Information Security Governing Policy

Reference: FPD0010

Version: 23

Owner: Lesley (new) Reeve

First Issued Date: 09/05/2023

Revision Issued Date: 09/05/2023

To outline FISCAL Technologies' Information Security Policies, responsibilities, and governance associated with the security of FISCAL Technologies and its 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

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:	Information Security Governing Policy
Associated Controls:	5.1 5.2 A.18.2.2 A.5.1.1
Reference ID:	FPD0010
Version:	23
Status:	Published
Approver:	
Approval Date:	
First Issued Date:	09/05/2023
Revision Issued Date:	09/05/2023
Reference Documents:	Linked Policies: • Acceptable Use Policy • Asset Management and Information Classification Policy • Business Continuity Management Policy • Change Management Policy • Clear Desk and Clear Screen Policy • Risk Management Policy Linked Procedures: • Business Continuity Management Procedure • Communications Procedure • Documents and Records Management Procedure • Incident Management Procedure • Internal Audit Programme Procedure • Malware Protection Procedure • Management of Non-Conformities and Corrective and Preventative Action Procedure • Management Review Procedure • Monitoring and Measurement Procedure • Operating Procedures • Patch Management Procedure • Risk Management Procedure • Task Schedule Procedure Linked Records: • Information Security Objectives Plan • Internal Audit Report Template • ISMS Scope • Roles, Responsibilities, Training and Competence

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
20	10/11/2022	James Pobgee
21	07/12/2022	James Pobgee
22	05/05/2023	James Pobgee
23	09/05/2023	James Pobgee

3 RESPONSIBILITIES

3.1 EVERYONE

Everyone at FISCAL Technologies (the "Company") and its subsidiaries are responsible for looking after the Company's assets which includes our information, data, and business security. This policy provides a framework within which FISCAL may handle information and data in the most secure way given the demands of the business and our customers.

FISCAL Technologies is committed to protecting its employees, partners, clients, and itself from damaging acts that are intentional or unintentional. Security is critical and requires participation and support of every FISCAL user that interacts with data and information systems.

It is the responsibility of everyone to know and understand these policies and to conduct their activities accordingly.

Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data FISCAL Technologies controls:

- CONFIDENTIALITY – Preserving restrictions on information access and disclosure so that access is limited to authorised users and services.
- INTEGRITY – The concern that sensitive data has not been modified or deleted in an unauthorised and undetected manner.
- AVAILABILITY – Ensuring timely and reliable access to and use of information.

All users are required to:

- Understand this policy and put it into regular practice.
- Remember that all employees and contractor staff that have been trusted with Company Information and resources are expected to use them as intended.
- Raise any doubts about what is expected with your Line Manager or the I.T. Department.
- Take ownership and report any risks to our Information or Systems to your Line Manager or the I.T. Department.

3.2 FISCAL LEADERSHIP

The FISCAL Technologies Executive Leadership Team has the objective to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. Ensuring the ISMS programme must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

The FISCAL Technologies Board has assigned the COO overall responsibility for:

- Ensuring that the ISMS conforms to the requirements of ISO27001:2013
- Development and dissemination of IS Standards within FISCAL Technologies
- Reporting on the performance of the ISMS
- Electing members of the IS Forum and chairing meetings

COO may choose to delegate some or all these responsibilities from time to time to the Chief Information Security Officer (CISO), Technical Information Security Officer (TISO) or to others as appropriate.

At current the role of COO is assuming all responsibilities comparable to those of CISO.

FISCAL Technologies allocates role of Technical Information Security Officer (TISO) to the Head of IT to ensure proper technology risk considerations are addressed at each phase and provide proactive solutions to correct exposures or mitigate risk. They are responsible for interpreting procedures, and guidelines for multiple platforms and environments in designing solutions, recommending enhancements, or defining mitigating controls to existing systems.

