Risk Management Policy

Reference: FPD0018-2022

Version: 12

Owner: Lesley (new) Reeve

First Issued Date:

Revision Issued Date:

To outline FISCAL Technologies' approach to risk management for security threats.

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:	Risk Management Policy
Associated Controls:	10.1 6.1 6.1.1 6.1.2 6.1.3 8.2 8.3 B.5.2 B.5.4 B.6.4
Reference ID:	FPD0018-2022
Version:	12
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	20/10/2023
Revision Issued Date:	
Reference Documents:	Linked Policies: • Information Security Governing Policy Linked Procedures: • Risk Management Procedure Linked Records: • ISMS Scope

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
9	09/12/2022	James Pobgee
10	09/12/2022	James Pobgee
12		James Pobgee

3 PURPOSE AND SCOPE

3.1 PURPOSE

The purpose of this policy is to define the principles managing how FISCAL Technologies identifies potential information security threats to the organisation, minimises their impact and effectively monitors and evaluates the risk management strategy.

3.2 SCOPE

This policy is applicable to all information and IT assets (including networks, systems, and infrastructure), information processing facilities, personnel as well as all third-party personnel within the scope of FISCAL Technologies' Information Security Management system.

4 RISK MANAGEMENT POLICY

Information Security Risk Management (ISRM) is the process of continuously identifying, assessing, evaluating, and treating risks related to the organisation's information.

4.1 POLICY STATEMENTS

1. The risk management methodology shall be designed and approved by CISO / TISO in collaboration with the ELT, who shall identify the people within FISCAL Technologies responsible for risk assessment operations.
2. FISCAL Technologies shall define the following requirements:
    a. How to identify the risks that could impact confidentiality, integrity and/or availability of information.

    b. Identification of the risk owners.

    c. Criteria for assessing impact and the likelihood of the risk.

    d. How the total risk will be calculated.

    e. Criteria for accepting risks.

    f. How to achieve continual improvement.
3. The risk assessment process shall consider likelihood and impact of risks in terms of time, scale of damage and recovery period.
4. The risk assessment process shall identify, quantify, and prioritise risks against criteria and objectives relevant to the organisation, including critical resources, impacts of disruptions, allowable outage times and recovery priorities.
5. Based on the results of the assessment and after obtaining the risk owner's approval, the risk treatment plan shall be outlined to determine which controls will be implemented and acceptance of the residual information security risks.
6. The development, implementation and execution of remediation programs are the joint responsibility of Management, the IT infrastructure management team, and the department responsible for the systems / areas being assessed.
7. Employees are expected to co-operate fully with risk assessments on assets or systems for which they are held accountable and in the development of a remediation plan.

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.