The University of Wisconsin System Administrative Policy 1030

Title: Information Security: Authentication

Original Issuance Date: September 14, 2016
Last Revision Date: September 16, 2019
Effective Date: 6 months after publication

1. POLICY PURPOSE

The purpose of this policy is to establish specific minimum standards for authentication across the University of Wisconsin System. This policy is designed to ensure that the UW System manages authentication in a consistent manner and to appropriately safeguard account-based access to information assets.

2. RESPONSIBLE UW SYSTEM OFFICER

Associate Vice President (AVP) for Information Security

3. SCOPE

This policy applies to all authentication administered throughout the UW System, whether centrally managed, managed in a distributed fashion, or departmentally managed. This policy applies to all individuals and entities who intend to access the UW System's information systems and data. To the extent possible, the elements of Section 6 of this policy should be incorporated into contracts with third party providers.

4. BACKGROUND

The President of the University of Wisconsin System is empowered to establish information security polices under Regent Policy Document 25-5, *Information Technology: Information Security*. The UW System is committed to a secure information technology (IT) environment in support of its mission. This policy is designed to help ensure strong and consistent authentication standards throughout the computing environments of the UW System.

5. DEFINITIONS

The following key terms are presented in this policy. Please refer to the UW System Information Security Program Glossary for the following definitions:

- Authentication
- Multi-factor Authentication (MFA)

Low Risk Data: Data assets classified as being of low risk as defined in UW System Administrative Policy 1031, *Information Security: Data Classification and Protection.*

Moderate Risk Data: Data assets classified as being of moderate risk as defined in UW System Administrative Policy 1031, *Information Security: Data Classification and Protection.*

High Risk Data: Data assets classified as being of high risk as defined in UW System Administrative Policy 1031, *Information Security: Data Classification and Protection.*

6. POLICY STATEMENT

Authentication methods for moderate and high risk data shall meet the standards outlined in UW System Administrative Procedure 1030.A, *Information Security: Authentication Standard*.

Access to view low risk data does not require authentication. However, access to modify low risk data shall use authentication methods that meet the requirements for accessing moderate risk data.

7. RELATED DOCUMENTS

Regent Policy Document 25-5, *Information Technology: Information Security*
UW System Administrative Procedure 1030.A, *Information Security: Authentication Standard*
UW System Administrative Policy 1031, *Information Security: Data Classification and Protection*
UW System Information Security Program

8. POLICY HISTORY

Revision 3:	September 16, 2019
Revision 2:	January 09, 2019
Revision 1:	July 31, 2017
First approved:	September 14, 2016

9. SCHEDULED REVIEW

September 16, 2020 (One year from published date)

APPROVED BY:

_____

Raymond W. Cross
President
University of Wisconsin System