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

<table>
<thead>
<tr>
<th>Minimum Length</th>
<th>8 characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Length</td>
<td>128 characters</td>
</tr>
<tr>
<td>Password History</td>
<td>10 password changes are required before reusing a previous password</td>
</tr>
<tr>
<td>Expiration</td>
<td>180 days for faculty and staff 365 days for students and other members</td>
</tr>
<tr>
<td>Minimum Password Age</td>
<td>1 day</td>
</tr>
<tr>
<td>Lockout</td>
<td>After 10 attempts</td>
</tr>
<tr>
<td>Inactivity Lockout</td>
<td>After 3 months of inactivity for faculty and staff After 6 months of inactivity for students and other members</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date Reviewed</th>
<th>Reviewed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>August 24, 2015</td>
<td>IAM Advisory Committee</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Issued By</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Chief Information Officer</td>
<td>October 2015</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Target Audience</th>
<th>Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memorial University</td>
<td>October 2017</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Approved By</th>
<th>Approved Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ken Forward, IT Security Officer Shelley Smith, CIO</td>
<td>September 1, 2015</td>
</tr>
</tbody>
</table>