

***Physical and Environmental 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 2](#_Toc83815165)

[Document Change History 2](#_Toc83815166)

[Introduction 5](#_Toc83815167)

[Background 5](#_Toc83815168)

[Purpose 5](#_Toc83815169)

[Scope and Applicability 5](#_Toc83815170)

[Physical and Environmental Protection Policies 5](#_Toc83815171)

[(PE-2) Physical Access Authorizations 5](#_Toc83815172)

[(PE-3) Physical Access Control 5](#_Toc83815173)

[(PE-4) Access Control for Transmission Medium 6](#_Toc83815174)

[(PE-5) Access Control for Output Devices 6](#_Toc83815175)

[(PE-6) Monitoring Physical Access 6](#_Toc83815176)

[(PE-8) Visitor Access Records 6](#_Toc83815177)

[(PE-9) Power Equipment and Cabling 7](#_Toc83815178)

[(PE-10) Emergency Shutoff 7](#_Toc83815179)

[(PE-11) Emergency Power 7](#_Toc83815180)

[(PE-12) Emergency Lighting 7](#_Toc83815181)

[(PE-13) Fire Protection 7](#_Toc83815182)

[(PE-14) Temperature and Humidity Controls 7](#_Toc83815183)

[(PE-15) Water Damage Protection 7](#_Toc83815184)

[(PE-16) Delivery and Removal 8](#_Toc83815185)

[(PE-17) Alternate Work Site 8](#_Toc83815186)

[(PE-18) Location of Information System Components 8](#_Toc83815187)

[(PE-19) Information Leakage 8](#_Toc83815188)

[(PE-20) Asset Monitoring and Tracking 8](#_Toc83815189)

[Procedures 8](#_Toc83815190)

[Resources 8](#_Toc83815191)

[Roles and Responsibilities 8](#_Toc83815192)

[Train Personnel 9](#_Toc83815193)

[Follow Up 9](#_Toc83815194)

[Compliance 9](#_Toc83815195)

[Documentation Compliance Review 9](#_Toc83815196)

[Security Officer Documentation Compliance Review 9](#_Toc83815197)

[Acronyms/Definitions 10](#_Toc83815198)

[References 11](#_Toc83815199)

[Forms (If applicable) 12](#_Toc83815200)

# 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. Physical and environmental protection controls are in place to protect the interests of {{ORG ABBREVIATED NAME}’s} information systems and personnel by providing a safe, secure, and reliable environment in which to work.

## Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information stored within the information systems held, authorized, and in use by {{ORG ABBREVIATED NAME}} by defining the specific controls required for physical and environmental protections required for the facilities and the information systems.

## Scope and Applicability

This policy applies to all facilities that process information {{ORG ABBREVIATED NAME}} and all personnel within those facilities.

Exceptions

Please see Appendix “A” for organizational specific exceptions.

# Physical and Environmental Protection Policies

## (PE-2) Physical Access Authorizations

{{ORG ABBREVIATED NAME}’s Security Officer, Human Resources, and Facilities Management:

* Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides.
* Issues authorization credentials for facility access.
* Reviews the access list detailing authorized facility access by individuals at a minimum annually.
* Removes individuals from the facility access list when access is no longer required.

## (PE-3) Physical Access Control

 {{ORG ABBREVIATED NAME}’s Security Officer, Human Resources, and Facilities Management}:

* Enforces physical access authorizations at {ORG Abbreviated Name} -defined entry/exit points to the facility where the information system resides.
* Verifies individual access authorizations before granting access to the facility.
* Controls ingress/egress to the facility using {ORG Abbreviated Name} -defined physical access control systems/devices.
* Maintains physical access audit logs for {ORG Abbreviated Name} -defined entry/exit points.
* Provides {ORG Abbreviated Name} -defined security safeguards to control access to areas within the facility officially designated as publicly accessible.
* {ORG ABBREVIATED NAME} IT Staff escorts visitors and monitors visitor activity for {ORG Abbreviated Name} -defined circumstances requiring visitor escorts and monitoring.
* Secures keys, combinations, and other physical access devices.
* Human Resources, Receptionist, and Facilities Management inventories {ORG Abbreviated Name} -defined physical access devices at a minimum annually.
* Facilities Management changes combinations and keys at a minimum annually when keys are lost, combinations are compromised, or individuals are transferred or terminated.

