Password and credential Policy

Ensure good password practices within Microlink are followed and ensure the policies extend 3rd party systems wherever possible.

# Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change |
| 0.1 | 02/03/2022 | David Henderson | Initial draft to combine multiple password policy items into a central policy |
| 1.0 | 29/03/2022 | David Henderson | Change wording and punctuation  |
| 1.1 | 30/09/2022 | D Henderson | Included inline document owner |
|  |  |  |  |

Document Owner **IT**

# Introduction/Overview

This password policy is to ensure all staff are aware of good password hygiene and best practices. What staff are responsible for regarding how password should be created managed and protected throughout their use, and what is acceptable with regards to password storing.

Across many industries, weak passwords have been the main cause for account compromise. Ensuring strong and healthy password hygiene, creation and management regime ensures this threat is minimised.

It is also understood that Microlink’s internal IT department is unable to enforce password measures across systems outside of its control, and therefor responsibility for good password management must be passed down to all staff.

The policy also ensures we remain in compliance with “The Regulation of Investigatory Powers Act 2000 (RIPA)” “Data Protection Act 2018 (DPA 2018)” and the “General Data Protection Regulation (GDPR)”

Contents

-----

[Version Control 1](#_Toc99379839)

[Introduction/Overview 1](#_Toc99379840)

[1. Definitions 3](#_Toc99379841)

[Applicability 3](#_Toc99379842)

[2. Activities 3](#_Toc99379843)

[Included activities 3](#_Toc99379844)

[Controls 3](#_Toc99379845)

[3. Password Management software 3](#_Toc99379846)

[3.1. Approved Password management software 3](#_Toc99379847)

[3.2. Appropriate password management uses 4](#_Toc99379848)

[4. Password hygiene 4](#_Toc99379849)

[4.1. Password should be difficult to guess yet memorable 4](#_Toc99379850)

[4.2. Requirements for changing a password. 4](#_Toc99379851)

[4.4. Unique passwords 4](#_Toc99379852)

[5. Multiuser Scenarios – Shared passwords 5](#_Toc99379853)

[6. Password compromise 5](#_Toc99379854)

[7. Multi Factor Authentication 5](#_Toc99379855)

[8. Exceptions 5](#_Toc99379856)

[9. Failure to comply. 5](#_Toc99379857)

[10. Monitoring 5](#_Toc99379858)

[11. Addendum 5](#_Toc99379859)

[Why is Single Sign on and Same Sign on (SSO) Exempt from Unique password policy? 5](#_Toc99379860)

|  |  |
| --- | --- |
| *Definition* | *Meaning* |
| Password | Passphrase, Passwords, Secret. A memorable set of characters used to authenticate and or gain access to a system. Note: Unlike the name implies passwords are not necessarily singular, predictable “Words” but a combination of random, as humanly memorable, characters and combined words. |
| Authenticate | The process in which a person proves their identity. Such as providing a password. |
| Single Sign on | SSO provides the business a safe way to use a single set of credentials (username and password) to authenticate across multiple systems without each system having any access to those credentials. |
| Multi Factor Authentication (MFA) | Multi Factor Authentication. There are 3 main factors to prove who you are, Something You Know, Something You Have, Something of You.* Something you know is a memorised password or PIN.
* something you have could be a phone that received SMS message, a physical Smartcard issued only to you, device that generate time based onetime Passwords such as Phone authentication app or RSA Keyring.
* Something of you is any type of Bio metric such as fingerprint scan, Iris scan, DNA sequence, face, or voice recognition.
 |

# Definitions

# Applicability

This policy will apply to you when conducting the following activities even when the system does not enforce any controls:

## Activities

### Included activities

* 1. Signing into any work-related system either:
	2. Owned by Microlink or
	3. Owned by any 3rd party and provided to Microlink for work related purposes.
	4. And where the system login credentials are set or able to be changed by the account holder.
	5. Or where your job roles involve you managing other passwords, such as resetting access to a portal or primary account holder for a service that uses shared credentials.
	6. Creating password for purposes of protecting a document.

# Controls

## Password Management software

### Approved Password management software

The following password managers are **approved** for staff to use under the following conditions.

* + 1. Microsoft Edge – Built in password manager

You **must** be signed into a Microlink supplied workstation.

You **must** be signed into Edge using Microlink credentials

* + 1. Intranet Password Manager – Built into Intranet [Vault - Microlink Intranet (Microlinkpc.com)](https://intranet.microlinkpc.com/user/vault/)
		2. KeePass
		3. All other password management software is **prohibited** within Microlink.

### Appropriate password management uses

*Each of the above password management systems have different strengths and are approved for certain uses*
*Microsoft Edge for example is good for managing all web-based portal passwords Whilst the intranet is good for storing password for protected documents or portals that need internally sharing.*

* + 1. Microsoft Edge – Generating, storing, and auto filing of all passwords for web-based portals.
		2. Intranet Password Manager

Storing passwords – Documents, Web portals

Sharing passwords with other staff - limited portals that do not support individual user access for our business.

* + 1. KeePass – storing generating password. – Use of KeePass is not for general availability and only in certain circumstances which will be looked at on a case-by-case basis.

