***Risk Assessment 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)

[Risk Assessment Policies 1](#_1t3h5sf)

[Security Categorization 1](#_4d34og8)

[Risk Assessment 1](#_2s8eyo1)

[Vulnerability Scanning 1](#_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](#_3j2qqm3)

[References 5](#_1y810tw)

[Forms (If applicable) 6](#_4i7ojhp)

# 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. Risk assessment controls are in place to ensure a consistent methodology is in place for the management and acceptance of risk to the business.

## 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 the methodology related to the management of risk within {ORG Abbreviated Name}

## Scope and Applicability

This policy applies to all personnel, business processes and information systems managed by {{ORG ABBREVIATED NAME}.

Exceptions

Any {{ORG ABBREVIATED NAME}} exceptions to this policy are documented in Appendix “A” of this document.

# Risk Assessment Policies

## (RA-2) Security Categorization

{{ORG ABBREVIATED NAME} shall categorize information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security categorization results (including supporting rationale) shall be documented in the security plan for the information system. The security categorization decision shall be reviewed and approved by the authorizing official or authorizing official designated representative.

## (RA-3) Risk Assessment

{{ORG ABBREVIATED Security Officer shall:

* Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
* Document risk assessment results in a risk assessment report.
* Review risk assessment results at least annually
* Disseminate risk assessment results to Executive Management.
* Update the risk assessment at least annually or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

## (RA-5) Vulnerability Scanning

{{ORG ABBREVIATED NAME} Security Officer or Designee shall scan for vulnerabilities in the information system and hosted applications quarterly and when new vulnerabilities potentially affecting the system/applications are identified and reported. The vulnerability scanning tools and techniques shall facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

* Enumerating platforms, software flaws, and improper configurations.
* Formatting checklists and test procedures.
* Measuring vulnerability impact.

{{ORG ABBREVIATED NAME} Security Officer shall analyze vulnerability scan reports and results from security control assessments and ensure that {{ORG Abbreviated Name} IT Technology staff remediate legitimate vulnerabilities in accordance with an {ORG Abbreviated Name} assessment of risk. The Security Officer shall share information obtained from the vulnerability scanning process and security control assessments with {{ORG Abbreviated Name} IT Technology Staff} to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

# 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} 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} NAME | Management Council of the Ohio Education Computer Network |
| Personnel | Employees, contractors, consultants, temporary workers, and other workers. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# References

# Forms (If applicable)