***Personnel Security 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)

[Personnel Security Policies 1](#_1t3h5sf)

[Position Risk Designation 1](#_4d34og8)

[Personnel Screening 1](#_2s8eyo1)

[Personnel Termination 1](#_17dp8vu)

[Personnel Transfer 2](#_3rdcrjn)

[Access Agreements 2](#_26in1rg)

[Third-Party Personnel Security 2](#_lnxbz9)

[Personnel Sanctions 2](#_35nkun2)

[Procedures 3](#_1ksv4uv)

[Resources 3](#_44sinio)

[Roles and Responsibilities 3](#_2jxsxqh)

[Train Personnel 3](#_z337ya)

[Follow Up 3](#_3j2qqm3)

[Compliance 3](#_1y810tw)

[Documentation Compliance Review 3](#_4i7ojhp)

[Security Officer Documentation Compliance Review 4](#_2xcytpi)

[Acronyms/Definitions 5](#_3whwml4)

[References 6](#_2bn6wsx)

[Forms (If applicable) 7](#_qsh70q)

# 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. Personnel security controls are in place to ensure that all personnel are properly screened, informed, and managed through all phases of employment.

## Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information systems in use by {{ORG ABBREVIATED NAME}} by describing the controls related to the management of human resources.

## Scope and Applicability

This policy applies to all personnel who interact with information systems held by {ORG ABBREVIATED NAME}.

Exceptions

Please see Appendix “A” for organizational specific exceptions.

# Personnel Security Policies

## (PS-2) Position/Roles Risk Designation

{{ORG ABBREVIATED NAME}’s Security Officer, IT Staff, Human Resources, and Executive Director:

* Assigns a risk designation to all {ORG Abbreviated Name} positions/roles.
* Establishes screening criteria for personnel filling those positions/roles.
* Reviews and updates position/roles risk designations at least annually.

## (PS-3) Personnel Screening

{{ORG ABBREVIATED NAME}’s Security Officer, IT Staff, Human Resources, and Executive Director}:

* Screens personnel prior to authorizing access to the information system.
* Rescreens personnel according to {ORG Abbreviated Name} -defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening every 5 years thereafter

## (PS-4) Personnel Termination

{{ORG ABBREVIATED NAME}}, upon termination of personnel employment:

* Disables information system access immediately for involuntary and close of business for voluntary.
* Terminates/revokes any authenticators/credentials associated with the personnel.
* Conducts exit interviews that include a discussion of {ORG Abbreviated Name} -defined information security topics.
* Retrieves all security-related {ORG Abbreviated Name} information system-related property.
* Retains access to {ORG Abbreviated Name} information and information systems formerly controlled by terminated personnel.
* Notifies all relevant parties within 30 days.

## (PS-5) Personnel Transfer

{{ORG ABBREVIATED NAME}’s Security Officer, IT Staff, Human Resources, and Executive Director}:

* Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within {ORG Abbreviated Name}
* Initiates {ORG Abbreviated Name} -defined transfer or reassignment actions within {ORG Abbreviated Name} -defined time period.
* Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
* Notifies relevant parties within 30 days.

## (PS-6) Access Agreements

{{ORG ABBREVIATED NAME}’s Security Officer, IT Staff, Human Resources, and Executive Director}:

* Develops and documents access agreements for {ORG Abbreviated Name} information systems.
* Reviews and updates the access agreements annually.
* Ensures that personnel requiring access to {ORG Abbreviated Name} information and information systems:
	+ Sign appropriate access agreements prior to being granted access.
	+ Re-sign access agreements to maintain access to {ORG Abbreviated Name} information systems when access agreements have been updated or every 3 – 5 years thereafter.

## (PS-7) Third-Party Personnel Security

{{ORG ABBREVIATED NAME}’s Security Officer, IT Staff, Human Resources, and Executive Director}:

* Establishes personnel security requirements including security roles and responsibilities for third-party providers.
* Requires third-party providers to comply with personnel security policies and procedures established by the {ORG Abbreviated Name}.
* Documents personnel security requirements.
* Requires third-party providers to notify {ORG Abbreviated Name} -defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess {ORG Abbreviated Name} credentials and/or badges, or who have information system privileges within 1 day.
* Monitors provider compliance.

## (PS-8) Personnel Sanctions

{{ORG ABBREVIATED NAME}}:

* Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures and
* Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

# 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} 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)