***Contingency Planning Policy***

version 1.0

August 2021

*ITC/ORG Name Here*

## 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)

[Contingency Planning Policies 1](#_1t3h5sf)

[Contingency Plan 1](#_4d34og8)

[Contingency Training 2](#_2s8eyo1)

[Contingency Plan Testing 2](#_17dp8vu)

[Alternate Storage Site 2](#_3rdcrjn)

[Alternate Processing Site 3](#_26in1rg)

[Telecommunications Services 3](#_lnxbz9)

[Information System Backup 3](#_35nkun2)

[Information System Recovery and Reconstitution 4](#_1ksv4uv)

[Procedures 4](#_44sinio)

[Resources 4](#_2jxsxqh)

[Roles and Responsibilities 4](#_z337ya)

[Train Personnel 4](#_3j2qqm3)

[Follow Up 4](#_1y810tw)

[Compliance 4](#_4i7ojhp)

[Documentation Compliance Review 4](#_2xcytpi)

[Security Officer Documentation Compliance Review 5](#_3whwml4)

[Acronyms/Definitions 6](#_2bn6wsx)

[References 7](#_qsh70q)

[Forms (If applicable) 8](#_3as4poj)

# 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. Contingency planning controls are in place to ensure that {{ORG ABBREVIATED NAME}’s} information system availability is maintained or recoverable in the event of an unplanned interruption to functionality.

## 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 controls required to maintain the availability of the system in the event of unplanned occurrences.

## Scope and Applicability

This policy applies to the information systems managed by {{ORG ABBREVIATED NAME}} and personnel involved in the design, development, and operation of information systems critical to the operation of {{ORG ABBREVIATED NAME}}.

Exceptions

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

# Contingency Planning Policies

## (CP-2) Contingency Plan

{{ORG ABBREVIATED NAME}} shall develop a contingency plan for the information system that identifies essential missions and business functions and associated contingency requirements, provides recovery objectives, restoration priorities, and metrics, addresses contingency roles, responsibilities, assigned personnel with contact information, addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure, addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented, and is reviewed and approved by {{ORG ABBREVIATED NAME}} Executive Director.

{{ORG ABBREVIATED NAME}} shall distribute copies of the contingency plan to personnel or groups with mission-critical responsibilities.

Contingency planning exercises, tests, and events shall be coordinated with Incident Response Team.

The contingency plan shall be reviewed for mission critical information systems annually, and updated where necessary to address changes to the {ORG Abbreviated Name} information system, environment, and/or any problems identified during plan implementation, execution, or testing.

Contingency plan changes shall be communicated to personnel or groups with mission-critical responsibilities upon approval. The contingency plan shall be protected from unauthorized changes.

The contingency plan development shall be managed by the business-process owners, and coordinated with Human Resources, and {ORG ABBREVIATED NAME} IT Staff.

|  |  |
| --- | --- |
| Mission Critical System | Recovery Time Objective |
| See appendix |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## (CP-3) Contingency Training

{{ORG ABBREVIATED NAME}} shall provide contingency training to personnel consistent with their assigned roles and responsibilities. Training shall occur within 30 days of assuming a contingency role, when an information system change merits, and annually thereafter.

## (CP-4) Contingency Plan Testing

{{ORG ABBREVIATED NAME}} shall test the contingency plan for mission-critical information systems annually. The business process owner shall ensure that the contingency plan is tested via tabletop exercise or walk-through. {ORG ABBREVIATED NAME}} IT Director shall ensure that a functional test of the information system is conducted. Tabletop exercises and functional tests must be documented to be considered complete. The documentation shall include a description of the test, personnel present, corrective actions, and other pertinent information.

Corrective actions shall be assigned an owner. The business process owner is responsible to ensure that corrective actions are completed, if necessary.

## (CP-6) Alternate Storage Site

{{ORG ABBREVIATED NAME}} shall maintain an alternate storage site, to include safe storage and retrieval agreements, to maintain the availability of information system backup information. The alternate storage site must provide physical security for the information that is at least the equivalent of the primary site.

The alternate storage site must be physically separate from the primary site to reduce the susceptibility to like threats. {{ORG ABBREVIATED NAME}} shall address potential accessibility issues to the alternate storage site in the event of an area-wide disruption or disaster, outlining explicit mitigation actions within their Business Continuity Plan.

## (CP-7) Alternate Processing Site

{{ORG ABBREVIATED NAME}} shall establish an alternate processing site, to include the necessary agreements to permit the transfer and resumption of mission critical systems and/or business functions within the time specified in the {ORG ABBREVIATED NAME} Disaster Recovery Plan.

The alternate processing site shall contain equipment and supplies required to transfer and resume operations or have contracts in place to support delivery to the site within time specified in the {ORG ABBREVIATED NAME} Disaster Recovery Plan for transfer/resumption.

{{ORG ABBREVIATED NAME}} ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

## (CP-8) Telecommunications Services

{{ORG ABBREVIATED NAME}} shall establish an alternate telecommunications services to include necessary agreements to permit the resumption of mission critical information system operations and/or business functions within the time specified in the {ORG ABBREVIATED NAME} Disaster Recovery Plan, when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

## (CP-9) Information System Backup

{{ORG ABBREVIATED NAME}} shall conduct backups of user-level information and system-level information contained in the information system, and information system documentation to include security-related documentation, all in support of recovery time and point objectives.

{{ORG ABBREVIATED NAME}} shall protect the confidentiality, integrity, and availability of backup information at all storage locations.

## (CP-10) Information System Recovery and Reconstitution

{{ORG ABBREVIATED NAME}} shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure as documented in the system baseline.

## (CP-11) Alternate Communications Protocols

The information system provides the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.

## (CP-12) Safe Mode

The information system, when [Assignment: organization-defined conditions] are detected, enters a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].

## (CP-13) Alternative Security Mechanism

The organization employs [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.

# 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}’s} 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 defined 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)