The University of Wisconsin Oshkosh
Policy # 1030
Information Security: Authentication

UNIVERSITY OF WISCONSIN OSHKOSH

Original Issuance Date:	September 14, 2016
Last Revision Date:	September 14, 2016
Next Review Date:	March 2017

1. PURPOSE

The purpose of this policy is to establish specific minimum standards for authentication and authentication management 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 OFFICER

Chief Information Officer.

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 University's information systems and data. To the extent possible, the elements of Section 6 of this policy shall 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 (https://www.wisconsin.edu/regents/policies/information-technology-information-security/). The UW System is committed to a secure information technology 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

Authentication: The process of verifying that someone who holds an account on an information system is who they purport to be.

Level of Assurance: The degree of confidence that someone who holds an account on an

information system is who they purport to be.

Low Risk Data: Data assets classified as being of low risk as defined in UW System Administrative Policy 1031, *Information Security: Data Classification* (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/).

Moderate Risk Data: Data assets classified as being of moderate risk as defined in UW System Administrative Policy 1031, *Information Security: Data Classification* (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/)

High Risk Data: Data assets classified as being of high risk as defined in UW System Administrative Policy 1031, *Information Security: Data Classification* (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/).

6. POLICY STATEMENT

1. Any access to data not defined as *low risk* must meet, at a minimum, the current National Institute of Standards and Technology (NIST) Special Publication 800-63 Level of Assurance requirements. Access to low risk data does not require authentication.
2. Authentication methods to access moderate risk data must meet Level of Assurance 2 (LOA 2) requirements.
3. Authentication methods to access high risk data must meet Level of Assurance 2 (LOA 2) requirements and in addition employ multi-factor authentication.

7. REFERENCES

Levels of assurance, the associated authentication requirements, and the required procedures to implement this policy are outlined in UW System Administrative Procedure 1030.A, Information Security: Authentication (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/information-security-authentication/).

NIST Special Publication 800-63, Electronic Authentication Guideline (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf)

UW System Administrative Policy 1030, Information Security: Authentication (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/)

UW System Administrative Procedure 1030.A, Information Security: Authentication (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/information-security-authentication/)

UW System Administrative Policy 1031, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/)

UW System Administrative Procedure 1031.A, Information Security: Data Classification (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-data-classification/information-security-data-classification/)

UW System Administrative Policy 1032, Information Security: Awareness (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/)

UW System Administrative Procedure 1032.A, Information Security: Awareness (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-awareness/)

UW System Administrative Policy 1033, Information Security: Incident Response (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-incident-response/)

UW System Administrative Policy 1034, Information Security: Acceptable Use (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-acceptable-use/)

UW System Operational Policy GEN 13 Layoff for Reasons of Budget or Program (https://www.wisconsin.edu/ohrwd/download/policies/ops/gen13.pdf)

Regent Policy Document 25-5, Information Security (https://www.wisconsin.edu/regents/policies/information-technology-information-security/)

Wisconsin Administrative Code s. 35.93, Chapter UWS 4, Procedures for Dismissal (http://docs.legis.wisconsin.gov/code/admin_code/uws/4.pdf)

Wisconsin Administrative Code s. 35.93, Chapter UWS 11, Dismissal of Academic Staff for Cause (http://docs.legis.wisconsin.gov/code/admin_code/uws/11.pdf)

Wisconsin Administrative Code s. 35.93, Chapter UWS 17, Student Nonacademic Disciplinary Procedures (http://docs.legis.wisconsin.gov/code/admin_code/uws/17.pdf)

8. PROCEDURES

UW System Administrative Procedure 1030.A, Information Security: Authentication (https://www.wisconsin.edu/uw-policies/uw-system-administrative-policies/information-security-authentication/information-security-authentication/)

9. REVISION HISTORY

09/14/2016	Effective date of UW System policy.
06/30/2017	Approved by Chancellor Leavitt.

APPROVED BY:

Chancellor Andrew Leavitt