Access Control Policy

Reference: FPD0090-2022

Version: 1

Owner: James Pobgee

First Issued Date:

Revision Issued Date:

To define how access control is governed in order to prevent unauthorised access to FISCAL Technologies' information.

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

FISCAL TECHNOLOGIES

1 CONFIDENTIALITY

Table of Contents

2 DOCUMENT CONTROL

Item	Description
Document Title:	Access Control Policy
Associated Controls:	B.5.15 B.5.16 B.5.17 B.5.18 B.5.2 B.6.4 B.6.5 B.8.2 B.8.3
Reference ID:	FPD0090-2022
Version:	1
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	08/09/2023
Revision Issued Date:	
Reference Documents:	Linked Policies: • Clear Desk and Clear Screen Policy • Information Security Governing Policy Linked Procedures: • Access Control Procedure • Password Procedure 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 policy is to define how access control is governed in order to prevent unauthorised access to FISCAL Technologies' information and protect it from unauthorised disclosure, deletion, or modification.

The organisation shall implement access controls to ensure the Confidentiality, Integrity, and Availability (CIA) requirements of information assets are met based on their value, risk exposure, classification, and regulatory and compliance requirements.

3.2 SCOPE

This policy is applicable to all systems, information processing facilities and personnel, as well as all third-party personnel within the scope of FISCAL Technologies' Information Security Management System.

4 ACCESS CONTROL POLICY

4.1 LOGICAL ACCESS CONTROL MANAGEMENT

Logical access to information shall be restricted to authorised users only. The following security controls shall be used to manage access to all information assets:

1. Access controls shall be managed by a defined process on the principle of *'deny all unless explicitly permitted'* and on a least privilege basis.
2. Accesses for highly privileged roles and conflicting areas of responsibility shall be sufficiently segregated.
3. Relevant legislation and contractual obligations regarding limitation of access to data or services shall be taken into consideration when assigning access.
4. Unique user IDs shall be in place for users to be personally identified with secure authentication controls in place (i.e., a password or passphrase; token device or smart card; or biometrics).
5. Users shall protect their ID's and passwords through secure behaviour including never writing down or sharing details and changing the authentication details whenever there is any indication of possible compromise.
6. Privileged rights shall have additional controls implemented so that their allocation and usage is restricted and controlled. These rights shall be monitored for unauthorised access and abuse.
7. Privileged access rights shall be limited to a defined time where possible and reviewed regularly (at least bi-annually) to ensure that this access is still required.
8. There shall be a process in place to periodically identify redundant user IDs and disable and then remove. They will not be issued to other users.
9. The access rights to information and information processing facilities shall be maintained to ensure timely adjustment and reallocation of access rights upon change of role, termination of employment or contract.
10. The asset owner or designated parties shall review all user access rights at regular intervals (at least bi-annually) or after any user role changes or on termination.

4.2 ACCESS TO NETWORKS AND NETWORK SERVICES

1. Access to the network and network services shall also be restricted on a least privilege basis and follow the formal access control process.
2. Remote access shall have strong authentication controls in place (i.e., multi-factor authentication) with monitoring and logging and monitoring controls in place.

4.3 SYSTEM AND APPLICATION ACCESS CONTROL

1. System or application access management controls shall be designed to minimise the opportunity for unauthorised access and ensure the minimum disclosure of information within the system or application.
2. Application password management systems shall be interactive, ensure unique and quality passwords and prevent the use of brute force attacks.

5 ENFORCEMENT AND VIOLATIONS

5.1 ENFORCEMENT

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

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

5.2 VIOLATIONS

Violations of this policy 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 policy will be reviewed by the organisation’s Internal Audit Team.