THE UNIVERSITY OF TENNESSEE HEALTH SCIENCE CENTER

UT Health Science Center: AC-001.02-Privileged Account Management	
Version 3	**Effective Date: 09/30/2017**

Responsible Office: Office of Cybersecurity	Last Review: 09/29/2022 Next Review: 09/29/2024
Contact: Chris Madeksho	Phone: 901.448.1579 Email: mmadeksh@uthsc.edu

Purpose

The purpose of this Practice is to define roles and expectations of Privileged Accounts affording elevated user rights on systems and applications. Specifically, these rights can bypass, modify, or disable technical or operational security controls. Examples may include the ability to install software; install or modify system processes; create or modify system configurations; create or modify system access controls; view or control the screen of the user through remote access technologies in order to assist users. This standard is also designed to meet compliance requirements for data regulated by federal or state law. This includes, but is not limited to, security requirements and safeguards for the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), or Gramm-Leach-Bliley Act (GLBA).

Scope

This practice applies to all individuals who have been granted access to Privileged Accounts with elevated access to any UTHSC system or application where the account has been afforded rights beyond that of a typical user.

Definitions

Privileged Account – An account which, by virtue of function, and /or security access, has been granted special privileges within the computer system, which are significantly greater than those available to the majority of users, including but limited to, local administrative accounts, privileged user accounts, domain administrative accounts, emergency accounts, service accounts, and application accounts.

Security Categorization - The process of determining the security category for data or an information system. Security categorization methodologies are described in Federal Information Processing Standard (FIPS 199) and National Institute for Standards and Technology (NIST) SP 800-60. The security categorization helps identify the appropriate level of controls to be applied to the system or data.

System or Application Owner/Custodian - Person or organization having responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system

Responsibilities

System/Application Owner: authorize, review and reverify privileged access accounts, creating separate credentials for that account, separate from a normal user account.
System/Application Custodian: create separate, unique credentials for the privilege account.
Individual with privilege access: comply with all guidance in this practice.
Chief Information Security Officer (CISO): governance, oversight, and monitoring of the Privileged Account Management process

Practice

1. Privileged access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff performing computing account administration, or other such employees whose job duties require special privileges over a computing system or network. Privileged access might provide such users with technical access capabilities that are beyond their functional access authority such as upgrade their functional access authority.

2. Individuals with privileged access must not abuse their access capability and strictly respect their functional access authority limits, respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Individuals also have an obligation to familiarize themselves regarding any procedures, business practices, and operational guidelines pertaining to the activities of their local department. In particular, the privacy of information holds important implications for computer system administration at UTHSC. Individuals with privileged access must comply with applicable policies, laws, regulations, precedents, and

procedures, while pursuing appropriate actions to provide high-quality, timely, reliable, computing services.

3. The CISO will maintain the responsibilities of governance, oversight, and monitoring of the Privileged Account Management process

4. Requirements:
    a. Privileged access shall only be granted to authorized individuals.
    b. Individuals may request privileged access from the System or Application Owner. Each Owner must establish a standard process for review, approval, and provisioning of administrative access to systems and applications. This process must include proper segregation of duties and provide the CISO with the ability to monitor compliance with the established information security policies and processes.
    c. 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.
    d. Every privileged account must have its own unique password when provisioned as a dedicated administrative account. Passwords should be configured using the guidance from AC-002.02-Password Management and Complexity.
    e. 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.
    f. Administrators may not use their privileged access for unauthorized viewing, modification, copying, or destruction of system or user data.
    g. Users with privileged access have a responsibility to protect the confidentiality of any information they encounter while performing their duties. Never disclose confidential or sensitive information about the UTHSC or the University of Tennessee and its students, staff, faculty or alumni. Types of data with a classification rating of 3 in any area include but not limited to Protected Health Information (PHI), Personal Identifiable Information (PII), FERPA-protected student information, Social Security numbers, credit card numbers and medical records. Comply with the guidance set forth in GP-002-Data & System Classification.

h. Users with privileged access are responsible for complying with all applicable laws, regulations, policies, and procedures.
i. As a representative of the UTHSC and the University of Tennessee, it is imperative to maintain the same standards of conduct expected of all employees as per UTSA policy HR0580-Code of Conduct.
j. Users with privileged access will be required to take an assigned Information Security Training course specially for this type of access.

5. Non-Compliance and Sanctions
    a. Failure to comply with these standards may result in a loss of access or other disciplinary actions, up to and including termination.

References

1. AC-001-Access Control
2. AC-002-Authentication
3. IR-001-Security Incident Response
4. GP-002-Data & System Classification
5. AC-002.02-Password Management and Complexity
6. UTSA policy HR0580-Code of Conduct