

***Security Planning 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 i](#_30j0zll)

[Document Change History i](#_1fob9te)

[Introduction 1](#_3znysh7)

[Background 1](#_2et92p0)

[Purpose 1](#_tyjcwt)

[Scope and Applicability 1](#_3dy6vkm)

[Security Planning Policies 1](#_1t3h5sf)

[System Security Plan 1](#_4d34og8)

[Rules of Behavior (Acceptable Use) 2](#_2s8eyo1)

[Information Security Architecture 2](#_17dp8vu)

[Procedures 2](#_3rdcrjn)

[Resources 2](#_26in1rg)

[Roles and Responsibilities 2](#_lnxbz9)

[Train Personnel 3](#_35nkun2)

[Follow Up 3](#_1ksv4uv)

[Compliance 3](#_44sinio)

[Documentation Compliance Review 3](#_2jxsxqh)

[Security Officer Documentation Compliance Review 3](#_z337ya)

[Acronyms/Definitions 4](#_1y810tw)

[References 5](#_4i7ojhp)

[Forms (If applicable) 6](#_2xcytpi)

# 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. Security planning controls are in place to promote a common set of standards for the management of information systems and facilities across the enterprise.

## Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information systems and facilities in use by {{ORG ABBREVIATED NAME}} by defining the vision for the security architecture.

## Scope and Applicability

This policy applies to all personnel who interact with information systems or facilities managed by {{ORG ABBREVIATED NAME}.

Exceptions

Please see Appendix “A” for organizational specific exceptions.

# Security Planning Policies

## (PL-2) System Security Plan

{{ORG ABBREVIATED NAME}} shall develop a security plan for the mission critical information systems that is consistent with the {ORG Abbreviated Name} enterprise architecture, explicitly defines the authorization boundary for the system, and describes the operational context of the information system in terms of missions and business processes. The Security Plan shall provide the security categorization of the information system including supporting rationale, describe the operational environment for the information system and relationships with or connections to other information systems. It shall provide an overview of the security requirements for the system, and identify any relevant overlays, if applicable. The Security Plan will describe the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions. The Security Plan is reviewed and approved by the Security Officer prior to plan implementation.

ORG Abbreviated Name Security Officer shall distribute copies of the security plan and communicate subsequent changes to the plan to the Executive Director. The Security Officer will review the security plan for the information system annually and update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments. The Security Plan will be protected from unauthorized disclosure and modification.

##  (PL-8) Information Security Architecture

{{ORG ABBREVIATED NAME}} shall develop an information security architecture for the information system that:

* Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of {ORG Abbreviated Name} information
* Describes how the information security architecture is integrated into and supports the enterprise architecture
* Describes any information security assumptions about, and dependencies on, external services

The information security architecture shall be reviewed and updated annually to reflect updates in the enterprise architecture and ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

# Procedures

## Resources

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## 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}} 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 Directory will validate compliance with this policy on an annually 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)