Account and Credential Management Standard Template

Courtesy of

Nebraska Cybersecurity Network for Education

November 2024

Table of Contents

Account and Credential Management Standard Template

Purpose

Account and credential management is the process of creating, provisioning, using, and terminating accounts and credentials in the district. The Account and Credential Management Standard provides the processes and procedures for governing accounts and credentials.

Responsibility

- The Superintendent of ***<District Name>*** is responsible for the delegation of the responsibilities for managing the district's account and credential management functions. Those delegated are collectively known as the Information Technology team (IT). IT is responsible for informing all users of their responsibilities in the use of any accounts and credentials assigned to them.

Exceptions

Exceptions to this standard are likely to occur. Requests for exception must be made in writing and must contain:

- The reason for the request,
- Risk to the district of not following the written standard,
- Specific mitigations that will not be implemented,
- Technical and other difficulties, and
- Date of review.

Standard

Onboarding

1. IT must maintain procedures for modifying access, permissions, and roles to user accounts.
    a. Newly created accounts must be represented within this process.
    b. Changing user roles must be included in this process.
    c. The permissions granting process must enforce the principle of least privilege.
    d. Unnecessary default or generic accounts must be changed before a new system is deployed into the district.

Account Creation

1. IT must develop procedures for creating accounts and assigning privileges.
2. Administrator privileges must only be provided to administrative accounts.
    a. Administrator and privileged accounts must only be used for appropriate installation and maintenance tasks; not for daily use.
    b. Administrator accounts must be unique and assigned to a specific individual, unless technically constrained by a system or application.
3. It is the responsibility of IT to maintain an account inventory.
4. At a minimum the account inventory must contain the following data for each student account:
    a. Person's name
    b. Account name
    c. Date of enrollment start and stop
    d. Grade Level / Anticipated Graduation Year
5. Account status (i.e., enabled, disabled)
6. At a minimum the account inventory must contain the following data for each non-student account:
    a. Person's name
    b. Account name
    c. Date of employment start and stop
    d. Building / Department / Grade Level
    e. Account status (i.e., enabled, disabled)
7. All enabled accounts within the inventory must be regularly validated once a quarter, or more frequently

Credential Creation and Issuance

1. All passwords must be unique.
    a. Passwords created by users must not also be used for personal accounts.
    b. Passwords must not be shared by users.
2. Non-student passwords created for use with multi-factor authentication must be at a minimum 8 characters long.
3. Non-student passwords created for use without multi-factor authentication must be at a minimum 14 characters long.
4. Student passwords created for use on a network that is segmented such that access to non-student resources is restricted must be at a minimum 8 characters long.
5. Student passwords created for use on a network with unrestricted access to non-student resources must be at a minimum 14 characters.

Account and Credential Usage

1. All non-student users must use multi-factor authentication to access externally facing applications.
2. All non-student users must use multi-factor authentication to access applications hosted by a third-party service provider, where supported.
3. All remote users must use multifactor authentication to access internal systems and applications.
4. Multifactor authentication is required for all administrative accounts on all district assets, whether managed on-site or through a third-party provider.
5. All default user passwords must be changed at the first login.

Monitor

1. All account usage is subject to monitoring by IT, including, but not limited to:
    a. Login attempts, including successful and failed
    b. Password resets
    c. Multi-factor authentication attempts
    d. Privilege escalation
2. An acceptable threshold and criteria for abnormal behavior is defined, which includes, but is not limited to:
    a. Multiple failed logins
    b. Access from unusual locations

Modify Access

1. All user accounts that have not been accessed within 45 days of creation must be disabled.
2. Accounts of individuals on extended leave, as defined by human resources, must be disabled.
3. The Account Creation and Account Termination procedures must include the ability to change a user's role.

Account Termination

1. IT must develop procedures for revoking account access.
    a. Termination of employees must be included in this process.
2. All user credentials must be revoked immediately upon employee separation.
    a. Password self-service mechanisms for users must not allow them to re-enable their own account

Revision History

Each time this document is updated, this table should be updated.

Version	Revision Date	Revision Description	Name