3.3 INFORMATION SECURITY OFFICER

CISO and TISO act as Information Security Officers for FISCAL and shall:

- Develop and manage the FISCAL information security programme.
- Lead and work with the Information Security Forum to receive feedback from the wider business on matters pertaining to Information Security. Use this feedback to further the aims of the security strategy.
- Develop, issue, and maintain the IT security strategy and Policy.
- Orchestrate the development of a Business Continuity Plan with business leaders and advise the business on its implementation.
- Create an information security awareness programme to include briefings, training, and education.
- Provide information security consulting support to the business.
- Investigate breaches of security and report findings and recommended action to the business.
- Implement a compliance programme to evaluate the effectiveness of the information security programme.
- Report to the board on the effectiveness of the overall information security programme.

3.4 INFORMATION SECURITY FORUM (ISF)

The purpose of the ISF is to:

- Monitor the exposure of the company information to major business risks.
- Review the Security Policy and ISF responsibilities.
- Review security incidents and take appropriate action.
- Discuss recommendations for improvement to be submitted to enhance the ISMS including policy changes and training updates, etc.

The ISF shall meet 4 times a year to facilitate business-wide feedback on the Information Security Policies and to highlight any concerns regarding the implementation of same.

4 SCOPE OF POLICY

4.1 SCOPE DEFINITION

FISCAL has taken the decision to implement an Information Security Management System (ISMS) to protect the confidentiality, integrity, and availability of its information assets. To meet legal and professional requirements and satisfy obligation to our customers FISCAL must use cost effective security measures to safeguard its and its customer's information resources. This Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

The scope of the ISMS is:

The provision of a global web-based Procure-to-Pay (P2P) risk management solution management platform, including the provision of a SaaS, subscription-based platform for global clients, focussing on solutions to mitigate procure-to-pay-risks such as fraud, anomalies, duplication found within payment transactions and Master Supplier data.

4.2 REQUIREMENT

To meet legal and professional requirements and satisfy obligation to our customers FISCAL must use cost effective security measures to safeguard its and its customer's information resources.

This Policy will ensure a consistent approach to the implementation of appropriate security controls against common threats.

4.3 POLICY

The Policy of FISCAL is to accept willingly all obligations in respect of information security and to protect its information resources by implementing recognised best practices that will achieve a balance between cost and risk.

4.4 APPLICABILITY

The Policy shall apply to all employees, contractors and any other parties using FISCAL resources. Further it shall apply to those third parties providing hosting services to FISCAL or, by nature of a sub-contract, FISCAL customers.

4.5 IMPLEMENTATION

The requirements of the Policy shall be implemented by all employees, contractors and any other parties using FISCAL resources. Further it shall be implemented by those third parties providing hosting services to FISCAL or, by nature of a sub-contract, FISCAL customers.

Any member of staff noting any area of conflict between this Policy and any other company Policy must bring it to the attention of the Chief Information Security Officer (CISO) or Technical Information Security Officer (TISO) immediately for conflict resolution. The CISO/TISO will in any case be responsible for the routine periodic review of the Policy.

Internal audit shall undertake independent reviews to assess the adequacy of implemented security measures including compliance with the Policy.

Compliance with the Policy is the duty of all employees, contractors and any other parties using FISCAL resources. In serious cases, failure to comply with the Policy may be a disciplinary matter and could also result in a breach of the law or a criminal offence.

FISCAL staff and contractors have an obligation to report suspected breaches of the Policy immediately to CISO/TISO.

In the case of a breach or suspected breach that could affect the security of customer data CISO, TISO or member of the Executive Leadership Team is to notify the customer without delay.

4.6 INFORMATION ASSETS

The Policy applies to all information whether spoken, written, printed or computer-based, which is owned, held in the custody of, or used by FISCAL.

The Policy also applies to all resources used in creating, processing, transmitting, storing, using, or controlling that information.

