***ACCESS CONTROL 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](#_Toc82752940)

[Document Change History 2](#_Toc82752941)

[Introduction 5](#_Toc82752942)

[Background 5](#_Toc82752943)

[Purpose 5](#_Toc82752944)

[Scope and Applicability 5](#_Toc82752945)

[Access Control Policies 5](#_Toc82752946)

[(AC-2) Account Management 5](#_Toc82752947)

[(AC-3) Access Enforcement 6](#_Toc82752948)

[(AC-4) Information Flow enforcement 6](#_Toc82752949)

[(AC-5) Separation of Duties 7](#_Toc82752950)

[(AC-6) Least Privilege 7](#_Toc82752951)

[(AC-7) Unsuccessful Login Attempts 7](#_Toc82752952)

[(AC-8) System Use Notification 7](#_Toc82752953)

[(AC-9) Previous Logon (Access) Notification 8](#_Toc82752954)

[(AC-11) Session Lock 8](#_Toc82752955)

[(AC-12) Session Termination 8](#_Toc82752956)

[(AC-14) Permitted Actions Without Identification or Authentication 8](#_Toc82752957)

[(AC-17) Remote Access 9](#_Toc82752958)

[(AC-18) Wireless Access 9](#_Toc82752959)

[(AC-19) Access Controls for Mobile Devices 9](#_Toc82752960)

[(AC-20) Use of External Information Systems 10](#_Toc82752961)

[(AC-21) Information Sharing 10](#_Toc82752962)

[(AC-24) Access Control Decisions 10](#_Toc82752963)

[Procedures 10](#_Toc82752964)

[Resources 10](#_Toc82752965)

[Roles and Responsibilities 10](#_Toc82752966)

[Train Personnel 10](#_Toc82752967)

[Follow Up 11](#_Toc82752968)

[Compliance 11](#_Toc82752969)

[Documentation Compliance Review 11](#_Toc82752970)

[Security Officer Documentation Compliance Review 11](#_Toc82752971)

[Acronyms/Definitions 12](#_Toc82752972)

[References 13](#_Toc82752973)

[Forms (If applicable) 14](#_Toc82752974)

# 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. Access controls are in place to protect the interests of all authorized personnel of {{ORG ABBREVIATED NAME}’s} information systems by providing a safe, secure, and reliable environment in which to work. Therefore, only authorized personnel can access specific information assets.

## 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 for access to the information systems.

## Scope and Applicability

This policy applies to personnel who are granted access to any information systems managed by {{ORG ABBREVIATED NAME}}.

Exceptions

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

# Access Control Policies

## (AC-2) Account Management

Information system accounts in support of mission critical functions will be identified and categorized in the table below.

Each category of account will have an identified Account Manager who will establish the conditions for group or role membership.

Account Managers will maintain a list of authorized users of their respective information systems, along with the mission supporting need for the account.

Access to an information system without a specific business need as applied to a group or role requires authorization from ORG abbreviated name IT Directo}. Exceptions to this control must be reported, with authorization, to the ORG abbreviated name Security Officer.

Accounts are to be requested and access granted to information systems in accordance with personnel job functions. Human Resources will notify Account Managers upon personnel hire, transfer, or termination. Account Managers are responsible to identify when an information system usage or access requirement changes and accounts or access for assigned roles on that system are no longer necessary.

Account Managers will retain the request for user account creation, the intended use of the account, and other information that pertains to the use of that account as required.

Account Managers are required to review the accounts for which they are responsible regularly, with a time period based on the account sensitivity. Account Managers will maintain records of their review. Account Managers are responsible to ensure that shared account authentication methods are modified upon transfer or termination of an authorized shared account holder.

|  |  |  |
| --- | --- | --- |
| Account Group | Account Manager | Sensitivity / Review Frequency |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## (AC-3) Access Enforcement

All information systems shall enforce access authorizations for logical access in accordance with this policy.

## (AC-4) Information Flow enforcement

The information system shall restrict access to authorized pathways and control the flow of information by the deployment of:

* Firewall and Access Control Lists
* Elimination and disabling of unneeded services
* Requiring authentication on all services which provide access to sensitive information.

## (AC-5) Separation of Duties

In order to ensure that no personnel can provide greater access to an information system without collusion present, administrators should not have more than two of the listed roles. Where it is not possible to segregate duties, monitoring controls shall be employed to ensure that greater access cannot be provided without detection. (roles indicated below are examples only)

|  |  |
| --- | --- |
| Duty or Role | Titles/Groups/Account Manager |
| Firewall Administrator |  |
| Information System Administrator |  |
| Network Administrator |  |
| Logging/Monitoring |  |
| File Integrity Monitoring |  |
| Application Developer |  |

## (AC-6) Least Privilege

Authorized access for personnel shall be restricted to the access required for them to perform their function. Neither physical nor logical access is given without a mission requirement or business need.

