Purpose

This standard describes the password policy to be applied to the enterprise authentication sources.

Scope

This standard applies to MUNLDAP and Memorial Active Directory.

Password Policy

Minimum Length	8 characters
Maximum Length	128 characters
Password History	10 password changes are required before reusing a previous password
Expiration	180 days for faculty and staff 365 days for students and other members
Minimum Password Age	1 day
Lockout	After 10 attempts
Inactivity Lockout	After 3 months of inactivity for faculty and staff After 6 months of inactivity for students and other members
Complexity or Composition	[Windows Standard] Must contain **at least three** of the following types of characters: 1. Upper Case Letters: A through Z 2. Lower Case Letters: a through z 3. Numerals: 0 through 9 4. Special characters The password cannot contain the user's first name, middle name, last name, or username.

Related

- MUN Login ID Standard

Revision History

Version	Date Reviewed	Reviewed By
1.0	August 24, 2015	IAM Advisory Committee

Issued By	Office of the Chief Information Officer	**Effective Date**	October 2015
Target Audience	Memorial University	**Review Date**	October 2017
Approved By	Ken Forward, IT Security Officer Shelley Smith, CIO	**Approved Date**	September 1, 2015