***Identification and Authentication 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)

[Identification and Authentication Policies 1](#_1t3h5sf)

[Identification and Authentication ({ORG Abbreviated Name}anizational Users) 1](#_4d34og8)

[Device Authentication and Identification 1](#_2s8eyo1)

[Identifier Management 2](#_17dp8vu)

[Authenticator Management 2](#_3rdcrjn)

[Authenticator Feedback 3](#_26in1rg)

[Cryptographic Module Authentication 3](#_lnxbz9)

[Identification and Authentication (Non-{ORG Abbreviated Name}anizational Users) 3](#_35nkun2)

[Procedures 3](#_1ksv4uv)

[Resources 3](#_44sinio)

[Roles and Responsibilities 3](#_2jxsxqh)

[Train Personnel 4](#_z337ya)

[Follow Up 4](#_3j2qqm3)

[Compliance 4](#_1y810tw)

[Documentation Compliance Review 4](#_4i7ojhp)

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

[Acronyms/Definitions 4](#_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. Identification and authentication controls are in place to ensure that { ORG Abbreviated Name } information system grants access only through the use of proper credentials and that the credentials are only given to authorized personnel.

## 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 controls required to authenticate to the information system.

## Scope and Applicability

This policy applies to the information systems managed by { ORG Abbreviated Name } and personnel who access the information systems owned and maintained by { ORG Abbreviated Name }.

Exceptions

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

# Identification and Authentication Policies

## (IA-2) Identification and Authentication ({ORG Abbreviated Name} Users)

{{ORG Abbreviated Name}’s Technology Staff)} structures the information system so it uniquely identifies and authenticates {ORG Abbreviated Name} users or processes acting on behalf of {ORG Abbreviated Name} users.

##  (IA-3) Device Authentication and Identification

The information system uniquely identifies and authenticates {ORG Abbreviated Name} -defined specific and/or types of devices before establishing a {local or remote network} connection.

## (IA-4) Identifier Management

The {{ORG Abbreviated Name} Technology Staff } manages information system identifiers by

* For {ORG Abbreviated Name} personnel, {{ORG Abbreviated Name} Technology Staff} receives authorization from the Exec Director to assign {userid, physical key, access card, etc.} identifier.
* For clients, {{ORG Abbreviated Name} Technology Staff} receives authorization from Superintendent, Treasurer, or district designee to assign {userid, physical key, access card, etc.} identifier.
* {{ORG Abbreviated Name} Technology Staff}:
	+ selects an identifier that identifies personnel.
	+ {{ORG Abbreviated Name} Technology Staff} assigns the identifier to the intended personnel.
	+ {{ORG Abbreviated Name} Technology Staff} prevents reuse of identifiers
	+ {{ORG Abbreviated Name} Technology Staff} disables the identifier after:
		- Org staff 30 days,
		- School financial 90 days,
		- Teacher 180 days of inactivity.

## (IA-5) Authenticator Management

{{ORG Abbreviated Name Security Officer & IT Director manages information system authenticators by:

* Verifying, as part of the initial authenticator distribution, the identity of the specific personnel, group, role, or device receiving the authenticator.
* Establishing initial authenticator content for authenticators defined by {ORG Abbreviated Name}.
* Ensuring that authenticators have sufficient strength of mechanism for their intended use.
* Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
* Changing default content of authenticators prior to information system installation.
* Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators.
* Changing/refreshing authenticators every 182 days.
* Protecting authenticator content from unauthorized disclosure and modification.
* Requiring personnel to take, and having devices implement, specific security safeguards to protect authenticators.
* Changing authenticators for shared administrative or service group/role accounts when membership to those accounts changes.

The information system, for password-based authentication:

* Enforces minimum password complexity of {ORG Abbreviated Name} -defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type {8 char minimum with Upper, lower, special, and number}
* Enforces at least the following number of changed characters when new passwords are created:
	+ 4 for sensitive,
	+ 1 for non-sensitive
* Stores and transmits only encrypted representations of passwords.
* Enforces password minimum 1 day and maximum 182 days lifetime restrictions.
* Prohibits password reuse for 5 generations.
* Allows the use of a temporary password for system logons with an immediate change to a permanent password.

## (IA-6) Authenticator Feedback

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized personnel.

## (IA-7) Cryptographic Module Authentication

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

## (IA-8) Identification and Authentication (Non-{ORG Abbreviated Name} Users)

The information system uniquely identifies and authenticates non-{ORG Abbreviated Name} users, or processes acting on behalf of non-{ORG Abbreviated Name} users.

## (IA-9) Service Identification and Authentication

The organization identifies and authenticates [Assignment: organization-defined information system services] using [Assignment: organization-defined security safeguards].

## (IA-10) Adaptive Identification and Authentication

The organization requires that individuals accessing the information system employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].

## (IA-11) Re-Authentication

The organization requires users and devices to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].

# Procedures

## Resources

## Roles and Responsibilities

|  |  |
| --- | --- |
| Role | Responsibility |
| IT {ORG Abbreviated Name} staff | Validate compliance on a {Time Period} basis. |
| Security Officer | Provide policy during new hire process and informs personnel of changes. |
| IT Director |  |
| Executive Director |  |
|  |  |
|  |  |

## 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 |
|  |  |
| Personnel | Employees, contractors, consultants, temporary workers, and other workers. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# References

# Forms (If applicable)