Title:	Privileged Account Use Procedure

Division:	Business and Finance	**Department:**	Information Technology
Procedure Contact:	Chief Information Officer		
Date Posted:	1/7/2025		
Related Policies or Procedures:	Password Complexity and Expiration Requirements Workstation Permissions Procedure		

History

Revision Number:	Change:	Date:
1.0	Initial version	1/7/2025

A. Purpose

The purpose of this procedure is to establish and communicate clear guidelines for the appropriate, secure, and compliant use of privileged accounts. This procedure ensures that these accounts are used in a controlled manner, protecting the integrity, confidentiality, and availability of university resources, while minimizing the risk of unauthorized access, data breaches, and system misconfigurations.

Privileged access allows individuals to perform actions that can affect computing systems, network communications, or the accounts, files, data, and processes of other users. This level of access is usually granted to system administrators, network administrators, account management personnel, or other employees whose roles necessitate special permissions over a system or network. Privileged access may also provide these users with technical capabilities that exceed their regular access rights, such as the ability to elevate their functional access privileges.

B. Definitions

Privileged Account: A user account that provides elevated access permissions, typically allowing administrative, root, or superuser-level access to systems, applications, databases, or networks. These accounts are capable of making critical changes to configurations, managing system resources, and accessing sensitive data.

Least Privilege: A security principle that limits access rights to the minimum level necessary for users to perform their job functions, ensuring that users are granted only the privileges required to complete their tasks.

Two-Factor Authentication (2FA): An authentication method that requires the use of two or more verification factors—such as a password, fingerprint, or token—to gain access to a system or application, increasing the security of privileged account access.

C. Procedure

1. Individuals with privileged access must use their access responsibly, adhering to the boundaries of their designated privileges and respecting the rights of other system users. They are expected to maintain the integrity of systems and related physical resources. Protecting the privacy of information is a critical aspect of system administration at EWU. Those with privileged access must follow all applicable policies, laws, regulations, and procedures, while ensuring that their actions contribute to the delivery of high-quality, reliable, and timely technology services.

2. Requirements:
    - Privileged access is granted only to authorized individuals.
    - Individuals may request privileged access from the System or Application Owner. Each Owner is responsible for reviewing, approving, provisioning, and deprovisioning of administrative access to systems and applications. The provisioning process must include proper separation of duties and follow the principles of least privilege. Users who no longer require administrative access, changed roles, or have departed the institution must have their credentials promptly revoked.
    - Users with privileged access must inform the System or Application Owner when they no longer require those privileges.
    - Users with privileged access will have two user IDs in situations where providing access to their standard user id will create unacceptable risk: one for normal day-to-day activities and one for performing administrative duties.
    - Every privileged account must have its own unique password when provisioned as a dedicated administrative account. Passwords should be configured using the guidance from the Password Complexity and Expiration Requirements procedure.
    - Two-factor authentication (2FA) must be enabled, whenever possible, for all privileged accounts to enhance security.
    - Administrators may only use their administrator account to perform administrative functions and should not be used for day-to-day activities such as web browsing or reading email.
    - Administrators may not use their privileged access for unauthorized viewing, modification, copying, or destruction of system or user data.
    - Users with privileged access have a responsibility to protect the confidentiality of any information they encounter while performing their duties.
    - Users with privileged access are responsible for complying with all applicable laws, regulations, policies, and procedures.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.