***Information Security Program 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)

[Information Security Program Planning Policies 1](#_1t3h5sf)

[Information Security Program 1](#_4d34og8)

[Senior Information Security Officer 2](#_2s8eyo1)

[Information Security Resources 2](#_17dp8vu)

[Plan of Action and Milestones Process 3](#_3rdcrjn)

[Information System Inventory 3](#_26in1rg)

[Information Security Measures of Performance 3](#_lnxbz9)

[Enterprise Architecture 3](#_35nkun2)

[Critical Infrastructure Plan 4](#_1ksv4uv)

[Risk Management Strategy 4](#_44sinio)

[Security Authorization Process 4](#_2jxsxqh)

[Mission/Business Process Definition 5](#_z337ya)

[Insider Threat Program 5](#_3j2qqm3)

[Information Security Workforce 5](#_1y810tw)

[Testing, Training, and Monitoring 5](#_4i7ojhp)

[Contacts with Security Groups and Associations 6](#_2xcytpi)

[Threat Awareness Program 6](#_1ci93xb)

[Procedures 6](#_3whwml4)

[Resources 6](#_2bn6wsx)

[Roles and Responsibilities 6](#_qsh70q)

[Train Personnel 7](#_3as4poj)

[Follow Up 7](#_1pxezwc)

[Compliance 7](#_49x2ik5)

[Documentation Compliance Review 7](#_2p2csry)

[Security Officer Documentation Compliance Review 7](#_147n2zr)

[Acronyms/Definitions 8](#_23ckvvd)

[References 9](#_ihv636)

[Forms (If applicable) 10](#_32hioqz)

# Introduction

## Background

This policy is authorized and in use by {{ORG Name} name, hereafter referred to as {ORG Abbreviated Name} 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. The Information Security Program defines {ORG Abbreviated Name} organizational structure required to support the security infrastructure of {{ORG ABBREVIATED NAME}}

## Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information systems in use by {{ORG ABBREVIATED NAME}} by defining {ORG Abbreviated Name} organizational and resource requirements for the support of the information security architecture.

## Scope and Applicability

This policy applies to all personnel with information security administration responsibilities within {ORG ABBREVIATED NAME}.

Exceptions

Please see Appendix “A” for organizational specific exceptions.

# Information Security Program Planning Policies

## (PM-1) Information Security Program

{{ORG ABBREVIATED NAME}} shall develop and disseminate an {ORG Abbreviated Name} -wide information security program plan that:

* Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
* Includes the identification and assignment of roles, responsibilities, management commitment, coordination among {ORG Abbreviated Name} entities, and compliance.
* Reflects coordination among {ORG Abbreviated Name} entities responsible for the different aspects of information security (i.e., technical, physical, personnel, cyber-physical).
* Is approved by a senior official with responsibility and accountability for the risk being incurred to {ORG Abbreviated Name} operations including mission, functions, image, and reputation of {ORG Abbreviated Name} assets, individuals, and other {ORG Abbreviated Name} resources.

The information security program shall be reviewed at least annually and updated to address {ORG Abbreviated Name} changes and problems identified during plan implementation or security control assessments. The information security program plan shall be protected from unauthorized disclosure and modification.

## (PM-2) Senior Information Security Officer

{{ORG ABBREVIATED NAME}} shall appoint a Security Officer with the mission and resources to coordinate, develop, implement, and maintain an {ORG Abbreviated Name} -wide information security program.

## (PM-3) Information Security Resources

{{ORG ABBREVIATED NAME}} Security Officer shall:

* Ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.
* Employ a {business pla~~n~~ to record the resources required.

{

Executive Management} shall

* Ensure that information security resources are available for expenditure as planned.

## (PM-4) Plan of Action and Milestones Process

{{ORG ABBREVIATED NAME} Security Officer shall implement a process for ensuring that plans of action and milestones for the security program and associated {ORG Abbreviated Name} information systems:

* Are developed and maintained.
* Document the remedial information security actions to adequately respond to risk to {ORG Abbreviated Name} operations and assets, individuals, and other {ORG Abbreviated Name} resources.
* Are reported in accordance with OMB FISMA reporting requirements, if applicable
* {{ORG ABBREVIATED NAME}} Security Officer shall review plans of action and milestones for consistency with the {ORG Abbreviated Name} risk management strategy and {ORG Abbreviated Name} -wide priorities for risk response actions.

