Information Security Standard 9.2a

PRIVILEGED ACCOUNT STANDARD

Initially Approved: August 20, 2013 (as the Generic Systems Account Policy)
Revised: September 8, 2016 (as the Privileged Account Policy)
Revised: March 30, 2020 (as the Privileged Account Standard)
Standard Topic: Information Technology Security
Administering Office: Office of the CIO

I. STANDARD STATEMENT

This standard, operating under University Policy 117 Information Security, defines and establishes governance for the creation, usage and maintenance of privileged accounts used for the administration of Western Carolina University's systems.

When elevated privileges are required to perform administrative tasks on a system then staff must utilize a different account than their standard user account. Privileged accounts must be created and maintained for this purpose. These accounts must be limited in the scope of their use as much as possible and the authentication credentials must be unknown and hidden from the user as much as possible.

II. SCOPE AND APPLICATION OF THE STANDARD

This standard applies to accounts with elevated privileges that are used to administer systems owned or operated by the University. It applies to staff that manage and maintain these systems.

Student workers that need a privileged account must also have an Administrative Student Worker account which can be associated with their privileged account.

This standard does not apply to local administrator accounts for systems or devices owned or operated by individuals which are not publicly accessible (i.e. webservers).

III. DEFINITIONS

A System Account is a non-person account required to administer systems, applications, network devices, etc.

A Service Account is a non-person account required for system-to-system access of information assets; i.e. many database products, system and network monitoring tools require such accounts. These accounts are often used as proxies to provide information or services to person accounts.

A Local Account is an account created and maintained on a system or device that is not part of WCU's Active Directory (AD). Examples of this are local administrative accounts for a system, database, or network devices.

A Privileged Account is an account with elevated permission required to administer systems, applications, network devices, etc. The permissions may be granted explicitly to the account or be inherited through group memberships. The account may be a personal account, a generic system or service account or a local administrator account.

A Standard User Account is an account used by an individual for everyday work which includes reading Email and browsing the Internet. Generally, this account does not require elevated permissions and must not be used to administer systems and applications.

Privileged Account Management System (PAM) is the system adopted by the IT Division to manage privileged accounts for all systems and staff to the fullest extent possible. Among other things, this system will be capable of changing account passwords, connecting to systems using these accounts without the password being known to the user and logging usage of these accounts.

IV. PRIVILEGED ACCOUNT STANDARD

1. Accounts for privileged access to applications

    a. Use of a privileged utility program that does not require administrative access to the operating system level controls should be done with an account that is not a standard user account.

    b. This type of account may or may not be managed by the PAM.

    c. If the application contains sensitive data according to WCU's Data Handling Procedures, then privileged access to the application must be done via multi-factor authentication if possible.

2. Accounts for privileged access to operating systems and system consoles

    a. Privileged accounts will be assigned the least privileges required to do the job they are intended for, i.e. a lower tier AD Admin instead of a Domain Admin.

    b. A privileged account will be limited in scope as much as possible to a single user, a single system or a single service.

    c. Service accounts are not to be used by staff to log into a system to perform work. Personal AD accounts are not to be used as service accounts.

d. Whenever possible, a privileged account will be a campus authenticated directory level account (AD). If a local account is required, for purposes of documentation and accountability, local accounts will be created using WCU's account naming conventions and used for maintaining systems. Whenever possible the local default administrator account will not be used except for emergencies.

e. This type of account must be managed by the PAM to the fullest extent possible. Where the PAM cannot fully manage the account the PAM must be used to store the current password for the account.

3. Privileged accounts as defined by this standard must not be used at public access computers such as kiosks or lab computers.

4. Privileged accounts must adhere to the password standard as it applies to system-level accounts and must be periodically reviewed by the staff that manage and maintain the systems to assess their continued value.

5. Privileged accounts are requested using the Generic Account Request form accessed via myWCU. The account sponsor is responsible for ensuring that all necessary training has been provided and is responsible for all activities that are done using this account.

V. REVIEW

Exceptions to this standard must be reviewed and approved on a case-by-case basis by the Office of the CIO.

This standard will be reviewed periodically and updated as necessary.

VI. REFERENCES

International Standards Organization (ISO/IEC 27002, 9.2, User Access Management)

University Policy 117 Information Security

IT 9.3a Password Standard

Data Handling Procedures Related to the Data Security and Stewardship Policy