Security functions within the system, such as system administration functions like creation and deletion of user accounts, shall be limited to those who require this level of access to perform their job functions.

## (AC-7) Unsuccessful Login Attempts

The information system shall enforce a limit of 5 or less consecutive invalid login attempts by a user, and will {Lock / Disable} the offending account for a period of Minimum 15 minutes or until released by the Account Manager or designated system administrator.

## (AC-8) System Use Notification

All systems shall provide notice to users before granting access that provides privacy and security notice consistent with applicable federal, state, and local laws. The notice shall include notification that:

* Users are entering a private system
* Information system usage may be monitored, recorded, and/or subject to audit
* Unauthorized use is prohibited and may be subject to criminal and/or civil penalties
* Use of the system implies consent to monitoring

The notification should remain on the screen until acknowledged by the user.

The text of the notification will contain the following:

“This is a private information system. This system is private property and is provided only for authorized use. This system will be monitored for lawful purposes. All information placed on or sent over this system may be monitored. Unauthorized use may subject you to administrative action and/or civil or criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for prosecution. Use of this system constitutes consent to monitoring.”

Publicly accessible systems shall display a system use notification prior to granting further access. The notice should contain:

* Intended use of the system
* Information system usage may be monitored, recorded, and/or subject to audit

## (AC-9) Previous Logon (Access) Notification

The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access).

(AC-10) Concurrent Session Control

The information system limits the number of concurrent sessions for each administrative account to five.

## (AC-11) Session Lock

The information system shall lock and force a user to re-authenticate after 3o minutes of inactive time or upon request from the user. The locked session should not allow view of active work projects on the screen.

## (AC-12) Session Termination

The information system shall terminate a user session that is inactive for 60 minutes on systems that process {PII / Sensitive Information}.

## (AC-14) Permitted Actions Without Identification or Authentication

Personnel and others are permitted access to public-facing web systems, kiosks, and other public services without authentication. Areas of the facilities that are designated for public access may be visited without identification or authentication.

Specific information systems that provide non-sensitive public data are listed below.

|  |  |
| --- | --- |
| Information System | Purpose |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

##  (AC-17) Remote Access

Personnel whose responsibilities may require working from remote locations will be provided with VPN access to the information system. VPN users are instructed that use of the VPN follows the same rules, guidance, and code of conduct as use of internal information systems, and that use may be monitored for compliance with such. VPN Access must be authorized for the role that the VPN user fulfills for {ORG Abbreviated Name}

The system that provides VPN access must be monitored and log user authentications, both failed and successful, and time active sessions.

##  (AC-18) Wireless Access

Wireless access may be provided for multiple purposes.

Guest wireless access may be provided for non-personnel or non-company owned equipment. The guest wireless network should be treated as an untrusted network, and only access publicly available systems without further authentication. Guest wireless users must be informed that the wireless network is monitored in accordance with the system use notification. Guest wireless may or may not be encrypted.

Personnel wireless access for business use shall employ a personal authentication method and require encryption for all communication channels. This wireless network may provide access to non-public services, but shall still require authentication for access to these services. This level of access shall be restricted to company owned devices.

## (AC-19) Access Controls for Mobile Devices

Mobile devices shall not be permitted direct access to sensitive information systems. Mobile devices shall be used in accordance with a personally-owned devices agreement and only in support of mission critical functions when necessary. Mobile devices shall not be permitted to download or store sensitive information.

## (AC-20) Use of External Information Systems

Trust relationships with external systems may be necessary to support mission critical functions or business needs. External information systems must meet or exceed the standards for internal systems based on the type of data processed. Users of external information systems shall be managed by an Account Manager in accordance with Account Management Policies.

Use of external systems to process information other-than-public shall require an agreement authorized by the Executive Director and containing the following controls:

## (AC-21) Information Sharing

Sharing control of sensitive information may also be required in order to perform mission critical functions. The storage of {{ORG ABBREVIATED NAME}} owned data must match the access restrictions required for that data internally. Sharing of sensitive data must be authorized by the Executive Director and reviewed annually for continued need and compliance.

## (AC-24) Access Control Decisions

The organization establishes procedures to ensure security reviews are applied to each access request prior to access enforcement.

# 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. |
| Account Manager |  |
| IT Director |  |
|  |  |
|  |  |

## Train Personnel

Personnel are informed by an {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)