Multi Factor Authentication Policy

# Version Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Amended By | Summary of Change | Approved by: |
| 1.0 | January 2022 | D Henderson/S Smith | New | Michael Moore, Legal Counsel |
| 2.0 | September 2022 | D Henderson | Word changes | Michael Moore, Legal Counsel |
|  |  |  |  |  |

**Document Owner IT**

Contents

-----

[Version Control 1](#_Toc94083726)

[Summary 1](#_Toc94083727)

[1. Introduction 1](#_Toc94083728)

[2. Mobile Telephones 1](#_Toc94083729)

[3. Controls 2](#_Toc94083730)

[4. Failure to comply 2](#_Toc94083731)

[5. Monitoring 2](#_Toc94083732)

# Summary

Multi Factor Authentication (MFA) strengthens our cyber security obligations. Mobile telephones will be used to authenticate individual log ins took we gain access to a Microlink device.

# Introduction

 Using MFA strengthens our log in process and increases our security posture to prevent accounts being compromised. To protect our business overall, Microlink is adopting Microsoft Security Baseline, industry best practice and cyber security best practices as standard across its Microsoft 365 estate with effect from February 2022.

 The purpose of the MFA log on is:

1.1.1 Verify identify with high assurance.

 1.1.2. Protect accounts from compromise.

# Mobile Telephones

Individuals’ mobile telephones will no longer be prohibited for the purposes of authentication and can be registered by in several ways ***Refer to Guidance Notes on how to register issued by IT***.

* + 1. *Phone number, to receive a text message with a verification code.*
			1. *Code is entered on screen to finalise log in.*
		2. *Any Authentication app of your choosing that supports Time-based one-time passwords (TOTP)*
			1. *Code is entered on screen to finalise Log in.*
		3. *Microsoft App for Notification based Authentication (HOTP)*
			1. *Sends a push notification that you click “Approve” or “Deny” on.*

# Controls

 Hitherto, having a personal mobile telephone out on an individual’s desk remains prohibited. To strengthen our cyber security, it is however necessary to allow the use a mobile phone to strengthen authentication and gain access. After being successfully logged in, all employees will be required to place their mobile telephone in their desk drawer or away from their workspace and only bring it out when there is a need to log in/ authenticate using the device.

 We actively encourage our employees to place a great deal of emphasis on security and to take steps to prevent breaches in protocols involving mobile telephones.

# Failure to comply

 The use of personal mobiles other than for log on purposes is deterred and individuals who are not compliant may be subject to disciplinary action being taken against them.

# Monitoring

 Microlink will update this policy on an annual basis.

|  |  |
| --- | --- |
| Name:  | Michael Moore |
| Position: | Legal Counsel |
| Date: |  |
| Signature: |  |