Password Policy

**Classification**: Internal

This document may only be shared internally without prior confirmation from the owner.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Version | Approved By | Owner | Date Last Updated | Review Frequency | Next Review | Comments |
|  |  |  |  |  |  |  |

Contents

[Purpose of This Document 1](#_Toc169191293)

[Scope 1](#_Toc169191294)

[Information Security Team 2](#_Toc169191295)

[Staff 2](#_Toc169191296)

[Policy 2](#_Toc169191297)

[User Guidance 2](#_Toc169191298)

[Policy Specifics 2](#_Toc169191299)

[Password Creation Guidance 2](#_Toc169191300)

[Multi-Factor Authentication (MFA) 3](#_Toc169191301)

[Exceptions 3](#_Toc169191302)

[Reporting Compromised Passwords 3](#_Toc169191303)

# Purpose of This Document

This policy sets standards for creating and protecting complex passwords and their guidelines.

Effective passwords are crucial to safeguard user accounts and systems. A weak password can jeopardise our entire network and data.

# Scope

The policy covers all users of TechSolution.inc 's IT Systems: employees, contractors, temporary staff, and external third parties.

Responsibilities

## 

## Information Security Team

The IS team oversees policy enforcement and conducts regular compliance checks.

## Staff

All staff are responsible for adhering to this policy and must accurately follow the policy and protect data availability, confidentiality, and integrity where applicable.

# Policy

## User Guidance

The password guidelines follow the latest government/industry best practices.

We recommend passphrases over passwords. Relevant articles are in the Appendices. Technical controls support this approach.

## Policy Specifics

* Passphrases should be at least 12 characters.
* Use Multi-Factor Authentication where possible.
* Initial login prompts a passphrase change.
* Habitually lock/unlock your computer and log in daily.
* 5 incorrect attempts lock accounts.
* 14-day warnings precede passphrase expirations.
* Passphrase reuse is forbidden.
* Passphrase changes have a one-day interval.
* Sharing passwords, including with IT, is forbidden.
* Significant security events prompt passphrase changes.
* Never share credentials insecurely (e.g., unencrypted emails, paper).
* Store/transmit passwords using encrypted methods like Password Managers.

# Password Creation Guidance

Many password-remembering strategies are weak, like character substitutions or using dictionary words.

Here are three more robust methods:

* **Raw Strength:** Learning a random character set isn't as complicated as it seems. Repeated typing can help memory.
* **Personal Phrases:** Turn "I love sports and exercise 2 times per week at my Croydon gym" into "Ils&e2t/w@mCg".
* **Unique Long Phrases:** Merge "Dark Side of the Moon" & "It's nice to see you, to see you, nice" into "Dark side 2 see you, nice!"

# Multi-Factor Authentication (MFA)

Requiring an additional layer of verification beyond a password enhances the security of user accounts and protects sensitive information.

All users must enable Multi-Factor Authentication (MFA) on their accounts wherever possible. This includes but is not limited to, email accounts, cloud services, and critical internal applications.

Acceptable forms of MFA include

* One-Time Passwords (OTPs) sent via SMS or email.
* Authentication apps (e.g., Google Authenticator, Microsoft Authenticator).
* Hardware tokens (e.g., YubiKey).
* Biometric verification (e.g., fingerprint, facial recognition).

# Exceptions

Avoid using organisational passwords personally or vice-versa.

Passwords should never be shared unless IT Leadership or the Information Security Team approves, such as during training.

# Reporting Compromised Passwords

If a password is believed to have been compromised, notify the ServiceDesk and the Information Security Team immediately, and then change it.