University of Wisconsin Whitewater

Information Security Shared User Accounts Procedure

Intent:

This procedure is intended to outline appropriate guidelines for the request, use and management of shared user accounts at UW-Whitewater.

Scope:

This procedure applies to:

- **user account management practices** for interactive user accounts in which multiple individuals have knowledge of the credential, and use the account for authentication and access to resources.
- **new shared user accounts** which are created and managed by UW-Whitewater and for shared user accounts which are provisioned to UW-Whitewater employees by third-party services. This procedure does NOT apply to system or service accounts.
- **all existing shared user accounts**, including shared user accounts created prior to the issuance of this directive. Any department with an existing shared user account created prior to the issuance of this directive must complete the request, approval, and periodic review process as described below for the shared account to remain active. Unapproved shared user accounts will be disabled.

Definitions:

Help Desk: For the intents and purposes of this procedure, "Help Desk" refers to the UW-W iCIT Service Center.

Role: A group of permissions assigned to a user's account which are used to provide access to resources.

Shared User Account: A single interactive account that is available for use by multiple individuals to allow them to appear as a single business entity or accomplish a single shared function. These individuals share knowledge, management and responsibility of the account credentials. Activity performed by the account would not be associated with a specific individual, rather the activity performed by the account would appear as a single business entity. As the credentials are known to multiple individuals, the risk to the confidentiality, integrity and availability of the account, the account credentials and the resources to which the account has been authorized to access is increased. Due to the increased risk, the use of a shared user account is strongly discouraged. Justification and use of a shared account must be documented, approved, and periodically reviewed.

System or Service Account: An account which is used to authenticate an automated process or service, or used when establishing connections between web, application, and database servers, or external applications or services. This type of account is not used for individual interactive logins by users.

User Account: Unique identifier assigned to an individual for purposes of granting access to information or resources. User accounts and their associated credentials are under the control of a specific individual and are not accessible to others. The primary user accounts are the UW-Whitewater assigned user

accounts, commonly referred to as the user's "NetID", which are managed centrally by the UW-Whitewater credential and authentication system and used campus wide. In addition to the primary user account, there are two (2) other types of named accounts which may be provisioned to users:

- **Local user accounts** are additional user accounts assigned to an individual that are typically managed within a specific application or service and may use an external vendor's credential authentication system. Management of local user accounts are typically manual, and performed by authorized staff managing that specific system or application.
- **Privileged accounts** are user accounts which are provisioned to a user in addition to their standard user account, and used to perform tasks which require elevated access to configure or significantly change the behavior of a computing system, device, application or other aspect of the Information Technology (IT) resource or IT infrastructure.

Table of Contents

Procedure

The use of a shared user account is highly discouraged due to increased risk associated with confidentiality, integrity, and visibility. Shared accounts result in limited accountability and traceability to the individual(s) responsible if incidents of misuse occur. If a department feels a shared user account is required to conduct university business, the department must submit appropriate justification when requesting creation of the account, and when periodic review of the account activity is requested.

Access to Shared Resources:

At the time a user account is created and provisioned to an individual user, the initial role and associated permissions commensurate with scope of responsibilities of this individual are granted. It is the responsibility of the individual user to maintain the account credentials and not disclose the credentials. All activity performed by the account is associated with the single account holder. It is common that a workgroup or multiple individuals need access to shared resources, such as a shared folder, data storage, or departmental email. Current authentication and authorization systems can accomplish this by providing individual user accounts access to the shared resources without the need to create a shared user account. When multiple individuals require access to a shared resource, authorization can be provided to each individual user account, allowing for improved flexibility in managing access, and improving the confidentiality, integrity and availability of the resources. This method provides each individual account with the appropriate access, while eliminating the need for account credentials to be shared between multiple individuals. The approach is to provide access for multiple authorized individual user accounts to a shared resource rather than sharing a user account between multiple individuals to access a resource.

Shared User Account Risks

Due to the increased risk associated with shared user accounts, only Low Risk data should be authorized for access by shared accounts unless appropriate approved mitigating controls have been reviewed and implemented.

- **Compromised Account Access:** When credentials for a user account are shared, the activity cannot be associated to the single individual, as more than one individual have access to the user account. The method for sharing the user account credentials puts the account at higher risk of being compromised, such as in the scenario in which the password is changed and then must be communicated between the individuals sharing the user account. There is increased risk that individuals other than those who have the need to know the credential may become aware of the shared credential.
- **User Account Activity Tracking:** There is also increased risk to the confidentiality, integrity and availability of the resources that can be accessed by the shared user account, as unauthorized use of the account to access the data is more difficult to detect. Many of the methods to detect suspicious activity from unauthorized use of a user account, such as having the account log in from multiple physical locations, are not effective.

Requesting Shared Accounts:

To request a Shared account, the department must submit a request via the Help Desk. Justification for the shared account must be provided by the department responsible for the use, management and activity of the account, and must include the following:

1. Account name
2. Department which will be responsible for the use of the shared account and management of the account credentials
3. Intended use of the account
4. System or vendor provisioning the user account, such as UW-Whitewater or the name of the third-party/vendor for hosted services.
5. Resources to which the shared account requires access
6. Business justification for not using individual user accounts
7. Business process and procedure for managing the credential, including but not limited to:
    a. Method of identifying individuals who will share the account
    b. Method to securely communicate credentials

c. Process for resetting the account credentials when an individual no longer needs access to the account
d. Recording and monitoring account access and activity
e. Identifying inappropriate and/or unauthorized use of the credential
f. Method for identifying and reported a compromise to the credential.

8. Primary and secondary contact responsible for the appropriate use of the account.
9. List of individuals with access to the account, including effective date

The request will be reviewed by ICIT to evaluate and assist the department in developing alternative options where appropriate. If no alternative individual user authentication options are available, and it is determined the use of a shared user account is justified, the request will be approved and the department will be notified of the process to activate the shared user account and assign the credentials.

Review and Continued Use of Shared Accounts

Continued Use

Shared user accounts must only remain active while there is a valid business justification for having the shared user account. Review and justification for shared user accounts will occur for any of the following conditions:

- At least once every 180 days, or once a semester
- When the primary or secondary shared account contact change
- When the list of individuals with access to the account credentials change
- When the list of authorized resources change, such as requesting access to additional resources or removing access to existing resources.

Failure to comply with the review and justification of the shared account will result in the account being disabled.

Disabling the Account

When a Shared user account is no longer required, the department contact will file a request to the Help Desk for deactivation of the shared user account, providing the account name, date of removal, and approval for removal from the department which requested and is responsible for the use of the shared user account.

Resources:

Information Security Account Lifecycle Practice Directive and Procedure

---

Administration:

Approval Details

Approval Authority:	UW System: UW System Administrative Policy 1030: Information Security: Authentication , UW System Administrative Procedure 1030.A: Information Security: Authentication Regent: Regent Policy 25-5: Information Technology: Information Security State: State Statute Subchapter 8: Information Technology Federal: U.S. Department of Commerce: Security and Privacy Controls for Federal Information Systems and Organizations
Approval date:	11/02/2020

Version no:	V1.0
Date for next review:	11/02/2022

Revision History

Version	Revision date	Description of changes	Author
1.0	11/02/2020	Procedure established	Quality Assurance Improvement Manager

Contact Person/Unit

Contact Person/Unit:	Chief Information Technology Officer

Keywords

Keywords:	Information Security, Information Technology, NetID, Shared user account, Credential, User account, Access, IT Access.