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:	**January 2022**
Mandatory Revision date:	**January 2023**
Contact:	**Director, Information Security (ITS)**

Policy:

Passwords are a critical part of information and network security at Carleton University. Poorly chosen passwords, if compromised, may result in unauthorized disclosure, modification or destruction of University information assets. To mitigate this risk, unique user accounts with strong, secure passwords are required at all times.

In any scenario where password controls cannot comply with established password standards; e.g.; due to technology 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. The Policy also supports 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:

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

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:

Parameter	Standard	Comments
Length	• At least 8 characters in length	
Password change frequency	• Must be changed every 120 days	

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.)

Parameter	Standard	Comments
Length	• At least 15 characters in length	
Password change frequency	• Must be changed every 120 days • Not required for *automated* system or service accounts	

4.0 Accounts and Passwords for Systems In-Scope for PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) specifies compliance requirements for all systems and supporting infrastructure that process, store or transmit credit card information. In addition to the requirements in section **1.0** above, the following PCI DSS specific requirements exist:

Parameter	Standard	Comments
Length	• At least 8 characters in length	
Password change frequency	• Must be changed every 90 days	

In the event that other forms of authentication mechanisms are employed, those mechanisms must be assigned to the individual account for which it was created and not shared among multiple accounts.

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, visitors and vendors.

The only established 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
- 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 cruciazl to securing confidential and sensitive information on IT assets:

- Support staff must never request user passwords

- Passwords must be treated as confidential information
- If someone demands your password, refer them to this Policy or have them contact the relevant IT Department; e.g., ITS
- 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 are not to be transmitted or stored in insecure manners such as via "post-it-notes", e- mail or unencrypted network services (ex: telnet, ftp)
- 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, it must be reported to ITS or the appropriate IT group and the password changed immediately

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

All users are required to:

- Protect their user credentials from disclosure to unauthorised individuals
- Report any suspicious behaviour or suspected compromise of their user account to ITS or their respective IT support team

Compliance:

Non-compliance with this Policy may result in disciplinary action.

Contacts:

Director, Information Security, ITS

Links to related Policies: http://carleton.ca/secretariat/policies/

- Acceptable Use Policy for Information Technology (IT)