Policy Name: Password Policy for Information Systems
Originating/Responsible Department: Information Technology Services (ITS)
Approval Authority: Senior Management Committee
Date of Original Policy: April 2006
Last Updated: September 2019
Mandatory Revision Date: September 2020
Contact: AVP (ITS) & Chief Information Officer

Policy:
Passwords and second factor authentication are a critical part of information and network security at Carleton University. Poorly chosen passwords, if compromised, may result in unauthorised disclosure, modification or destruction of university and personal information assets. To mitigate this risk, unique user accounts with strong, secure passwords are required at all times. In addition to provide adequate security, University enterprise applications and systems that process financial, sensitive or confidential information or provide users privileged access require that users have second factor authentication enabled.

In any scenario where password controls cannot comply with established password standards; e.g.; solely to due to technological system limitations, the risk must be mitigated through appropriate compensating controls.

Purpose:
The purpose of this Policy is to:
- Define the parameters for creating, protecting, and managing passwords such that identified risks are appropriately addressed;
- Provide for the use of a second factor (2-factor) for securing enterprise applications, systems and sensitive, financial and confidential information;
- Provide for the requirement for uniquely identifiable accounts in support of forensic and security investigations, ensuring that actions can be attributable to a single individual.

Scope:
This Policy applies to all IT systems that connect to the Campus Network and use passwords for authentication with the exception of student accounts.

Procedures:
1.0 Implementation
Password requirements are grouped into three categories:
- Regular (non-privileged) accounts
- Privileged accounts that have elevated privileges or are used in automated system processes (ex: Administrator, System level, Service Accounts, Root)
- Accounts used on IT systems that are in-scope for the Payment Card Industry Data Security Standard
For all passwords, the following are common requirements:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Standard</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complexity</td>
<td>• At least 1 lowercase character</td>
<td>Any 3 of these 4 standards must be met</td>
</tr>
<tr>
<td></td>
<td>• At least 1 uppercase character</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• At least 1 numeric character</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• At least 1 special character</td>
<td></td>
</tr>
<tr>
<td>Prohibited content</td>
<td>• Password must not contain account ID, email, words found in common dictionaries</td>
<td></td>
</tr>
<tr>
<td>Password history</td>
<td>• No reuse of last 10 passwords</td>
<td>Common practice to subvert the policy and get back to the current password is multiple changes in one day</td>
</tr>
<tr>
<td>Change Frequency</td>
<td>• Permitted once per day</td>
<td></td>
</tr>
<tr>
<td>Incorrect password entries before lockout</td>
<td>• After 10 incorrect password entries within 20 minutes, the user will be locked out of the account for 30 minutes</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Identities must be verified before any authentication credential can be reset.

Passwords for first-time use (temporary) and upon reset must be set to a unique value for each user, and changed immediately after the first use.

### 2.0 Regular Accounts

In addition to the common requirements identified in section **1.0** above, the following additional requirements exist for IT system passwords for regular, non-privileged accounts:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Standard</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>• At least 8 characters in length</td>
<td></td>
</tr>
<tr>
<td>Password change frequency</td>
<td>• Must be changed every 120 days</td>
<td></td>
</tr>
</tbody>
</table>

### 3.0 Privileged Accounts

In addition to the common requirements identified in section **1.0** above, the following requirements pertain to:
- System accounts or services accounts used to facilitate IT system functions; e.g.; batch processes, system tasks, etc., and not associated with an individual
- Accounts with elevated privileges (root level, administrator level, backup operator, etc.)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Standard</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>• At least 15 characters in length</td>
<td></td>
</tr>
<tr>
<td>Password change frequency</td>
<td>• Must be changed every 120 days</td>
<td>Not required for <em>automated</em> system or service accounts</td>
</tr>
</tbody>
</table>

4.0 2-Factor Required For Access
For university enterprise applications and systems that:
- Process financial, sensitive or confidential information; or
- Accounts with elevated privileges (root level, administrator level, backup operator, etc.)
a second factor must be added to provide an elevated level of security.

5.0 Account Uniqueness
Non-system accounts must be unique and identifiable as belonging to a specific individual. Documented processes must exist to ensure the identity of individuals is confirmed before granting credentials. With the exception of student accounts, this applies to the entire University community including guests, contractors, visitors and vendors.

The only permitted exception to this statement is for the provisioning of temporary wireless access to support University business. Provisioning of wireless network services may be established conditional upon the following requirements:
- The wireless service is being provisioned on behalf of a staff or faculty member of Carleton University;
- The requesting staff or faculty member assumes responsibility for the use of the wireless service for the duration of the service in accordance with the University’s Acceptable Use Policy;
- The duration of the service does not exceed 5 business days; and
- The wireless service uses a unique Service Set Identifier (SSID) and password that is associated with the staff or faculty member.

6.0 Password Protection Requirements
Protection of the confidentiality of passwords is crucial to securing confidential and sensitive information on IT assets:
- Support staff must never request another user’s password;
- Passwords must be treated as confidential information;
- The use of group and shared IDs and/or passwords or other shared authentication methods are prohibited without a strong and valid business justification;
- Wireless passwords or passphrases are not to be shared except as noted in section 5.0 above;
- Passwords must not be transmitted or stored using insecure methods such as “post-it-notes”, e-mail or unencrypted network services (ex: telnet, ftp);
- The requirements in the Cloud Computing Security Policy are to be met for any cloud based password management systems;
- Industry standard encryption must be used for electronic storage and transmission;
- Physical security controls must restrict access to hardcopy records of passwords;
- Passwords used to gain access to University systems must not be used as passwords to access non-university accounts or information;
- If an individual suspects that their password has been compromised, the individual must change their password immediately and report the incident to the ITS Service Desk or their local IT support if the authentication service is provided through the local IT support;
- Passwords used on Carleton systems must not be re-used on non-Carleton systems; and
- Individual (non-system or non-service) accounts that have been inactive for three years or more must be disabled and assessed for deletion.
Roles and Responsibilities:
ITS is responsible for:
- Providing and managing enterprise authentication services for the University community in accordance with this Policy

All IT Support groups are responsible for:
- Ensuring local authentication services are managed in accordance with this Policy
- Validating a user's identity before changing or resetting a user's password

All users are required to:
- Protect their user credentials from disclosure to all individuals and/or entities
- Change their password on suspicion or indication that their password has been compromised
- Report any suspicious behaviour or suspected compromise of their user account to the ITS Service Desk or their respective IT support team
- Ensure their Carleton password is not used on non-Carleton systems
- Ensure that passwords are stored securely

Compliance:
Non-compliance with this policy may result in disciplinary action.

Contacts:
AVP (ITS) & Chief Information Officer

Links to related Policies: [http://carleton.ca/secretariat/policies/](http://carleton.ca/secretariat/policies/)

- Acceptable Use Policy for Information Technology (IT)
- Information Security
- Information Technology (IT) Security
- Data and Information Classification and Protection
- Cloud Computing Security