***System and Information Integrity 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)

[System and Information INtegrity Policies 1](#_1t3h5sf)

[Flaw Remediation 1](#_4d34og8)

[Malicious Code Protection 2](#_2s8eyo1)

[Information System Monitoring 3](#_17dp8vu)

[Security Alerts, Advisories, and Directives 4](#_3rdcrjn)

[Software, Firmware, and Information Integrity 5](#_26in1rg)

[Spam Protection 5](#_lnxbz9)

[Information Input Validation 6](#_35nkun2)

[Error Handling 6](#_1ksv4uv)

[Information Handling and Retention 6](#_44sinio)

[Memory Protection 7](#_2jxsxqh)

[Procedures 7](#_z337ya)

[Resources 7](#_3j2qqm3)

[Roles and Responsibilities 7](#_1y810tw)

[Train Personnel 7](#_4i7ojhp)

[Follow Up 7](#_2xcytpi)

[Compliance 7](#_1ci93xb)

[Documentation Compliance Review 8](#_3whwml4)

[Security Officer Documentation Compliance Review 8](#_2bn6wsx)

[Acronyms/Definitions 9](#_3as4poj)

[References 10](#_1pxezwc)

[Forms (If applicable) 11](#_49x2ik5)

# 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 and information integrity controls are in place to ensure that the security architecture protects the validity of the information processed by the information systems.

## Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information systems in use by {org abbreviated name} by determining the controls placed upon the inputs and outputs of the information systems.

## Scope and Applicability

This policy applies to all information systems and networks managed by {org abbreviated name}.

Exceptions

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

# System and Information Integrity Policies

## (SI-2) Flaw Remediation

{org abbreviated name} Technology Staff:

* Identifies, reports, and corrects information system flaws.
* Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
* Installs externally-visible security-relevant software and firmware updates within the timelines indicated below:
  + Critical/High – 48 hours
  + Moderate – 10 business days
  + Low - 40 business days
* Incorporates flaw remediation into the {org abbreviated name} configuration management process.
* {org abbreviated name} employs automated mechanisms to determine the state of information system components with regard to flaw remediation.

## (SI-3) Malicious Code Protection

{org abbreviated name}:

* Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
* Updates malicious code protection mechanisms whenever new releases are available in accordance with {org abbreviated name} configuration management policy and procedures.
* Configures malicious code protection mechanisms to:
  + Perform periodic scans of the information system {servers are real time scanned, end user systems real-time and daily scans} and real-time scans of files from external sources at network entry/exit points as the files are downloaded, opened, or executed in accordance with {org abbreviated} name security policies.
  + Block malicious code; quarantine malicious code; send alert to network administrator.in response to malicious code detection.
* Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

## (SI-4) Information System Monitoring

{org abbreviated name Technology Staff shall:

* monitor the information system to detect:
  + Attacks and indicators of potential attacks
  + Unauthorized local, network, and remote connections.
* Identifies unauthorized use of the information system
* Deploys monitoring devices:
  + (i) strategically within the information system to collect {org abbreviated name} determined essential information; and
  + (ii) at ad hoc locations within the system to track specific types of transactions of interest to {org abbreviated name}, within the core and up to district handoff
* Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
* Heightens the level of information system monitoring activity whenever there is an indication of increased risk to {org abbreviated name} operations, assets, individuals, and other {org abbreviated name} designated systems.
* Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.
* Provides system monitoring information to {org abbreviated name} Security Officer as needed; at least annually}.

## (SI-5) Security Alerts, Advisories, and Directives

{org abbreviated name} and/or Technology Staff)}:

* Receives information system security alerts, advisories, and directives from {at least CERT)} on an ongoing basis.
* Generates internal security alerts, advisories, and directives as deemed necessary.
* Disseminates security alerts, advisories, and directives to appropriate {org abbreviated name} personnel.
* Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

## (SI-7) Software, Firmware, and Information Integrity

{org abbreviated name} employs integrity verification tools to detect unauthorized changes to software, firmware, and information.

The information system performs an integrity check of at least transitional states or security-relevant events, at least daily.

## (SI-8) Spam Protection

{org abbreviated name}:

* Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
* Updates spam protection mechanisms when new releases are available in accordance with {org abbreviated name} configuration management policy and procedures.

{org abbreviated name} centrally manages spam protection mechanisms.

## (SI-12) Information Handling and Retention

{org abbreviated name} handles and retains information within the information system and information output from the system in accordance with applicable federal laws, state of Ohio laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

## (SI-13) Predictable Failure Prevention

The organization:

* Determines mean time to failure (MTTF) for [Assignment: organization-defined information system components] in specific environments of operation; and
* Provides substitute information system components and a means to exchange active and standby components at [Assignment: organization-defined MTTF substitution criteria].

## (SI-14) Non Persistence

The organization implements non-persistent [Assignment: organization-defined information system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]].

## (SI-16) Memory Protection

The information system implements memory resident anti-virus security safeguards to protect its memory from unauthorized code execution.

## (SI-17) Fail Safe Procedure

The information system implements [Assignment: organization-defined fail-safe procedures] when [Assignment: organization-defined failure conditions occur].

# Procedures

## Resources

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| {org abbreviated name} Technology Staff | Validate compliance on a {Time Period} basis. |
| Human Resources | Provide policy during new hire process and informs personnel of changes. |
|  |  |
|  |  |
|  |  |
|  |  |

## Train Personnel

Personnel are informed by a {{{ORG ABBREVIATED NAME} Human Resource} 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 |
| org abbreviated name | Management Council of the Ohio Education Computer Network |
| Personnel | Employees, contractors, consultants, temporary workers, and other workers. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# References

NIST 800-53

Perhaps separate references for some

# Forms (If applicable)