INFORMATION TECHNOLOGY – ACCOUNT MANAGEMENT

Responsible: Office of Information Technology

PURPOSE

This Administrative Procedure shall establish the process for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at the Washoe County School District (District).

DEFINITIONS

1. "Administrative (Privileged) Accounts" refers to accounts that may have elevated privileges related to the management of a device, application, or system.
2. "Data Steward" refers to Chief Officers, Department heads, or school leaders that create, originate, and safeguard a particular class of data to perform District operations. Data stewards retain responsibility for safeguarding information but may appoint trusted designees to make decisions regarding access to data.
3. "Guest Accounts" refers to accounts created to facilitate work across collaboration with external entities or third parties that need temporary access to District resources. Guest accounts may be created for parents, community partners, vendors, or contractors.
4. "Provisioning" or "User Provisioning" refers to an identity management process that ensures user accounts are created, given proper permissions, changed, disabled, and deleted through an automated or manual process.
5. "Service Accounts" refers to an account explicitly created to provide a security context for services running on Information Systems which determines the service's ability to access local and network resources.
6. "Shared Accounts" refers to an account that can be accessed by multiple individuals to accomplish a single shared function, such as supporting the functionality of a process, system, device, or application. For example, a shared departmental email inbox or calendar. Shared accounts for departments may also be called "delegated accounts."

PROCEDURE

1. User accounts are a combination of a unique user identifier and one or more authenticators that grant individual user access to a computer, application, the District network, or any other information or technology resource. Accounts that access IT resources require prudent oversight to ensure the safety and security of the District's computing environment.
2. All persons or processes granted access to an information system, beyond those explicitly intended for unauthenticated public access such as the District Guest Wireless network, must be uniquely identified and authenticated before being

granted access to computing resources.

3. The Office of Information Technology provides an enterprise account (District ID) to support access to both centrally managed and distributed computing resources. District IDs are permanently assigned and can't be changed unless there is a major life change (i.e., marriage, divorce, legal name change, etc.).

4. Account Management activities including creation, maintenance, and deletion must be centralized with the central directory managed by the Office of Information Technology. District Information Systems must use enterprise directory services and avoid creating system-specific accounts and authentication or authorization systems whenever possible.

5. The Office of Information Technology manages and maintains an enterprise identity system including an inventory of all accounts managed in the enterprise. The inventory must include all user, administrator, service, and guest accounts. The inventory must contain the person's name, username, start/stop dates, and department.

6. District IDs and all other user accounts may not be used by anyone other than the individual to whom they have been assigned. All users are responsible for actions initiated from accounts issued to them and must not allow others to perform any activity with their accounts.

7. User accounts are maintained in accordance with the current version of the Nevada Local Government Records Retention Schedules.

8. Role-based Access Control (RBAC).

    a. The District uses RBAC to restrict network access based on a user's occupation, status, and functional responsibilities within the District. Roles refer to the levels of access that employees have to the network and information systems.

    b. All Information Systems must be configured to separate typical user and privileged user functionality through technological means whenever possible.

    c. General computing activities, such as internet browsing, email, and productivity suite use, must be performed from the user's primary, non-privileged account. This may be performed through the creation of an entirely separate account or through system controls.

    d. Users must be granted the minimum necessary rights or authorizations (least privilege) to perform their assigned duties and roles.

e. All users and accounts must only be permitted to access the information and systems necessary to effectively perform their job duties.

f. All accounts may be disabled, revoked, or deleted if account privileges are no longer used or required to perform an individual's function within the District, the account is potentially compromised or misused, or the user's need-to-know status changes.

9. Account Creation.

    a. Prior to creating a user account:

        i. An appropriate sponsor, typically Human Resources or the Student Registrar, must:

            1) Verify the identity of the user;

            2) Verify the user's affiliation with the District;

        ii. The user must:

            1) Read, understand, and sign the District Acceptable Use Policy;

            2) Read, understand, and sign applicable Data Disclosure Agreements; and

            3) Receive IT security skills training that is relevant and appropriate for their role in the District.

10. Account Provisioning.

    a. Access to data resources is managed through Data Stewards and their trusted designees based on the nature, sensitivity, and categorization of the information.

    b. The School or Department that operates an IT resource is generally responsible for requesting account provisioning, activation, and configuration to access resources by requesting services through the Office of Information Technology.

    c. Data stewards:

        i. Retain the responsibility for ensuring that all access to sensitive data is authorized, appropriate, and complies with relevant legal requirements;

ii. Must request services through the Office of Information Technology to promptly deactivate or revoke access privileges when user employment status changes or when there is no longer a legitimate need for access to continue. The accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location; and

iii. Perform comprehensive access reviews for their Information Resources semi-annually. The Data steward must ensure that access and account privileges are commensurate with job function, need-to-know, and employment status.

11. Account Security.

a. All account activity is monitored and audited.

b. Privileged accounts are subject to additional monitoring and safeguards, including mandatory Multi-Factor Authentication, to ensure that they are not used inappropriately.

c. All District IT Systems may be configured to allow for account lockouts after repeated failed login attempts whenever technically feasible. Accounts must be locked out for a minimum of five minutes unless a system administrator intercedes. Lockouts are logged and tracked.

d. Default or built-in accounts that are built into IT systems and software, such as "root", "administrator", and other pre-configured vendor accounts must have their default credentials changed and either be completely disabled or otherwise restricted from use.

e. Inactive, dormant, and unassociated accounts may be deleted or disabled after 45 days of inactivity.

f. Any suspicious activity, misuse, unauthorized access of a user account must be reported immediately to the Office of Information Technology.

12. Shared, Service, and Departmental Accounts.

a. Shared, Service, and Departmental accounts are not permitted under normal circumstances.

b. In some situations, an exception to support the functionality of a process, system, device (such as servers, switches, or routers), or an application may be approved by the Chief Information Officer or designee. Exceptions require a documented justification and approval in writing.

c. Shared, Service, and Departmental accounts must be configured to provide the least privilege necessary to perform their functions.

d. Each shared account must have a designated owner (Account Owner) who is responsible for the management, maintenance, and actions of the account.

e. The Account Owner is responsible for documenting all individuals with access to the shared account and shared secrets that control access to the account. Credentials to shared, service, and departmental accounts must be changed regularly, and upon personnel change or departure.

f. Shared, Service, and Departmental accounts must have auditable procedures in place to ensure proper control in the event of an account compromise.

13. Guest and Vendor Access.

a. Guest and Vendor accounts may be requested for users who are not regular employees or members of the District community but require a District account.

b. Guest and vendor accounts must be uniquely identifiable and comply with all existing District policies regarding account management, registration, and access control.

c. All guest accounts with access to computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first.

d. External vendor access activity must be monitored and audited.

e. Access to all vendor-maintained equipment on the District network must restricted through District proxy, Virtual Private Network, or firewalls.

LEGAL REQUIREMENTS AND ASSOCIATED DOCUMENTS

1. This Administrative Procedure reflects the goals of the District's Strategic Plan and aligns/complies with the governing documents of the District.

2. This Administrative Procedure aligns with Nevada Revised Statutes (NRS) and Nevada Administrative Code (NAC) to include:

a. Family Educational Right to Privacy Act (FERPA); and

b. Health Insurance Portability and Accountability Act (HIPAA).

REVISION HISTORY

Date	Revision	Modification
09/23/2015	1.0	Adopted
10/27/2022	2.0	Revised: Update and clarify process