the {ORG Abbreviated Name} continuous monitoring strategy.
* Ongoing security status monitoring of {ORG Abbreviated Name} -defined metrics in accordance with the {ORG Abbreviated Name} continuous monitoring strategy
* Correlation and analysis of security-related information generated by assessments and monitoring
* Response actions to address results of the analysis of security-related
* reports the security status of {ORG Abbreviated Name} and the information system to the {ORG Abbreviated Name} -defined personnel at the {ORG Abbreviated Name} -defined frequency.

## (CA-9) Internal System Connections

The organization authorizes internal connections of {ORG Abbreviated Name} -defined information system components or classes of components to the information system; and documents for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

# Procedures

## Resources

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| {ORG ABBREVIATED NAME} security group | Validate compliance on an annual basis. |
| Security officer | Provide policy during new hire process and informs personnel of changes. |
| {ORG Abbreviated Name} Technology Staff |  |
| OECN Security Group |  |
|  |  |
|  |  |

## 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 Executive Director will validate compliance with this policy on an annual basis.

# Acronyms/Definitions

|  |  |
| --- | --- |
| Acronym/Term | Definition |
| MC {ORG ABBREVIATED NAME} | Management Council of the Ohio Education Computer Network |
| Personnel | Employees, contractors, consultants, temporary workers, and other workers. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# References

# Forms (If applicable)