University of Wisconsin Whitewater

Information Security Shared User Accounts Practice Directive

	Division: Academic Affairs
	Department: Instructional, Communication & Information Technology (ICIT)
	Contact Information: CIO / Elena Pokot / (262) 472-7790 / pokote@uww.edu
	Effective Date: 11/02/2020
	Revised Date: 11/02/2022

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

Objective:

The University of Wisconsin-Whitewater is committed to providing a secure information technology (IT) environment in support of the mission of the university. This Practice Directive is intended to ensure compliance with UW System Policies, Regent Policies, State Statutes, and Federal Statutes regarding information security account management.

Statement:

This Practice Directive and its corresponding Procedure highlight the importance of proper account management, specifically concerning how to request and manage a shared user account. These guidelines include the additional controls needed to manage these accounts, and annual confirmation that the account is still required to fulfill a business need, to reduce risk and safeguard access to information associated with the accounts.

Procedures:

Information Security Account Lifecycle Practice Directive and Procedure

Searchable Words:

Information Security, Information Technology, NetID, Role, Account, Shared Account, User Account, Credential, Access, Extended Access, IT Access, Authorization.