***System and Communications Protection 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 Communication Protection Policies 1](#_1t3h5sf)

[Application Partitioning 2](#_4d34og8)

[Information in Shared Resources 2](#_2s8eyo1)

[Denial of Service Protection 2](#_17dp8vu)

[Boundary Protection 2](#_3rdcrjn)

[Transmission Confidentiality and Integrity 3](#_26in1rg)

[Network Disconnect 4](#_lnxbz9)

[Cryptographic Key Establishment and Management 4](#_35nkun2)

[Cryptographic Protection 4](#_1ksv4uv)

[Collaborative Computing Devices 4](#_44sinio)

[Public Key Infrastructure Certificates 5](#_2jxsxqh)

[Mobile Code 5](#_z337ya)

[Voice Over Internet Protocol 5](#_3j2qqm3)

[Secure Name/Address Resolution Service (Authoritative Source) 5](#_1y810tw)

[Secure Name/Address Resolution Service (Recursive or Caching Resolver) 6](#_4i7ojhp)

[Architecture and Provisioning for Name/Address Resolution Service 6](#_2xcytpi)

[Session Authenticity 6](#_1ci93xb)

[Protection of Information at Rest 6](#_3whwml4)

[Process Isolation 6](#_2bn6wsx)

[Procedures 7](#_qsh70q)

[Resources 7](#_3as4poj)

[Roles and Responsibilities 7](#_1pxezwc)

[Train Personnel 7](#_49x2ik5)

[Follow Up 7](#_2p2csry)

[Compliance 7](#_147n2zr)

[Documentation Compliance Review 7](#_3o7alnk)

[Security Officer Documentation Compliance Review 7](#_23ckvvd)

[Acronyms/Definitions 8](#_32hioqz)

[References 9](#_1hmsyys)

[Forms (If applicable) 10](#_41mghml)

# 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 communication protection controls are in place to ensure that the security architecture properly isolates sensitive services and protects data both at rest and in-transit

## 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 inter-system communications.

## 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 Communication Protection Policies

## (SC-2) Application Partitioning

The information system separates user functionality including user interface services from information system management functionality.

## (SC-4) Information in Shared Resources

The information system prevents unauthorized and unintended information transfer via shared system resources.

## (SC-5) Denial of Service Protection

The information system takes reasonable measures to protect against or limit the effects of denial of service attacks.

## (SC-6) Resource Availability

The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]].

## (SC-7) Boundary Protection

 ({ORG ABBREVIATED NAME}’s} information system:

* Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.
* Implements subnetworks for publicly accessible system components that are physically, logically separated from internal {ORG Abbreviated Name} networks.
* Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with {ORG Abbreviated Name} security architecture.

## (SC-8) Transmission Confidentiality and Integrity

The information system protects the confidentiality, integrity of transmitted sensitive information.

The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information; detect changes to information during transmission unless otherwise protected by {ORG Abbreviated Name} defined alternative physical safeguards.

## (SC-11) Trusted Path

## The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication]

## (SC-12) Cryptographic Key Establishment and Management

 {{ORG Abbreviated Name} Technology Staff establishes and manages cryptographic keys for required cryptography employed within the information systems.

## (SC-13) Cryptographic Protection

The information system implements appropriate cryptographic controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

## (SC-15) Collaborative Computing Devices

The information system:

* Prohibits remote activation of collaborative computing devices unless otherwise authorized.
* Must provide an explicit indication of use to the users physically present at the device

## (SC-16) Transmission of Security Attributes

The information system associates [Assignment: organization-defined security attributes] with information exchanged between information systems and between system components.

## (SC-17) Public Key Infrastructure Certificates

The {{ORG Abbreviated Name} issues public key certificates under an {ORG Abbreviated Name} defined certificate policy or obtains public key certificates from an approved service provider.

## (SC-18) Mobile Code

{ORG Abbreviated Name} Technology Staff

* Defines acceptable and unacceptable mobile code and mobile code technologies.
* Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

## (SC-19) Voice Over Internet Protocol

{ORG Abbreviated Name} Technology staff)}:

* Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.
* Authorizes, monitors, and controls the use of VoIP within the information system.

## (SC-20) Secure Name/Address Resolution Service (Authoritative Source)

The information system:

* Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
* Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

## (SC-21) Secure Name/Address Resolution Service (Recursive or Caching Resolver)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

## (SC-22) Architecture and Provisioning for Name/Address Resolution Service

The information systems that collectively provide name/address resolution service for {ORG Abbreviated Name} are fault-tolerant and implement internal/external role separation.

## (SC-23) Session Authenticity

The information system protects the authenticity of communications sessions.

## (SC-24) Fail in Known State

The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.

## (SC-25) Thin Node.

The organization employs [Assignment: organization-defined information system components] with minimal functionality and information storage.

##  (SC-28) Protection of Information at Rest

The information system protects the confidentiality, integrity and availability of information at rest.

## (SC-29) Heterogeneity

 The organization employs a diverse set of information technologies for [Assignment: organization-defined information system components] in the implementation of the information system.

## (SC-31) Covert Chain Analysis

The organization:

* Performs a covert channel analysis to identify those aspects of communications within the information system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and
* Estimates the maximum bandwidth of those channels.

## (SC-32) Information System Partitioning

The organization partitions the information system into [Assignment: organization-defined information system components] residing in separate physical domains or environments based on [Assignment: organization-defined circumstances for physical separation of components].

## (SC-36) Distributed Processing and Storage.

The organization distributes [Assignment: organization-defined processing and storage] across multiple physical locations.

## (SC-37) Out of Band Channels

The organization employs [Assignment: organization-defined out-of-band channels] for the physical delivery or electronic transmission of [Assignment: organization-defined information, information system components, or devices] to [Assignment: organization-defined individuals or information systems].

## (SC-38) Operation Security

## The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle.

##  (SC-39) Process Isolation

The information system maintains a separate execution domain for each executing process.

## (SC-40) Wireless Link Protection

The information system protects external and internal [Assignment: organization-defined wireless links] from [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].

##  (SC-41) Port and I/O Devices Access.

The organization physically disables or removes [Assignment: organization-defined connection ports or input/output devices] on [Assignment: organization-defined information systems or information system components].

##  (SC-43) Usage Restrictions

The organization:

* Establishes usage restrictions and implementation guidance for [Assignment: organization-defined information system components] based on the potential to cause damage to the information system if used maliciously; and
* Authorizes, monitors, and controls the use of such components within the information system.

## (SC-44) Detonation Chambers

The organization employs a detonation chamber capability within [Assignment: organization-defined information system, system component, or location].

# Procedures

## Resources

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| {ORG Abbreviated Name} Technology Staff | 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}’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, and other workers. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# References

# Forms (If applicable)