## (PE-4) Access Control for Transmission Medium

{{ORG ABBREVIATED NAME}’s Security Officer, Human Resources, and Facilities Management} controls physical access to {ORG Abbreviated Name} -defined information system distribution and transmission lines within {ORG Abbreviated Name} facilities using {ORG Abbreviated Name} -defined security safeguards.

## (PE-5) Access Control for Output Devices

{{ORG ABBREVIATED NAME}’s Security Officer and IT Staff controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

## (PE-6) Monitoring Physical Access

{{ORG ABBREVIATED NAME}’s Security Officer, Human Resources, and Facilities Management}:

* Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.
* Reviews physical access logs quarterly and upon occurrence of {ORG Abbreviated Name} -defined security events or potential indications of security events.
* Coordinates results of reviews and investigations with the {ORG Abbreviated Name} incident response capability.

##  (PE-8) Visitor Access Records

{{ORG ABBREVIATED NAME}’s Security Officer, Human Resources, Facilities Management, and/or Receptionist}

* Maintains visitor access records to the facility where the information system resides for at least 1 year.
* Reviews visitor access records quarterly.

## (PE-9) Power Equipment and Cabling

{{ORG ABBREVIATED NAME}’s Security Officer, IT Staff and Facilities Management protects power equipment and power cabling for the information system from damage and destruction.

## (PE-10) Emergency Shutoff

{{ORG ABBREVIATED NAME}’s Security Officer, IT Staff, and Facilities Management}

* Provides the capability of shutting off power to the information system or individual system components in emergency situations.
* Places emergency shutoff switches or devices to facilitate safe and easy access for personnel.
* Protects emergency power shutoff capability from unauthorized activation.

## (PE-11) Emergency Power

{{ORG ABBREVIATED NAME}} provides a short-term uninterruptible power supply until facility power is restored, or an orderly shutdown of the information system occurs; or transition of the information system to long-term alternate power in the event of a primary power source loss.

## (PE-12) Emergency Lighting

{{ORG ABBREVIATED NAME}} employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

## (PE-13) Fire Protection

{{ORG ABBREVIATED NAME}} employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

## (PE-14) Temperature and Humidity Controls

{{ORG ABBREVIATED NAME}’s Facilities Management:

* Maintains temperature and humidity levels within the facility where the information system resides at {ORG Abbreviated Name} -defined acceptable levels.
* Monitors temperature and humidity levels continually.

## (PE-15) Water Damage Protection

{{ORG ABBREVIATED NAME}’s Facilities Management protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

## (PE-16) Delivery and Removal

{{ORG ABBREVIATED NAME}‘s Facilities Management, IT Staff authorizes, monitors, and controls {ORG Abbreviated Name} -defined types of information system components entering and exiting the facility and maintains records of those items.

## (PE-17) Alternate Work Site

{{ORG ABBREVIATED NAME}’s Security Officer and IT Staff}:

* Employs {ORG Abbreviated Name} -defined security controls at alternate work sites.
* Assesses as feasible, the effectiveness of security controls at alternate work sites.
* Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

## (PE-18) Location of Information System Components

The organization positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access

## (PE-19) Information Leakage

The organization protects the information system from information leakage due to electromagnetic signals emanations.

## (PE-20) Asset Monitoring and Tracking

The organization:

a. Employs [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas]; and

b. Ensures that asset location technologies are employed in accordance with applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance.

# 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 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 ITC 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)