Standard: Password Standard

Effective Date:	2017.02.21
Revision Date:	2020.02.06
Review Date:	2021.02.06
Approving Body:	Chief Information Officer
Authority:	Information Security Policy
Responsible Owner:	Director, Information Security and Compliance
Classification:	Public

Purpose

The Password Standard describes the acceptable standards for password construction and password management.

Who/what does the standard apply?

The requirements in this standard apply to computing passwords used to access any University of Manitoba owned systems and applications by:

- Students
- Academic staff
- Support staff
- IT Support
- Contractors
- Vendors

Definitions

- **User account:** refers to an account (username and password) that gives an individual access to a computer, network or service.
- **Administrative User account:** refers to an account that is used for performing IT system administrative activities
- **IT Support:** All staff in a unit or faculty who are responsible for maintaining computer systems and hardware, and for making decisions pertaining to those systems.
- **Service account:** refers to an account created to provide the privileges required by a computer program to perform its intended function
- **Brute Force attack:** an attempt to gain unauthorized access to a computer, network or system through a user account by trying every possible password combination until the correct one is entered

Compliance

Systems and applications must align to the requirements and specifications outlined within this standard. Where systems and applications are unable to comply, please submit an Information Security Decision Request to the Director of Information Security and Compliance for review.

Specifications

Requirement	Specifications
Password management systems must enforce minimum password length	Require a minimum of 10 characters for *User account* passwords. Require a minimum of 12 for *Administrative User account* passwords. Require a minimum of 16 characters for *service account* passwords.
Password management systems must enforce minimum character types	Passwords must contain at least 3 of the following 4 character types: • Upper case characters • Lower case characters • Numerical characters • Special characters
Password management systems must limit the life of passwords	The authentication service must enforce a maximum password lifetime of one year for user accounts, 90 days for administrative accounts, or one year for administrative accounts that use a second factor for authentication (i.e. a token).
Password management systems must enforce a password history	The authentication service must maintain a history of previous account passwords and prevent re-use of the previous 5 passwords.
Password management systems must prevent Brute Force password attacks	The authentication service must lock and disable end User and Administrative User accounts after a maximum of 6 consecutive failed login attempts.
Password management systems must safeguard stored passwords	Password Management systems must employ Encryption to safeguard password data stored within them.

References

Policy, Procedure or Standard	
Information Security Policy and Procedure	
Use of Computer Facilities Policy and Procedure	