Access Control Procedure

Reference: FPD0090A

Version: 1

Owner: James Pobgee

First Issued Date:

Revision Issued Date:

Prepared for:
All Employees, select Contractors,
Partners and Customers

Prepared by:
James Pobgee

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

2 DOCUMENT CONTROL

Item	Description
Document Title:	Access Control Procedure
Associated Controls:	B.5.17 B.5.18 B.5.2 B.5.3 B.5.4 B.6.3 B.6.5 B.8.2 B.8.3 B.8.5
Reference ID:	FPD0090A
Version:	1
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	08/09/2023
Revision Issued Date:	
Reference Documents:	Linked Policies: • Access Control Policy Linked Procedures: Linked Records:

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		James Pobgee

3 PURPOSE AND SCOPE

3.1 PURPOSE

The purpose of this procedure is to establish guidelines and procedures surrounding access control and to ensure that all users of FISCAL Technologies' information systems have the appropriate level of access to perform their duties while maintaining the confidentiality, integrity, and availability of the organisation’s information assets.

3.2 SCOPE

This policy applies to all employees, contractors, partners, and customers who have access to FISCAL Technologies information systems, whether remotely or on-site. This procedure covers all forms of electronic and physical access, including but not limited to network and system access, data access, and physical access to the organisation's facilities.

4 ACCESS CONTROLS

4.1 BASIC PRINCIPLES

Access control is a critical component of FISCAL Technologies' security posture, and to ensure its effectiveness, we will adhere to a set of basic principles. These principles are designed to establish a strong foundation for access control, and they are based on industry best practices and standards. By implementing these principles, we aim to achieve the following goals:

- Restrict access to sensitive information and systems to only those who require it to perform their job responsibilities.
- Prevent unauthorised access to our systems and data.
- Detect and respond to unauthorised access attempts.
- Ensure that access is provided only in a controlled and auditable manner.

The following basic principles will guide our access control efforts:

- **Least Privilege:** Access to information and systems will be granted only to those individuals who require it to carry out their job responsibilities.
- **Defence in Depth:** Access controls will be implemented in multiple layers, to ensure that if one control fails, there are additional controls in place to provide protection.
- **Need to Know**: Access will be granted only to those individuals who require it to carry out their job responsibilities. Information will be protected by restricting access to those who do not require it for their job responsibilities.
- **Need to Use**: Access will be granted only for the duration required to complete the job responsibility. Access will be revoked when the job is completed or when access is no longer required.

4.2 USER REGISTRATION AND DEREGISTRATION

The registration and deregistration of users is a critical component of access control. All users must be registered to access FISCAL Technologies' systems and services based on their job role and the principles mentioned above. To ensure that only authorised individuals have access to these resources, the following procedures must be followed:

- All user accounts must be registered with FISCAL Technologies' IT department before access is granted. Registration includes the completion of appropriate forms and verification of the user’s identity and need for access.
- When an employee or contractor is terminated, their access to systems and services must be immediately revoked. This includes disabling or deleting the user account and any associated access rights.

- In situations where access must be temporarily revoked, such as during a leave of absence or an extended absence from work, the user's access should be disabled until their return to work.

Access rights must be reviewed bi-annually and updated when required to ensure that users have access to only the information and resources, they need to perform their job responsibilities. Access rights must be removed or adjusted when there is a change in a user's job responsibilities, termination of employment, or if access is no longer required.

4.3 MANAGEMENT OF PRIVILEGED ACCESS RIGHTS

Privileged access rights are reserved for a limited number of individuals who require access to sensitive information or critical systems to perform their job functionalities. As such, management of privileged access rights must be approached with the utmost care and diligence.

The following guidelines must be adhered to when managing privileged access rights:

1. **Identification of Privileged Accounts:** The Technical Information Security Officer (TISO) must identify all privileged accounts and maintain a register of these accounts.
2. **Separation of Duties:** The TISO must ensure that privileged access rights are separated from standard user access rights, such that privileged access is granted only when necessary and revoked promptly when no longer required.
3. **Access Controls:** Access to privileged accounts must be restricted and controlled through a variety of access controls, such as multi-factor authentication, principle of least privilege, and privileged access management tools.
4. **Monitoring and Review:** The use of privileged accounts must be monitored regularly and reviewed at least bi-annually to ensure that access is granted and used appropriately. Any deviations from expected access must be investigated and reported.
5. **Password Management:** Passwords for privileged accounts must be complex and changed regularly. Password sharing must be prohibited, and password management tools must be used where possible.
6. **Training and Awareness:** All personnel with privileged access must receive training on the importance of access control, their responsibilities, and the consequences of non-compliance.

Addition of Privileged Access Rights must be reviewed by IT and approved by the CISO or TISO.

Any violations of privileged access rights must be reported to the CISO / TISO immediately, and remedial actions must be taken promptly. The IT team must also conduct at least a bi-annual review of privileged access rights to ensure that they remain appropriate and necessary.

5 ENFORCEMENT AND VIOLATIONS

5.1 ENFORCEMENT

All divisions & employees of the organisation must comply with the requirements of this procedure. Management is responsible for ensuring that the procedure is implemented within its area of responsibility.

FISCAL Tech expects all users to comply with the terms of this procedure and all other policies, procedures, guidelines, and standards published in its support.

5.2 VIOLATIONS

Violations of this procedure shall result in disciplinary action / legal ramifications by the organisation. Disciplinary action will be consistent with the severity of the incident as determined by an investigation and as deemed appropriate by Management and HR.

Compliance with this procedure will be reviewed by the organisation's Internal Audit Team.