UNIVERSITY of WISCONSIN
UWMILWAUKEE

Shared Account & Service Account Guidance

Introduction

Per UW System Authentication Procedure 1030.A:

"Individuals with access to moderate and high risk data shall not use a shared account. If, due to system limitation or problems, the shared account must be used, the institution shall establish procedures for documenting, approving, and monitoring the use of the shared account."

(https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/information-security-authentication/)

This document provides guidance for UWM IT professionals on the appropriate use of **shared** and **service** accounts. The use of **shared** and **service** accounts is governed by UW System Administration policy and the compensating controls for which UWM has received approval.

Definitions & Standards

For purposes of this document a **shared** account is an account that is used by multiple individuals to access systems or data. A **service** account is an account that is used by an automated process and is not used in an interactive way by a user. A single account and password that is given to students to log into a scientific instrument is a **shared** account. An account that is used by a vulnerability scanner to log into remote machines is a **service** account**.**

Necessary Shared Accounts

There are situations where **shared** accounts are sometimes necessary to provide limited service to individuals without affiliation with the institution or to share in the execution of legacy services. Examples include **shared** accounts that are used to access:

- WiFi
- Classrooms
- Computer Labs
- Additional shared applications that require profile specific settings

Please note: It is understood that interactive log-on sessions are a requirement of **shared** accounts but any further authorization to medium and high-risk data is strictly prohibited.

In cases where a **shared** account is needed, the password must be stored in a password vault with auditing capabilities. In addition, the password:

- will have a 12 character minimum
- will meet the standards for complexity requirements (upper case, lower case, numbers, symbols)
- will have a password lifespan of no more than 180 days

Please note: Shared accounts are *ONLY* to be used where there is no viable alternative.

Service Accounts

Service accounts are necessary for some applications, task execution, database services, job processing, etc. **Service** accounts are not used in an interactive manner, are able to have additional authentication restrictions set, and are not susceptible to the same account compromise risks as regular user accounts.

In cases of **service** account**s**, the password must be kept in a password vault with auditing capabilities. Additionally, the following requirements must be met:

- Character length: 16-32 (highest supported character length of application)
- Complexity requirements (upper case, lower case, numbers, symbols)
- Password lifespan: lesser of 3 years or upon any password holder's departure

Getting Assistance

If you believe you have a case that calls for a shared account or a service account, please contact the UWM Help Desk https://uwm.edu/technology/help/ for assistance. The issue will be escalated to the appropriate parties.