Responsible: Office of Information Technology

PURPOSE

This Administrative Procedure shall establish the process to create, manage, and secure privileged or administrative access accounts within Washoe County School District (District).

DEFINITIONS

1. "Authentication" refers to the process or action of verifying the identity of a user or process.
2. "Hardware Token" refers to a physical (i.e., hardware) security key used to protect access to computers, networks, and online services. Hardware tokens support multiple security technologies including One-Time Passwords (OTP), public key cryptography, and authentication.
3. "Multi-Factor Authentication" refers to an authentication method that requires the user to provide two or more verification factors to gain access to a resource.
4. "One-Time Password", or (OTP) refers to an automatically generated alphanumeric string of characters that authenticates a user for a single transaction or login session. OTPs may be generated by hardware or software tokens.
5. "Privileged access" or "Administrative access" refers to elevated permissions that enable an individual to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users.

PROCEDURE

1. The District provides access to information resources for business purposes in serving the interest of the District in normal operations. All users of District information systems must know their responsibility to know these guidelines and conduct their activities accordingly.
2. Inappropriate use of Information Resources exposes the District to risks including degradation of the confidentiality, integrity, and availability of District information systems and services.
3. This Administrative Procedure applies to all users of District personnel including students, employees, contractors, consultants, and users affiliated with third parties accessing the District network. This procedure applies to all equipment

that is owned or leased by the District, or any device accessing the District's network.

4. Privileged access is only granted to system and network administrators, employees performing computing account administration, or other such users whose duties and responsibilities require special privileges over a computing system or network.

5. Individuals with privileged access must comply with applicable policies, laws, regulations, precedents, and procedures while pursuing appropriate actions required to provide high-quality, timely, reliable, computing services.

6. Privileged access must only be used to perform assigned job duties or responsibilities.

7. If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other resources required clearly justifies using privileged access.

8. Privileged access may be used to perform standard system-related duties only on machines and networks whose responsibility is a part of assigned job duties. Examples include:

    a. Installing system software;

    b. Relocating individuals' files from critically overloaded locations;

    c. Performing repairs required to return a system to normal function, such as fixing files or file processes, or killing runaway processes;

    d. Running system diagnostic programs;

    e. Performing coursework directly related to Career and Technical Education programs within specific technical environments or labs; and

    f. Monitoring system to ensure reliability and security.

9. Privileged access must be restricted to dedicated administrator accounts that provide individual attribution on enterprise assets. Privileged user accounts must not be shared between users.

10. General computing activities such as internet browsing, email, and productivity suite user must be performed from the user's primary, standard user account.

11. Privileged Account Management.

a. Privileged Account management activities including creation, maintenance, and deletion must be centralized with the directory services 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.

b. Privileged account management activities must be associated with an Information Technology (IT) Service Request.

c. Prior to creating a privileged user account:

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

        1) The identity of the user;

        2) The user's affiliation with the District; and

        3) The operational need or justification for privileged access.

d. The user must:

    i. Read, understand, and sign:

        1) District Acceptable Use Policy;

        2) District Privileged Access Acceptable Use Procedure; and

        3) Any applicable Data Disclosure Agreements.

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

e. Privileged User Transfer or Departure.

    i. Privileged Access must be promptly deactivated or revoked when user employment status changes or when there is no longer a legitimate need to maintain privileged access.

    ii. Users with privileged accounts must return their hardware tokens to the Office of Information Technology:

        1) Upon request by the Office of Information Technology;

2) When their duties no longer require them to maintain a privileged account; or

3) Their affiliation with the District is terminated.

iii. Departing users may not transfer hardware tokens to other users directly. Hardware tokens must be received and reprovisioned by the IT Security Department as necessary.

iv. If an employee maintains an affiliation in the District and is simply changing roles or departments to one that does not require privileged access, the departing program should request data transfer to enable shared access by others as necessary.

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

12. Security of Privileged User Accounts.

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

b. The District has the right to review all account activity and material stored on District information systems.

c. Privileged accounts, systems, and networks may be disabled or disconnected from District computing resources when suspected of misuse, performing prohibited activities, or unauthorized access. Examples of prohibited activities include:

i. Performing illegal activities under local, state, or international laws;

ii. Bypassing authentication mechanisms or security boundaries and configurations;

iii. Subverting internet filters or controls to access forbidden content;

iv. Introducing malicious, unauthorized, inappropriately licensed, or unlicensed software into the computing environment including those that infringe upon third-party intellectual property rights;

v. Transmitting, storing, or deliberately accessing obscene, abusive, or otherwise offensive, objectionable, or unlawful information on the network;

vi. Improperly transferring or sharing of accounts;

vii. Misappropriation or misuse of information or files of other users;

viii. Spoofing the origin of activities;

ix. Using software to mount attacks on other hosts;

x. Using computing resources to conduct personal business, including outside business, publicize non-educational fund-raising opportunities, commercial advertisement, or misrepresentation;

xi. Performing unauthorized security scanning or monitoring activities including network "sniffing"; or

xii. Engaging in any activities designed to disrupt or degrade the confidentiality, integrity, or availability of information systems.

d. The District is the sole arbiter of what constitutes abusive conduct or violation of District policies.

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

13. Multi-Factor Authentication.

a. Multi-Factor Authentication is required for all administrative account access, where supported, whether managed on-site or through a third-party provider.

b. Where supported, privileged users must use approved hardware tokens (fob) as a second factor security during authentication in addition to their District account credentials. Software tokens may be used when approved by the IT Security Department.

c. Only approved and registered hardware tokens may be used as a second factor authenticator or for OTP generation.

d. Users must not use District-provided hardware tokens for personal services or accounts.

e. Users must take reasonable care of their assigned hardware token. Reasonable care includes, but is not limited to:

i. Physically securing them against loss or theft in District and public facilities;

ii. Never sharing them with another user;

iii. Protecting them from physical damage including water or moisture;

iv. Inventorying the devices and confirming possession monthly;

v. Disconnecting and storing devices separate from associated information systems; and

vi. Refrain from marking their hardware fobs or smartphones with any identifying information such as their name, associated accounts, password, or any reference to District Information Systems.

f. Lost, stolen, or damaged devices must be reported immediately to the IT Security Department (security@washoeschools.net).

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, to include:

   a. Board Policy 7205, Information Technology – Data Access Policy; and

   b. Board Policy 7210, Information Technology Services and Operations.

REVISION HISTORY

Date	Revision	Modification
10/27/2022	1.0	Adopted