***Incident Response 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](#_Toc83813597)

[Document Change History 2](#_Toc83813598)

[Introduction 5](#_Toc83813599)

[Background 5](#_Toc83813600)

[Purpose 5](#_Toc83813601)

[Scope and Applicability 5](#_Toc83813602)

[Incident Response Policies 5](#_Toc83813603)

[(IR-2) Incident Response Training 5](#_Toc83813604)

[(IR-3) Incident Response Testing 5](#_Toc83813605)

[(IR-4) Incident Handling 6](#_Toc83813606)

[(IR-5) Incident Monitoring 6](#_Toc83813607)

[(IR-6) Incident Reporting 6](#_Toc83813608)

[(IR-7) Incident Response Assistance 6](#_Toc83813609)

[(IR-8) Incident Response Plan 6](#_Toc83813610)

[(IR-9) Information Spillage Response 7](#_Toc83813611)

[~~Procedures~~ 7](#_Toc83813612)

[Resources 7](#_Toc83813613)

[Roles and Responsibilities 7](#_Toc83813614)

[Train Personnel 8](#_Toc83813615)

[Follow Up 8](#_Toc83813616)

[Compliance 8](#_Toc83813617)

[Documentation Compliance Review 8](#_Toc83813618)

[Security Officer Documentation Compliance Review 8](#_Toc83813619)

[Acronyms/Definitions 9](#_Toc83813620)

[References 10](#_Toc83813621)

[Forms (If applicable) 11](#_Toc83813622)

# Introduction

## Background

This policy is authorized and in use by {ORG Name, hereafter referred to as {ORG ABBREVIATED NAME}}, 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. Incident Response controls are in place to ensure that {{ORG ABBREVIATED NAME}} has a developed plan to handle security impacting events when they are detected.

## 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 steps to be taken in the event of a security event, incident, or breach.

## Scope and Applicability

This policy applies to the information systems managed by {{ORG ABBREVIATED NAME}} and personnel who access the information systems owned and maintained by {{ORG ABBREVIATED NAME}}.

Exceptions

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

# Incident Response Policies

## (IR-2) Incident Response Training

{{ORG ABBREVIATED NAME}} shall provide incident response training to information system users consistent with assigned roles and responsibilities:

* Within one year of assuming an incident response role or responsibility
* When required by information system changes
* Annually thereafter

## (IR-3) Incident Response Testing

{{ORG ABBREVIATED NAME}} shall test the incident response capability for the information systems at least annually to determine the incident response effectiveness, and document the results.

Testing methods can include tabletop exercises, functional drills, simulation exercises, and/or active penetration tests.

## (IR-4) Incident Handling

{{ORG ABBREVIATED NAME}} shall implement an Incident Response Plan for security incidents that includes:

* Preparation
* Detection and analysis
* Containment
* Eradication
* Recovery

{{ORG ABBREVIATED NAME}} shall coordinate incident handling activities with contingency planning activities and incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.

##  (IR-5) Incident Monitoring

{{ORG ABBREVIATED NAME}} shall track and document information system security incidents.

## (IR-6) Incident Reporting

{{ORG ABBREVIATED NAME}} shall require personnel to report suspected security incidents to the

{{ORG ABBREVIATED NAME}} Security Officer within one business day of detection.

The {{ORG ABBREVIATED NAME} Incident Response Team} shall report security incident information to the authorities as required by federal, state, and/or local laws.

##  (IR-7) Incident Response Assistance

{{ORG ABBREVIATED NAME}} shall provide an incident response support resource, integral to {ORG Abbreviated Name} incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

##  (IR-8) Incident Response Plan

{{ORG ABBREVIATED NAME}} shall develop an incident response plan that:

* Provides {ORG Abbreviated Name} with a roadmap for implementing its incident response capability.
* Describes the structure and organization of the incident response capability.
* Provides a high-level approach for how the incident response capability fits into {ORG Abbreviated Name} overall structure.
* Meets the unique requirements of {ORG Abbreviated Name}, which relate to mission, size, structure, and functions.
* Defines reportable incidents:
	+ Breach
	+ Incident
	+ Event
* Provides metrics for measuring the incident response capability within {ORG Abbreviated Name}.
* Defines the resources and management support needed to effectively maintain and mature an incident response capability.
* Is reviewed and approved by {{ORG ABBREVIATED NAME}}.

{{ORG ABBREVIATED NAME}} shall distribute copies of the incident response plan to {ORG Abbreviated Name} technology staff & Incident Response Team. The Incident Response Plan shall be reviewed annually and updated to address {ORG Abbreviated Name} system changes or problems encountered during plan implementation, execution, or testing. Changes to the Incident Response Plan shall be communicated to {ORG Abbreviated Name} technology staff & Incident Response Team. The Incident Response Plan shall be deemed confidential and protected from unauthorized disclosure and modification.

## (IR-9) Information Spillage Response

The organization responds to information spills by:

a. Identifying the specific information involved in the information system contamination;

b. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;

c. Isolating the contaminated information system or system component;

d. Eradicating the information from the contaminated information system or component;

e. Identifying other information systems or system components that may have been subsequently contaminated; and

f. Performing other [Assignment: organization-defined actions].

# Procedures

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Security Officer | Validate compliance on a {Time Period} basis. |
| Human Resource Representatives | Provide policy during new hire process and informs personnel of changes. |
| Executive Director |  |
| Incident Response Team |  |
|  |  |
|  |  |

## 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 every three years and/or 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, third-party vendors, and other workers. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# References

# Forms (If applicable)

Tom C – should policy remain consistent throughout, individual nuances are covered in “appendix”

Conversation is around the policy itself …… refer to appendix

Any deviations in the policy will be covered in “appendix”