



# Password Procedure

Reference: FPD0094

Version: 2

Owner: James Pobgee

First Issued Date:

Revision Issued Date:

*To outline FISCAL Technologies' password process.*

**Prepared for:**

All Employees, select Contractors,  
Partners and Customers

Prepared by:  
Rowan Botha

FISCAL Technologies Ltd  
448 Basingstoke Road,  
Reading, RG2 0LP  
Tel: 0845 680 1905



## 1 CONFIDENTIALITY

This document is the property of FISCAL Technologies. It may not be copied, distributed, or recorded on any electronic or other medium without the express written permission of the company.

All material contained in this document which is not readily available in the public domain is regarded as confidential to FISCAL Technologies and may not be divulged to any other parties without the express written permission of FISCAL Technologies.

## Table of Contents

<b>1</b>	<b>CONFIDENTIALITY</b>	<b>1</b>
<b>2</b>	<b>DOCUMENT CONTROL</b>	<b>2</b>
2.1	DOCUMENT PUBLICATION HISTORY	2
<b>3</b>	<b>PURPOSE AND SCOPE</b>	<b>3</b>
3.1	PURPOSE	3
3.2	SCOPE	3
<b>4</b>	<b>PASSWORD PROCEDURE</b>	<b>3</b>
4.1	PASSWORD REQUIREMENTS	3
4.2	PASSWORD RECOMMENDATIONS	4

## 2 DOCUMENT CONTROL

Item	Description
Document Title:	Password Procedure
Associated Controls:	A.9 A.9.4.3 B.5.17
Reference ID:	FPD0094
Version:	2
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	08/09/2023
Revision Issued Date:	
Reference Documents:	<p>Linked Policies:</p> <ul style="list-style-type: none"> <li>Acceptable Use Policy</li> <li>Access Control Policy</li> </ul> <p>Linked Procedures:</p> <ul style="list-style-type: none"> <li>Access Control Procedure</li> </ul> <p>Linked Records:</p>

### 2.1 DOCUMENT PUBLICATION HISTORY

(All revisions made to this document must be listed in chronological order, with the most recent revision at the bottom)

Version	Date	Author
1	04/05/2023	Bevan Lane
2		Rowan Botha

## 3 PURPOSE AND SCOPE

### 3.1 PURPOSE

FISCAL provides all employees a unique account to identify yourself and provide you access to its assets. This account is for your sole use and should not be shared with any other person.

Due to a global increase of security breaches, phishing and malware attempts, social engineering, and the progressive move towards cloud applications now more than ever the importance of strong and secure credentials can stop breaches and protect FISCAL and its customers.

### 3.2 SCOPE

Password policies are enforced on FISCAL systems and meet the below requirements. Where FISCAL utilises other software or services, wherever possible the use of SSO, MFA and/or these defined requirements should be enforced.

## 4 PASSWORD PROCEDURE

A strong password is an essential barrier against unauthorised access. Unfortunately, this area is often proven to be the weak link in an organization's security strategy and a variety of ways to improve the security of user authentication are available, including various forms of multifactor authentication and biometric techniques.

### 4.1 PASSWORD REQUIREMENTS

The table below outlines password requirements and password recommendations to be considered for all passwords used on FISCAL systems:

PARAMETER	VALUE
Minimum length	14 characters
Password expiry	Every 180 days
Re-use cycle	Passwords cannot be reused, remembering the last 24 passwords
Characters Required	A combination of the below must be used: <ul style="list-style-type: none"> <li>• Uppercase (A through Z) – <b>3</b></li> <li>• Lowercase (a through z) – <b>3</b></li> <li>• Numbers (0 through 9) – <b>3</b></li> <li>• Special Characters (~!@#\$%^&amp;* -+=` \\(){}[]:;'"&lt;&gt;.,?/) – <b>3</b></li> </ul>
Account Lockout	15-minute lockout duration following 10 invalid attempts in a 15-minute window
Multi-factor authentication (MFA) or Single Sign On (SSO)	<ul style="list-style-type: none"> <li>• Must be used where-ever possible.</li> <li>• Required to access the production systems and administration tools</li> </ul>
Password Throttling	<ul style="list-style-type: none"> <li>• This should not allow more than 10 guesses in 5 minutes.</li> <li>• Device locking after more than 10 unsuccessful attempts.</li> <li>• When the vendor doesn't allow you to configure the above, use the vendor's recommended setting.</li> </ul>

## 4.2 PASSWORD RECOMMENDATIONS

To help you with creating a strong password we recommend:

- Use a collection of 3 or 4 memorable words or places grouped with a number or date.
- Use Lyrics or lines from your favourite songs, films, TV shows or books.
- Use memorable quotes.
- Try typing it out a few times before committing to it to ensure it isn't cumbersome to type out.
- Do not use your name or family members names or addresses or anything that would be guessable about you.

Please remember:

- Protect and keep passwords confidential – they should not be disclosed to anyone including I.T or Management and should not be written down.
- If you access systems for personal use, choose a different password from the one(s) used for FISCAL systems.
- If you are prompted by an MFA request that you did not trigger or are unsure of, do not authorise it. If it was triggered by an action you initiated, it will fail to logon or re-prompt.
- If you experience issues, please contact the helpdesk or your line manager and we will work to support you.
- Don't leave your computer logged on and unattended. Anything that happens as your account is your responsibility.