

Password Policy

January 2026

TEMPLATE ONLY





[THIS PAGE IS INTENTIONALLY LEFT BLANK]





Contents

Password Policy	1
1. Introduction	4
2. Purpose	4
3. Scope.....	4
4. Policy.....	4
4.1 Password Creation	4
4.2. Password Change	4
4.3 Password Protection	5
5. Policy Compliance	5
5.1 Compliance measurement.....	5
5.2 Exceptions	5
5.3 Non-Compliance	5
6. Related Standards, Policies and Processes	6
7. Definitions and Terms.....	6





1. Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Peppermint IT's entire corporate network. As such, all Peppermint IT employees, or Interns/directors (including contractors and vendors with access to Peppermint IT systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

This policy applies to all personnel or intern/directors who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any Peppermint IT facility, and has access to the Peppermint IT network, or stores any non-public Peppermint IT information.

4. Policy

4.1 Password Creation

- 4.1.1 All user-level and system-level passwords must conform to the Guidelines for Password Construction.
- 4.1.2 The length and complexity is, at minimum, 12 characters and must include a combination of uppercase and lowercase letters, numbers and special characters.
- 4.1.3 Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.
- 4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as Sodo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.
- 4.1.5. Unique password must be unique and that they are not reused across multiple systems or applications.

4.2. Password Change

- 4.2.1 Passwords should be changed only when there is reason to believe a password has been compromised.
- 4.2.2 Users will be notified in advance of upcoming password expiration.
- 4.2.3 Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates or "penetration testers". If a password is guessed or cracked during one of these scans, the user will be required to change it to comply with the Password Construction Guidelines accounts.





4.2.4 User accounts that have system-level privileges granted through group memberships or programs such as Sodo must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommended that some form of multi-factor authentication is used for any privileged accounts.

4.2.5 Users must not reuse any of their last 5-10 passwords and that it must be significantly different from their previous ones.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, Confidential Peppermint IT information. Corporate Information Security recognises that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Please refer to Password Sharing Policy for Internal Password Sharing Guidelines.

4.3.3 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication, nor revealed over the phone to anyone.

4.3.4 All Passwords which link with Peppermint IT should be stored only in "password managers" authorised by the organisation.

4.3.5 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.6 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.3.7. All devices must be locked when unattended.

4.3.8 Passwords must not be stored on shared or unencrypted devices.

4.3.9 Do not attempt to bypass system password requirements or technical controls.

5. Policy Compliance

5.1 Compliance measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Compliance will be measured through using security incident reports, completion of mandatory security awareness and password training and audits.

5.2 Exceptions

Any Exception to the policy must be improved by the Infosec team in advance. They must also be formally conducted and approved my management or IT security and are time limited.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.





6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

Application Administration Account: Any account that is for the administration of an application (i.e., SQL database administrator, etc.).

Password: A string of characters that serve as authentication of a person's identity, which may be used to grant or deny access to private or shared data.

Strong Password: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password, the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about the password owner such as a birth date, social security number, and so on.

