University of Wisconsin Whitewater

Information Security Account Lifecycle – Change of Role and Separation Procedure

Intent

The University of Wisconsin-Whitewater is committed to supporting information security user account lifecycle best practices and compliance with UW System Policies, Regent Policies, State Statutes, and Federal Statutes. This procedure is intended to ensure that employee access to information technology resources and data is reviewed, and that appropriate level of access is granted upon the change of employee's role at (or affiliation with) UW-Whitewater.

Scope

This procedure applies to all individuals (i.e. employees, consultants) and entities (i.e. vendors) who have been provided a user account to access, or grant access to, the campus' information systems and data.

Definitions

Administrator: For the intents and purposes of this procedure, "Administrator" refers to the UW-W project or unit Supervisor, Manager, Division Head, Dean, Department Head, or designee etc. who has been granted the necessary delegated authority to request, approve, or revoke access to University systems, data, records, or other information that requires a user account and/or MFA. Administrators work in collaboration with iCIT to ensure appropriate oversight and management of user account access.

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

User Account: Unique identifier assigned to an individual for purposes of granting access to information or resources. User accounts 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. Examples may include, but are not limited to: Peachtree Departmental billing, Metasys system that controls thermostats on campus, or Digital Signage system.
- **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.

Shared Account: An account that can be accessed by multiple individuals to allow them to appear as a single business entity or accomplish a single shared function. As the credentials are known to multiple

individuals, the use of a shared account is strongly discouraged. Justification and use of a shared account must be documented, approved, and periodically reviewed.

Multi-Factor Authentication (MFA): Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction, the University of Wisconsin-Whitewater has a multi-factor authentication form for access.

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

Table of Contents

Procedure

UW-Whitewater user accounts are created to enable business operations of the university (I.e. education, research, service, and administrative functions), whether these accounts are centrally assigned and managed by the iCIT account provisioning and authentication system, or departmentally managed such as local accounts used to access specific, non-enterprise applications and systems. This procedure also applies to user accounts that are hosted locally in the UW-Whitewater Data Center or hosted and managed by external vendors. The guidelines described in this procedure address exercising proper user account management practices across different scenarios, including:

- When account holders' transition to a different role at UW-Whitewater, and
- When account holders change the nature of their relationship with UW-Whitewater (I.e. separation, retirement, etc.).

Condition	Process
Scenario 1: User Account Changes Individuals, including affiliates, have a change in job responsibilities and therefore require access to different resources.	The Administrator will complete the appropriate steps outlined in the iCIT Supervisor Off-Boarding Procedure and ensure that appropriate offices (such as Dean, Department Head, or designee) Human Resources and Diversity, ICIT and Registrar's office have been notified of the employee's change in status, and that appropriate user account access has been removed, data preservation requirements have been fulfilled, and institutional assets have been returned. This process must start immediately upon being notified of the employee's intent to leave the current position. These steps include: 1. Access Management: **Calendar management.** The Administrator will identify all shared accounts and rights used by the employee to manage calendars, and must assure that the duties were transferred to another employee upon removal of the former employee's access.

Local user accounts and privileged accounts. The Administrator will identify all locally-managed privileged accounts, as well as other local accounts, that were used by the employee, and will assure the duties were transferred to another employee in the department upon removal of the former employee's access.

2. Data Preservation:
   The Administrator will identify all systems and applications (i.e. Google Docs, OneDrive, Qualtrics, etc.) where an employee could have stored institutional or departmental data under their user account, and request the employee transfer the data to enable access by others.

3. Assets:
   The Administrator will collect all portable IT assets (laptop, tablet, phone, MFA fob), confirm the location of stationary IT assets (desktop computers, printers), and notify the Help Desk accordingly to confirm that appropriate access has been removed, data preservation requirements have been fulfilled, and institutional assets have been returned.

