Physical & Environmental Security Policy

Reference: FPD0110-2022

Version: 1

Owner: James Pobgee

First Issued Date:

Revision Issued Date:

To outline FISCAL Technologies' physical and environmental security requirements for the protection of the information and the related assets.

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:	Physical & Environmental Security Policy
Associated Controls:	B.5.2 B.5.30 B.6.4 B.7.1 B.7.11 B.7.2 B.7.3 B.7.4 B.7.5 B.7.6 B.7.8 B.8.15
Reference ID:	FPD0110-2022
Version:	1
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	25/09/2023
Revision Issued Date:	
Reference Documents:	Linked Policies: • Information Security Governing 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 policy is to mandate the physical and environmental security requirements for the protection of the information and the related assets of FISCAL Technologies. The objective is to prevent unauthorised physical access, damage and interference to the organisation's information and facilities.

3.2 SCOPE

This policy covers the security and integrity of the physical perimeter and internal locations within the scope of FISCAL's Information Security Management System, by considering the physical, electronic, and human elements. It also specifies the proactive and reactive approach towards environmental security.

4 PHYSICAL SECURITY POLICY

4.1 PHYSICAL PERIMETER SECURITY

The physical perimeters shall be defined, and controls implemented to protect the organisation from unauthorised access and environmental threats.

- Perimeters shall be secured through relevant physical controls (i.e., walls, secure access-controlled doors, alarms, security, and protected windows) and only authorised parties are allowed access into the locations.
- All doors shall be equipped with automatic locking mechanisms, which may include proximity cards, biometrics, or a combination thereof. Where such types of mechanism are not present, key-lock systems should be implemented with control and management of the keys.
- Offices shall be protected by adequate perimeter controls as above and where possible internally offices segmented with doors locked, camera systems and alarms after hours enabled.
- Entry to the data centre(s) and other sensitive computing facilities shall require strong access controls (i.e., biometrics, dual factor authentication, authorisation) and access information shall be logged and stored securely.
- The monitoring of the building entrances is the responsibility of the security personnel unless outsourced to an appropriate third party. The building shall be monitored through a real-time camera system with its footage being recorded and securely stored for at least 3 months.

4.2 PHYSICAL ACCESS CONTROL

- Physical access to the organisation's premises shall be controlled appropriately through a formal access control process.
- All sites where computers and other information assets are located shall be protected from theft, unauthorised access, and other human threats.
- All physical access to and movement of information assets shall be monitored, the details securely stored and reviewed.
- Secure areas shall be protected with a combination of access controls, equipment access logging, equipment activity monitoring and security guards.
- Physical access controls shall be authorised, regularly reviewed, and updated, based on the criticality of the information system.
- Visitors' access must be recorded either via the fobbing system or via the physical logbook on each site to record when they entered and left the premises.
- Every individual is responsible for questioning and verifying the identity of unfamiliar persons or visitors when they are not under the supervision of a FISCAL employee. If necessary, they should notify a senior person on-site to ensure proper documentation or escort the individual off-site. Any security breaches must be promptly reported through the helpdesk.
- Visitors' access to secure areas shall only be allowed if they are supervised and their access is monitored and securely controlled and they are clearly identified (e.g., visitor badges, stickers etc.).
- Physical access to FISCAL's data centre shall be authorised based on the need, logged, and monitored continuously.
- Physical access rights shall be revoked immediately upon termination / resignation of employees or completion of a consultation or supplier agreement.

4.3 EQUIPMENT SECURITY

- All hardware and software assets held by FISCAL Technologies shall be held on hardware register.

- No alteration to the hardware configuration of the system may take place without the permission of the Director of IT and Security. Under no circumstances are modems, mobile-dongles, or other communication devices to be attached to any internal systems excluding (Laptops / Desktops).
- The use of external data devices, such as USB storage or hard drives, may not be attached to FISCAL's hardware unless the device has been provided or approved by FISCAL's IT or has been virus scanned.
- Maintenance agreements are in place with approved vendors to ensure the ongoing support of FISCAL's Hardware, Internet, and Networking equipment.
- A detailed record of faults is recorded on the Helpdesk and is to be reviewed at regular intervals by CISO or TISO.
- Only approved systems engineers and FISCAL's IT staff will be allowed access to hardware or software and such access is recorded.
- No remote diagnosis or repair services are permitted unless explicitly approved by the Director of IT and Security and supplied by our approved vendors under the existing maintenance / support agreements. A record of all such diagnosis and repair must be recorded via the helpdesk.
- Computer hard discs are not to be removed from FISCAL premises without the written permission of CISO, TISO, Director of IT and Security or a board member.
- The disposal of any storage media is subject to specific security control. Simple deletion of files is not adequate and the advice of a member of IT is to be sought before any disposal / destruction of media via the helpdesk.
- Specific work instructions for secure destruction of data must be followed.

4.4 SUPPORTING UTILITIES

- Data centre and other critical equipment shall be protected from power failures and electrical anomalies. This includes un-interruptible power supply (UPS) and backup power generating equipment. Contingency plans shall describe in detail the action to be taken in case of a continued power outage.
- Power supply backup equipment including UPS's, backup generators etc. shall be subject to regular maintenance and testing as per the manufacturer's specifications. Maintenance records shall be kept for future reference.

5 ENVIRONMENTAL SECURITY POLICY

- FISCAL's premises and data centres shall be protected from natural, manmade and environmental threats and disasters through environmental controls (i.e., fire detection, air conditioners, monitoring systems).
- The temperature and humidity in the data centre and other information processing areas shall be controlled, monitored, and maintained using adequate air and humidity controlling equipment.
- All premises (including secure areas) shall have an emergency evacuation plan along with clearly marked secure emergency exit doors.
- The environmental security equipment shall undergo regular maintenance as per the manufacturer's recommendations and records kept.
- The environmental security equipment shall undergo regular tests (once per year at least) and test results shall determine the efficiency and adequacy of such equipment.
- Hazardous and combustible materials shall be stored at a safe distance from the data centre, server rooms and equipment rooms.
- Eating and drinking inside server rooms is strictly prohibited.

6 ENFORCEMENT AND VIOLATIONS

6.1 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.

6.2 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.