Account and Credential Management Standard

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 IT business unit is responsible for all account and credential management functions. This information is relayed to other business units within the District such as student information systems, finance, human resources as required or needed. IT is responsible for informing all users of their responsibilities in the use of any accounts and credentials assigned to them.
- Users are responsible for using their accounts in a manner consistent with District policy.

Exceptions

Exceptions to this policy 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 policy,
- Specific mitigations that will not be implemented,
- Technical and other difficulties, and
- Date of review.

Policy

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 and maintain 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 account:
    a. Person's name

   b. Account name
   c. Date of employment start and stop
   d. Business unit
   e. Account status (i.e., enabled, disabled)
5. 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. Passwords created for use with multifactor authentication must be at a minimum 8 characters long.
3. Passwords created for use without multifactor authentication must be at a minimum 14 characters long.

Account and Credential Usage

1. All users must use multifactor authentication to access externally facing applications.
2. All users must use multifactor 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. There are no IG1 safeguards that support this portion of the account and credential management process.

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

Version	Revision Date	Revision Description	Name
v1.0	01/02/2023	Initial Written Standard	Scott Tisinger