***System Maintenance 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)

[Systems Maintenance Policies 1](#_1t3h5sf)

[Controlled Maintenance 1](#_4d34og8)

[Maintenance Tools 2](#_2s8eyo1)

[Non-Local Maintenance 2](#_17dp8vu)

[Maintenance Personnel 2](#_3rdcrjn)

[Timely Maintenance 2](#_26in1rg)

[Procedures 2](#_lnxbz9)

[Resources 2](#_35nkun2)

[Roles and Responsibilities 2](#_1ksv4uv)

[Train Personnel 3](#_44sinio)

[Follow Up 3](#_2jxsxqh)

[Compliance 3](#_z337ya)

[Documentation Compliance Review 3](#_3j2qqm3)

[Security Officer Documentation Compliance Review 3](#_1y810tw)

[Acronyms/Definitions 4](#_4i7ojhp)

[References 5](#_2xcytpi)

[Forms (If applicable) 6](#_1ci93xb)

# 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. System maintenance controls are in place to protect the availability and integrity of information systems by determining the frequency and monitoring of maintenance of the information systems.

## 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 specific controls required for maintaining the information systems.

## Scope and Applicability

This policy applies to personnel who perform maintenance activities on any information systems managed by {{ORG ABBREVIATED NAME} }.

Exceptions

Please see Appendix “A” for organizational specific exceptions.

# Systems Maintenance Policies

## (MA-2) Controlled Maintenance

{{ORG ABBREVIATED NAME} IT Director:

* Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or {ORG Abbreviated Name} requirements.
* Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.
* Requires that Security Officer explicitly approve the removal of the information system or system components from {ORG Abbreviated Name} facilities for off-site maintenance or repairs.
* Sanitizes equipment to remove all information from associated media prior to removal from {ORG Abbreviated Name} facilities for off-site maintenance or repairs.
* Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
* Includes {{ORG Abbreviated Name} -defined maintenance-related information as outlined in Appendix “A”

## (MA-3) Maintenance Tools

{{ORG ABBREVIATED NAME} IT Director approves, controls, and monitors information system maintenance tools. Inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications. Checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

## (MA-4) Non-Local Maintenance

{{ORG ABBREVIATED NAME} IT Director:

* Approves and monitors nonlocal maintenance and diagnostic activities.
* Allows the use of non-local maintenance and diagnostic tools only as consistent with {ORG Abbreviated Name} policy and documented in the security plan for the information system.
* Employs strong authenticators in the establishment of non-local maintenance and diagnostic sessions.
* Maintains records for non-local maintenance and diagnostic activities.
* Terminates session and network connections when non-local maintenance is completed.
* Documents in the security plan for the information system, the policies and procedures for the establishment and use of non-local maintenance and diagnostic connections.

## (MA-5) Maintenance Personnel

{{ORG ABBREVIATED NAME} - IT Director:

* Establishes a process for maintenance personnel authorization and maintains a list of authorized {ORG Abbreviated Name} maintenance personnel.
* Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations.
* Designates {ORG Abbreviated Name} personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

## (MA-6) Timely Maintenance

{{ORG ABBREVIATED NAME} - obtains maintenance support and/or spare parts for all production systems within 48 hours of failure.

# Procedures

## Resources

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| Security Officer | Validate compliance on an annual basis. |
| IT Director | Provide policy during new hire process and informs personnel of changes. |
| Human Resources (HR) |  |
| Executive Director |  |
|  |  |
|  |  |

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

# References

# Forms (If applicable)