***Media 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](#_Toc83814822)

[Document Change History 2](#_Toc83814823)

[Introduction 4](#_Toc83814824)

[Background 4](#_Toc83814825)

[Purpose 4](#_Toc83814826)

[Scope and Applicability 4](#_Toc83814827)

[Media Protection Policies 4](#_Toc83814828)

[(MP-2) Media Access 4](#_Toc83814829)

[(MP-3) Media Marking 5](#_Toc83814830)

[(MP-4) Media Storage 5](#_Toc83814831)

[(MP-5) Media Transport 5](#_Toc83814832)

[(MP-6) Media Sanitization 5](#_Toc83814833)

[(MP-7) Media Use 6](#_Toc83814834)

[(MP-8) Media Downgrading 6](#_Toc83814835)

[Procedures 6](#_Toc83814836)

[Resources 6](#_Toc83814837)

[Roles and Responsibilities 6](#_Toc83814838)

[Train Personnel 6](#_Toc83814839)

[Follow Up 7](#_Toc83814840)

[Compliance 7](#_Toc83814841)

[Documentation Compliance Review 7](#_Toc83814842)

[Security Officer Documentation Compliance Review 7](#_Toc83814843)

[Acronyms/Definitions 8](#_Toc83814844)

[References 9](#_Toc83814845)

[Forms (If applicable) 10](#_Toc83814846)

# Introduction

## Background

This policy is authorized and in use by {{ORG Name} hereafter referred to as {ORG Abbreviated Name} abbreviation) }, 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. Media protection controls are in place to protect the confidentiality and integrity of information systems by determining the level of protection required for storage of the data processed by the information systems.

## 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 storage of the information systems protected data.

## Scope and Applicability

This policy applies to all media that contains information processed by any information systems held by the {{ORG ABBREVIATED NAME}.

Exceptions

Please see Appendix “A” for organizational specific exceptions.

# Media Protection Policies

## (MP-2) Media Access

{{ORG ABBREVIATED NAME} restricts access to {{ORG Abbreviated Name} -defined types of digital and/or non-digital media} to {{ORG Abbreviated Name} -defined personnel or roles}.

|  |  |
| --- | --- |
| Data Classification | Role / Access Requirements |
| PII or Corporate Highly Confidential | Security Officer / -  {ORG Abbreviated Name} Technology Staff / -  Executive Director - |
| Confidential | Security Officer / -  {ORG Abbreviated Name} Technology Staff / -  Executive Director - |
| Public | Public |

## (MP-3) Media Marking

{{ORG ABBREVIATED NAME} Security Office and Technology Staff:

* Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.
* Exempts any {ORG ABBREVIATED NAME} defined data from marking as long as the media remains within {{ORG ABBREVIATED NAME} defined areas.

## (MP-4) Media Storage

{{ORG ABBREVIATED NAME} Technology Staff

* Physically controls and securely stores {ORG Abbreviated Name} defined media within {ORG Abbreviated Name} -defined areas.
* Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

## (MP-5) Media Transport

{{ORG ABBREVIATED NAME} Security Officer and IT Technology Staff

* Protects and controls {ORG Abbreviated Name} -defined media during transport outside of controlled areas using {ORG Abbreviated Name} -defined security safeguards.
* Maintains accountability for information system media during transport outside of controlled areas.
* Documents activities associated with the transport of information system media.
* Restricts the activities associated with the transport of information system media to authorized personnel.
* (MP-5.4) The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

## (MP-6) Media Sanitization

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

* Sanitizes {ORG Abbreviated Name} -defined media prior to disposal, release out of {ORG Abbreviated Name} control, or release for reuse using {ORG Abbreviated Name} -defined sanitization techniques and procedures in accordance with applicable federal and {ORG Abbreviated Name} standards and policies.
* Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

## (MP-7) Media Use

{{ORG ABBREVIATED NAME} Security Officer and IT Technology Staff restricts, prohibits the use of {{ORG Abbreviated Name} -defined types of information system media on {{ORG Abbreviated Name} -defined information systems or system components using {{ORG Abbreviated Name} -defined security safeguards}.

## (MP-8) Media Downgrading

The organization:

a. Establishes [Assignment: organization-defined information system media downgrading process] that includes employing downgrading mechanisms with [Assignment: organization-defined strength and integrity];

b. Ensures that the information system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;

c. Identifies [Assignment: organization-defined information system media requiring downgrading]; and

d. Downgrades the identified information system media using the established process.

# 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} 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 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)