UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
PROCEDURE

Procedure:	**Password Standard**
Parent Policy:	Information Security Policy
Effective Date:	February 21, 2017
Revised Date:	
Review Date:	February 21, 2027
Approving Body:	Vice President (Administration)
Authority:	The University of Manitoba Act
Responsible Executive Officer:	Vice President (Administration)
Delegate: **(If applicable)**	Chief Information Officer
Contact:	Director, Information Security and Compliance
Application:	All Employees, All External Parties, Students

Part I
Reason for Procedure

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

Part II
Procedural Content

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

- Students
- Academic staff
- Administrative Support staff
- IT Administrators
- Distributed IT staff
- Contractors
- Vendors

2.2 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
- 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

2.3 Systems and applications must align to the requirements and specifications outlined within this standard. Where systems and applications are unable to comply, complete and submit an Information Security Decision Request Form for an Exception.

2.4 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.

Part III
Accountability

3.1 The Office of Legal Counsel is responsible for advising the President that a formal review of this Procedure is required.

3.2 The Vice-President (Administration) is responsible for the implementation, administration and review of this Procedure.

3.3 All employees, students and third parties are responsible for complying with this Procedure.

Part IV
Review

4.1 Governing Document reviews shall be conducted every ten (10) years. The next scheduled review date for this Procedure is June 23, 2027.

4.2 In the interim, this Procedure may be revised or repealed if:

(a) the Chief Information Officer or the Approving Body deems it necessary or desirable to do so;

(b) the Procedure is no longer legislatively or statutorily compliant;

(c) the Procedure is now in conflict with another Governing Document; and/or

(d) the Parent Policy is revised or repealed.

Part V
Effect on Previous Statements

5.1 This Procedure supersedes all of the following:

(a) all previous Board of Governors/Senate Governing Documents on the subject matter contained herein; and

(b) all previous Administration Governing Documents on the subject matter contained herein.

Part VI
Cross References

6.1 This Procedure should be cross referenced to the following relevant Governing Documents, legislation and/or forms:

(a) Information Security Policy

(b) Information Security Procedure

(c) Use of Computer Facilities Policy

(d) Use of Computer Facilities Procedure