## (PM-5) Information System Inventory

{ORG Abbreviated Name} Technology Staff shall develop and maintain an inventory of its information systems.

## (PM-6) Information Security Measures of Performance

{ORG ABBREVIATED NAME} Security Officer shall develop, monitor, and report on the results of information security measures of performance.

## (PM-7) Enterprise Architecture

{{ORG ABBREVIATED NAME}} Security Officer shall develop an enterprise architecture with consideration for information security and the resulting risk to {ORG Abbreviated Name} operations, {ORG Abbreviated Name} assets, individuals, and other {ORG Abbreviated Name} resources.

## (PM-8) Critical Infrastructure Plan

{{ORG ABBREVIATED NAME}} Security Officer shall address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

## (PM-9) Risk Management Strategy

{{ORG ABBREVIATED NAME}} Security Officer shall develop a comprehensive strategy to manage risk to {ORG Abbreviated Name} operations and assets, individuals, other {ORG Abbreviated Name} resources, and the Nation associated with the operation and use of information systems and implement the risk management strategy consistently across. {ORG Abbreviated Name}. The risk management strategy shall be reviewed and updated at least annually or as required, to address {ORG Abbreviated Name} changes.

## (PM-10) Security Authorization Process

{{ORG ABBREVIATED NAME}} Security Officer shall manage (i.e., documents, tracks, and reports) the security state of {ORG Abbreviated Name} information systems and the environments in which those systems operate through security authorization processes. The Security Officer may designate individuals to fulfill specific roles and responsibilities within {ORG Abbreviated Name} risk management process. The security authorization processes shall be integrated into an {ORG Abbreviated Name} -wide risk management program.

## (PM-11) Mission/Business Process Definition

{{ORG ABBREVIATED NAME}} Executive Management shall define mission/business processes with consideration for information security and the resulting risk to {ORG Abbreviated Name} operations, assets, individuals, other {ORG Abbreviated Name} resources, and determine information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained.

## (PM-12) Insider Threat Program

{{ORG ABBREVIATED NAME}} Security Officer shall implement an insider threat program that includes a cross-discipline insider threat incident handling team.

## (PM-13) Information Security Workforce

{ORG ABBREVIATED NAME} Security Officer shall establish an information security workforce development and improvement program.

## (PM-14) Testing, Training, and Monitoring

{{ORG ABBREVIATED NAME}} Security Officer shall implement a process for ensuring that {ORG Abbreviated Name} plans for conducting security testing, training, and monitoring activities associated with {ORG Abbreviated Name} information systems:

* Are developed and maintained.
* Continue to be executed in a timely manner.

{ORG ABBREVIATED NAME} Security Officer shall review testing, training, and monitoring plans for consistency with the {ORG Abbreviated Name} risk management strategy and {ORG Abbreviated Name} -wide priorities for risk response actions.

## (PM-15) Contacts with Security Groups and Associations

{ORG ABBREVIATED NAME} Security Officer and Technology Staff shall establish and institutionalizes contact with selected groups and associations within the security community:

* To facilitate ongoing security education and training for {ORG Abbreviated Name} personnel.
* To maintain currency with recommended security practices, techniques, and technologies.
* To share current security-related information including threats, vulnerabilities, and incidents. (MS/ISAC, CERT, CIAC, Infragard, etc.)

## (PM-16) Threat Awareness Program

{{ORG ABBREVIATED NAME}} Security Officer shall implement a threat awareness program that includes a cross- {ORG Abbreviated Name} information-sharing capability.

# Procedures

## Resources

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
|  | Validate compliance on a {Time Period} basis. |
|  | Provide policy during new hire process and informs personnel of changes. |
|  |  |
|  |  |
|  |  |
|  |  |

## 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)