Clear Desk and Clear Screen Policy

Reference: FPD0112-2022

Version: 12

Owner: Lesley (new) Reeve

First Issued Date:

Revision Issued Date:

To ensure FISCAL Technologies' information is not exposed to unauthorised access and to reduce the risk of an unauthorised person using the information, accessing the internet, or sending emails on behalf of another person, in direct contravention of the Information Security Policy.

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

Prepared by:
Lesley (new) Reeve

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:	Clear Desk and Clear Screen Policy
Associated Controls:	A.11.2.9 B.5.15 B.5.2 B.6.4 B.7.7
Reference ID:	FPD0112-2022
Version:	12
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	08/09/2023
Revision Issued Date:	
Reference Documents:	Linked Policies: • Access Control Policy • 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
11	09/12/2022	Lesley (new) Reeve
12		Lesley (new) Reeve

3 PURPOSE AND SCOPE

3.1 PURPOSE

The purpose of this policy is to outline the FISCAL Technologies' policy for clear desk and screens, to ensure the security and confidentiality of papers, removable storage media and information processing facilities.

The purpose of the policy is to ensure that information is not exposed to unauthorised access and to reduce the risk of an unauthorised person using the information, accessing the internet, or sending emails on behalf of another person, in direct contravention of the Information Security Policy.

3.2 SCOPE

This policy is applicable to all FISCAL Technologies' permanent, temporary, or contracted staff employed by FISCAL, and to third parties who can access information under supervision.

Note that in this document Clear Desks refer to confidential or other sensitive information only. It does not mandate that desks are clear of personal artefacts or other items, so long as such items are not offensive and do not interfere with business activities.

The tenets of this policy apply to remote working locations, including homeworking, as well as working within a FISCAL office.

All staff are responsible for monitoring their compliance with the principles and procedures detailed in this policy; departmental managers and supervisors should also monitor compliance on a regular basis. All staff must be made aware of these principles at induction.

4 CLEAR DESK

Clear Desk refers to confidential or other sensitive information only. It does not mandate that desks are clear of personal artefacts or other items, so long as such items are not offensive and do not interfere with business activities.

- It is policy that where possible confidential information should not be printed.
- When confidential information must be printed it should be retrieved from the printer immediately. When available the Secure Print facility should be used.
- Where practical, paper, and digital media holding confidential information should be stored in suitable locked safes, cabinets, or other forms of security furniture when not in use, especially outside working hours.
- Each team has access to one or more item of lockable security furniture. It is each employee's responsibility to identify the appropriate location and ask for guidance from line management if the location is not clear.
- It is good practice to lock all office areas when they are not in use.
- Any visitor books should be stored out of sight when not in use.
- The reception desk should always be kept as clear as possible, confidential records or other personally identifiable information should not be held on the desk within reach/sight of visitors.
- Personal items (i.e., keys, handbags, wallets etc.) should be stored safely in the interests of security. It is the responsibility of the owner to ensure all security precautions are taken.

5 CLEAR SCREEN

- Computers must not be left logged on when unattended and should be password protected.
- Computer screens should be angled away from the view of unauthorised persons.
- The Windows Security Lock should be set to activate when there is no activity for a short pre-determined period.
- The Windows Security Lock should be password protected for reactivation.
- When leaving computers unattended users should lock their machines.
  This is quickly and easily done by holding the Windows key and pressing L.
- Users should shut down machines at the end of the workday unless long running processes require the system to be left active. In this case the machine should be locked.

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.