***Configuration Management 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)

[Configuration Management Policies 1](#_1t3h5sf)

[Baseline Configuration 1](#_4d34og8)

[Configuration Change Control 2](#_2s8eyo1)

[Security Impact Analysis 3](#_17dp8vu)

[Access Restrictions for Change 3](#_3rdcrjn)

[Configuration Settings 3](#_26in1rg)

[Least Functionality 3](#_lnxbz9)

[Information System Component Inventory 3](#_35nkun2)

[Configuration Management Plan 4](#_1ksv4uv)

[Software Usage Restrictions 4](#_44sinio)

[User Installed Software 5](#_2jxsxqh)

[Procedures 5](#_z337ya)

[Resources 5](#_3j2qqm3)

[Roles and Responsibilities 5](#_1y810tw)

[Train Personnel 5](#_4i7ojhp)

[Follow Up 5](#_2xcytpi)

[Compliance 6](#_1ci93xb)

[Documentation Compliance Review 6](#_3whwml4)

[Security Officer Documentation Compliance Review 6](#_2bn6wsx)

[Acronyms/Definitions 7](#_3as4poj)

[References 8](#_1pxezwc)

[Forms (If applicable) 9](#_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. Configuration management controls are in place to ensure that {{ORG ABBREVIATED NAME} information systems are maintained in a known state, updated in accordance with corporate policy, and identifies un-authorized changes to promote a stable system.

## Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information stored within the information systems managed, authorized, and in use by {{ORG ABBREVIATED NAME} by defining the specific controls required to change or update the information systems.

## Scope and Applicability

This policy applies to the information systems managed by {{ORG ABBREVIATED NAME} and personnel involved in the maintenance, update, or deprecation thereof.

Exceptions

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

# Configuration Management Policies

## (CM-2) Baseline Configuration

For mission critical systems, {{ORG ABBREVIATED NAME} shall develop, document, and maintain under version control a current baseline configuration of the information system. The baseline shall provide the hardware and software components of the system and any configuration information or steps required to bring this system into service.

.

## (CM-3) Configuration Change Control

Change Control is a formal process used to ensure that changes to a product or system are introduced in a controlled and coordinated manner. It reduces the possibility that unnecessary changes will be introduced to a system without forethought, introducing faults into the system, or undoing changes made by other users of the software. The goals of a Change Control procedure include minimal disruption to services, reduction in back-out activities, and cost-effective utilization of resources involved in implementing change.

The following change types will be regarded as changes within the scope of this policy:

* Operating System installation, update, or modification.
* Application installation, update, or modification.
* Any change to an Access Control list on a Firewall or other network device in support of the information system.
* Changes to group permissions.
* Database changes, including but not limited to table adds, moves, or deletion.
* Patch installation.

## (CM-4) Security Impact Analysis

{{ORG ABBREVIATED NAME} Change Review Committee will develop and maintain a Security Impact Analysis checklist. The checklist must be included in each Change Control ticket. The change approver will review the Security Impact Analysis prior to approving the change request, and escalate to the {{ORG ABBREVIATED NAME} Security Officer when the requested change negatively impacts the security posture of the environment.

## (CM-5) Access Restrictions for Change

Changes to the system may only be made by authorized Systems Administrators. Systems shall be configured to require elevated access to perform change, and access to System Administrative accounts will be restricted to those who require elevated access to perform their job functions.

## (CM-6) Configuration Settings

Systems Administrators will document the configuration settings for information technology products during deployment. These will be stored in the baseline configuration document, and reviewed and utilized when subsequent deployments occur, if applicable. Like-kind deployments shall utilize the same configuration settings as prior deployments to ensure consistency within the environment. Deviations from the established configuration settings shall be documented in a change control record, to include a Security Impact Analysis, and reviewed during the scheduled quarterly review meeting.

For mission critical systems, changes to configuration setting files are to be monitored by file integrity management software and reported to the Change Review Committee. Unauthorized changes will be investigated by the Change Control committee and the responsible manager.

## (CM-7) Least Functionality

Mission critical systems shall be configured to provide only essential services. On networked systems, unneeded services, ports, and processes shall be blocked and turned off. Necessary services and processes shall be listed in the Baseline Configuration document for the system. Firewalls shall be configured in a Deny-Unless-Specifically-Allowed stance, and any open network port to a production server requires a business need be documented by the change requestor and approved by the Change Review Committee, IT Director, or Security Officer.

In addition to file integrity management, regular network scans, and anti-virus/anti-malware software running on all systems, production systems shall be reviewed by the Systems Administrator no less than {annually} to determine if the processes listed in the Baseline Configuration are current and if there are any unauthorized processes or services running on the system. Anti-virus/anti-malware software is to be installed on all systems, regularly maintained, and configured to block known viral and malicious programs from execution.

## (CM-8) Information System Component Inventory

{{ORG Abbreviated Name} IT Technology Staff shall maintain an inventory of production systems that accurately reflects the current systems. The inventory will include:

* Public and Private IP address
* Hostname
* System description
* Hardware type
* Serial number
* Additional notes

Additional hardware and detailed system specifications are maintained in the Baseline Configuration document for the production system to include:

* Processor(s)
* Firmware
* Memory
* Storage hardware
* Installed software

The information system component inventory shall be kept up to date at all times, and is reviewed no less than annually by the {ORG Abbreviated Name} IT Technology Staff

{ORG Abbreviated Name} IT Technology Staff shall maintain an inventory of all physical information system assets. This inventory includes company-owned servers, desktops, laptops, and tablets, and non-information processing hardware such as monitors, phones, and projectors. This inventory contains asset tags, serial numbers, and a description of the assets, and is audited every {year}.

{ORG Abbreviated Name} IT Technology Staff maintains a software inventory of all licensed and approved software in the environment. This software inventory is updated as new software is purchased or old software is deprecated. It is reviewed at a minimum annually.

## (CM-9) Configuration Management Plan

Mission critical systems may be repurposed for other functions when they are no longer viable for their original purpose. The IT Director is responsible for the reallocation of hardware resources and approves all reallocations. These changes are documented within the change management system when they occur, and the information system component inventory is updated. Any media that may have stored sensitive information is to be sanitized in accordance with the Media Protection policy: Media Sanitation section.

## (CM-10) Software Usage Restrictions

On all systems, personnel are required to report any unauthorized use of software that they encounter to the IT Director. Use of software in violation of copyright laws or EULA’s is not tolerated or permitted.

{{ORG ABBREVIATED NAME} IT Director shall track the use of software protected by quantity licenses on their software inventory.

Peer-to-peer file sharing technology is prohibited on mission critical systems and specifically blocked at the perimeter. On non-production systems, file sharing software may be used for legitimate software or operating system acquisition, but never for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

## (CM-11) User Installed Software

Personnel, other than Systems Administrators, are specifically prohibited from installing software on mission critical systems. Mission critical systems shall be configured such that elevated privileges are required to install software.

If business need is documented, personnel users may be granted elevated privileges to non-mission critical systems. The IT Director maintains the list of users and the approval for elevated privileges. These users permitted to install software on their non-mission critical systems so long as it does not violate copyright law and it does not compromise the security of the system.

# 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 an annual basis.

# Acronyms/Definitions

|  |  |
| --- | --- |
| Acronym/Term | Definition |
| MC {ORG ABBREVIATED NAME} NAME | Management Council of the Ohio Education Computer Network |
| Personnel | Employees, contractors, consultants, temporary workers, and other workers. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# References

# Forms (If applicable)