Microlink maintains complete control over the above password mangers and their contents. All passwords stored within the manager remain the property of Microlink.

Whilst it would not be deemed a breach of this policy, for the security of your own personal accounts, it is **not** recommended to store any personal password or credentials in any of the business provided password management tools.

## Password hygiene

*Where password managers cannot be used to generate and store complex immemorable passwords, good password hygiene is required.*

*Password hygiene is the practice of ensuring passwords are difficult to guess, unique, and hard to crack. It is the set of guidelines and principles that, when leveraged correctly, help keep your passwords protected from cybercriminals.*

### Password should be difficult to guess yet memorable

* + 1. When creating a password, you **must** ensure that all passwords are at least 15 characters in length.
			1. Technical controls **must not** restrict the maximum length of a password.
		2. Passwords **must not** contain common keyboard patterns or consecutive keys on the keyboard such as “qwerty”, “1234” or “abc123”
		3. Password **must not** contain commonly used passwords such as “Admin”, “admin123” or “Password”
		*A list of top 10,000 passwords can be found on Wikipedia here:* [*Wikipedia:10,000 most common passwords - Wikipedia*](https://en.wikipedia.org/wiki/Wikipedia%3A10%2C000_most_common_passwords)
		4. Password **must not** contain words that form a passage from any published literature, such as a book or poster bible.
		5. Passwords **must not** contain “microlink” or any derivative of the company and or any partners names or derivatives.
		6. Passwords **must not** contain all or part (3 consecutive characters) of your username.

*It is recommended that a user create a password in the form of a list of random words. This helps keeping password length high whilst keeping it easy to remember, there still some pitfalls that should be avoided.*

### Requirements for changing a password.

* + 1. Passwords **must** be changed if the password is thought to be compromised.
		2. Technical controls **must not** require passwords to be changed at regular intervals.
		3. Passwords **must** be completely different to previous passwords.
		4. Passwords **must not** contain any section or consecutive characters from previous passwords.

### Unique passwords

* + 1. Passwords **must** be unique for each system or account used.
		2. You **must not** re-use passwords.
		3. You **must not** use passwords you use for personal accounts such as social media, gaming, personal email etc.

### Password Protection

* + 1. Employees are prohibited from sharing Microlink user account passwords with anyone inside or external to the company including colleagues, Line Managers, Directors, IT Staff etc, those claiming to represent a stakeholder or business partner with a legitimate need to access a system.

### Credential Resets

* + 1. Use Self-service password reset from the workstation login screen.
		2. Contact IT help desk via Teams or Phone to be authenticated using One Time Pin registered in the intranet.
		3.

## Multiuser Scenarios – Shared passwords

3rd party systems that **only** provide a single account for the business to access, and/or their services do not support the ability to issue Microlink staff unique sign-ins for all/each user that needs access.
**It is acceptable** to share the account password with those who require access

* 1. An account owner **must** be designated to manage the credentials.
		1. the owner **must** ensure the password is changed when one of the users no longer requires access.
		2. the owner **must** **only** use approved methods/systems for distributing credentials.
		*See:* [*“Approved password management software”*](#_Approved_Password_management)
		3. All passwords that are shared **must** remain tightly controlled and only shared with the account owner’s permission.

## Password compromise

If a password is compromised or suspected of being compromised:

* 1. You **must** change the password immediately.
	2. You **must** inform Internal IT as soon as possible 02380 240 328 or it@Microlinkpc.com
	3. You **must** raise and Incident on the incident management system.

## Multi Factor Authentication

Multi factor authentication is now widely supported on most modern services.
therefore, where available:

* 1. You **must** enable Multifactor authentication on systems where it is available.
	2. Technical controls **must** enforce Multifactor authentication where available possible.
	3. Smart cards and security tokens
		1. When not in use all security token or smart cards issued to you should remain securely stored.
		2. All security tokens and smart cards must be kept on your person during your working day.
		3. It is prohibited to share the use of Security tokens and/or smart cards issued to you.
		4. Any smartcards or security tokens issued to you must be returned at the end of your employment.

# Exceptions

* 1. Services that implement Single Sign on or Same Sign On do not require unique passwords.
	For example, PeopleHR and Office365, Intranet, Sage CRM all use your Microlink login to gain access.

# Failure to comply.

Use of non-approved password managers is a disciplinary offence and will be dealt with using Microlink disciplinary process.

# Monitoring

This policy should be reviewed annually

# Addendum

## Why is Single Sign on and Same Sign on (SSO) Exempt from Unique password policy?

Systems that implement SSO are by nature more secure. This is because each system that subscribes to SSO never actually gets to see, and therefore store, the user’s credentials. This means if one of the systems gets compromised your password does not. That renders the requirement for unique passwords - void.

SSO is also heavily adopted due to the convenience for end users this means the technology is more mature and available as an off-the-shelf and platform as a service (PaaS) solution, meaning it far less likely to be compromised.

This Policy was approved & authorised by:

|  |  |
| --- | --- |
| Name:  | Michael Moore |
| Position: | Legal Counsel |
| Date: | 28 March 2022 |
| Signature: |  |