



## Information Security Account Lifecycle – Change of Role and Separation Practice Directive

<b>Division:</b> Academic Affairs
<b>Department:</b> iCIT
<b>Contact Information:</b> CIO / Elena Pokot / (262) 472-7790 / pokote@uww.edu
<b>Effective Date:</b> 09/29/2020
<b>Revised Date:</b> MM/DD/YYYY

### 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 supporting a variety of safety and risk management best practices across our campus. This procedure is intended to ensure compliance with UW System Policies, Regent Policies, State Statutes, and Federal Statutes regarding information security access and authentication.

### Statement:

This Practice Directive and its corresponding Procedure highlight the importance of information security authentication by ensuring information and technology access is only granted to those who need it, those with appropriate access follow information security training and best practices, and that internal controls are enforced such that low, moderate, and high risk data is protected to foster a safe campus technological environment.

### Procedures:

[Information Security Account Lifecycle Procedure](#)

### Searchable Words:

Information Security, Information Technology, Authentication, Password, Passwords, Password Guidance, Net ID, Shared Accounts, Continued Affiliation, Continued Access, Extended Access, IT Access.