4. Check Out Form:
   The Administrator will complete the iCIT Employee Check Out Form.

5. Removal of Account Access:
   Upon completion of the aforementioned steps, ICIT will proceed with removing the following access and accounts on the employee's last day of the current job:
   - Access to High Risk Data (such as social security numbers)
   - Shared Email (Full Access/Send-as)
   - Shared Document Storage Folders (such as T:drive)
   - Email Distribution Lists
   - Blogs and Spaces
   - CMS (Ingeniux) and Master Calendar
   - Campus Web Applications Access (such as HR Change of Status, FP&M Key Requests)
   - Privileged account access to other systems and applications that use university-level authorization
   - Local account access

6. Access provisioning for the employee's new role:
   If the individual is maintaining affiliation with UW-Whitewater, and is simply changing roles or departments, etc. the Administrator for the new role will submit the access request

	form which indicates the new level of access requested. The Help Desk will grant or remove the individual's access to resources as well as to the individual's data to the Administrator as specified. Once the access requests are completed, the Help Desk will notify the individual and the Administrator.
Scenario 2: Separation for Cause Individuals, including affiliates, are terminated.	1. At the time of separation, Human Resources & Diversity (HR&D) will notify the appropriate departmental contact person as well as the appropriate ICIT contact person, to immediately disable all accounts assigned to the individual. • Note: The Administrator must also change password(s) to any shared accounts the individual had access to. The Administrator may also request access to the employee's G: Drive and email folders, with approval from Human Resources & Diversity. 2. The ICIT Help Desk will proceed with disabling the account(s) and removing access to resources. 3. The Administrator will also follow other Access Management, Data Preservation, and Assets requirements as outlined in Scenario 1.
Scenario 3: Separation in a good standing Individuals, including affiliates, who leave employment or affiliation in good standing.	On or prior to the individual's termination date, the Administrator will contact the ICIT Help Desk requesting all account(s) assigned to the individual be disabled as outlined in Scenario 1. At which point iCIT will disable the individual's UW-Whitewater assigned user account and remove access to the managed resources in accordance with UWSA procedure.

Continued Access for Affiliates

Accounts must only remain active while there is a valid business justification for having the account, however, there may be times where accounts need to remain active past their normal defined periods. Individuals who leave employment in good standing and retain a documented affiliation with the university (emeriti, sponsorship, retiree/annuitant, adjunct faculty, instructional staff/faculty, etc.) may retain account access provided the stipulated conditions are met. The following chart provides guidance concerning how to enforce appropriate access for individuals whose accounts remain active. Note: The workflow described in the "Account Lifecycle" are used for managing role changes and account deactivation processes for any accounts which are approved for use by affiliates.

Condition	Enforcement Action
Condition 1: An Individual's affiliation must be formally	1. The Administrator will indicate the individual's intent to continue affiliation and request that a new role (such as

documented and verified at least once every 365 calendar days.	"retired" OR appropriate POI type) be reflected on the individual's HR record. The Administrator, along with any necessary support from HR&D as needed, will inform the individual of their responsibilities and obligations associated with continuing the affiliation, if applicable. • The Administrator will follow the steps outlined in Scenario 1. 2. New access will be granted based on the type of affiliation. The Administrator for the new affiliation will submit the access request form, if supplementary access is required in addition to the access that is provisioned based on the new status ("Retired" or "POI"). Once the supplementary access request is completed, the Help Desk will notify the individual, and Administrator. • It is the responsibility of the separated individual to request an annual extension of their affiliation, following the aforementioned steps.
Condition 2: Individuals remain subject to Board of Regents rules	At the time of separation, for any reason, the employee will be advised of their status as a separating employee (emeriti, retiree/annuitant, adjunct, faculty/researcher, etc.) by their Administrator. • The employee will be made aware that their continued access must be approved by their Administrator. The Administrator will notify the Help Desk when access needs to be changed. • The individual will also receive a notice every time they change the password for their UW-Whitewater account, via an automated process.
Condition 3: Individuals are required to annually complete information security awareness training	Shared Services will notify separated individuals to ensure they are included in the annual security awareness training process. • Note: Failure to complete the annual security awareness training by the completion date will result in revocation of the continued access and disabling the individual's account. The separated individuals may not appeal the revocation, once their account has been disabled.
Condition 4: Access will be disabled after one (1) year of inactivity based on last login date	iCIT will disable the account after one year of inactivity. Once an account is deprovisioned, it cannot be appealed or reinstated.

Resources:

Information Security Account Lifecycle Practice Directive

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:	09/29/2020
Version no:	V1.0
Date for next review:	09/29/2022

Revision History

Version	Revision date	Description of changes	Author
1.0	09/29/2020	Procedure established	Quality Assurance Improvement Manager

Contact Person/Unit

Contact Person/Unit:	CIO / Elena Pokot / (262) 472-7790 / pokote@uww.edu

Keywords

Keywords:	Information Security, Information Technology, NetID, Continued Affiliation, Continued Access, Extended Access, IT Access.