5 OBJECTIVES OF THE POLICY

The objectives of the Policy are to ensure that:

- Security Controls are implemented in line with current recommended practices.
- Business continuity controls are in place and assessed regularly.
- Security risks are properly identified, assessed, recorded, and managed.
- Information and equipment are protected against threats, and accidental or malicious damage.
- Security education and training will be provided to all staff as appropriate to their assessed needs.

These objectives shall be achieved through the implementation of security controls as described in the remaining sections of this Policy and the Information Security Objectives Plan supports the ongoing monitoring of these goals.

Reference: Refer to ***Information Security Objectives Plan.***

6 HUMAN RESOURCE SECURITY

6.1 PRIOR TO EMPLOYMENT (WHEN RECRUITING PERMANENT EMPLOYEES, CONTRACTORS, OR TEMPORARY STAFF)

All authorised personnel that are recruiting staff are responsible for ensuring that:

- All background / security checks should be carried out in accordance with relevant laws, regulations, and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.
- The contractual agreements with employees and contractors should state their and their supporting organisation's responsibilities for security.
- All relevant policies have been provided, reviewed, and signed prior to access rights being granted to employees or contractors.

6.2 DURING EMPLOYMENT / RELATIONSHIP WITH FISCAL

All FISCAL personnel are responsible for ensuring that:

- Proper control and security procedures operate within their authorised areas.
- The protection of assets provided, including data and hardware.
- Procedures embodied in this document and associated policies are enforced.
- Security processes and policies are implemented to their associated areas.
- Security processes, policies and access are reviewed on a periodic basis.
- Security education and training is provided to all staff as appropriate to their assessed needs.
- The Company's business is protected against fraud and misuse of information in connection with computer-based systems.

- The authorised systems and information allocated are used in accordance with the procedures in this document and associated policies.
- Every recipient of information is responsible for the security of that information.
- Compliance with Local law, GDPR, and company compliance standards (ISO and Cyber Essentials).

All FISCAL employees are responsible for ensuring that in event of change of role for employees reporting to them that they advise HR and I.T:

- Request a review / change of access for the employee.
- Request a review / change of any assets that the employee is responsible for.
- Request any relevant assets that are required for the new role.

The I.T. Department will monitor the operation of security procedures, and physically action security changes for central systems they are responsible for or inform system owners where required. Security of data is everyone’s responsibility.

Individual Departmental Managers are responsible for the operation and review of procedures to provide secure access to department systems managed by them (for instance H.R., Finance or Marketing systems).

6.3 TERMINATION AND CHANGE OF EMPLOYMENT

All FISCAL personnel are responsible for ensuring that in case of termination of employment of any employee they:

- Notify HR of ALL Leavers Temporary/Contract/Fixed Term/Permanent staff, to ensure access to systems can be removed.
- Return all assets back to I.T. or the relevant asset owners.
- Acquire and return Access Cards/fobs to I.T. or HR.
- Request termination of access to information systems.
- Retrieve all security-related organisational information system property and organisational information formerly controlled by terminated individual.
- Where access to a Leaver’s Email/Mailbox and data is required, a request for authorisation should be provided to the H.R. Department, who will provide approval for access and liaise with the I.T. Department to provide the privileged access.

6.4 SEGMENTATION OF ROLES

Security roles are segregated into:

- Designing and implementing security responsibilities
- Testing security, conducting security audits, or monitoring and reporting on security.

Responsibilities are assigned to individuals to establish:

- Checks and balances within the system.
- Minimise the opportunity for unauthorised access and fraud.
- Ensure separation between the development, operation and testing of security and all controls.
- Auditing compliance levels are upheld.
- Departments are structured so they are only able to make changes/amendments in their own areas. They do not have permissions outside these areas.

7 VIOLATIONS

Any FISCAL user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violation of local and/or international law will be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Any person employed by a contractor or any other entity that engages in misuse or inappropriate use of any resources provided by the FISCAL will be reported to the contracting company and may result in removal from any Company assignment.

8 MONITORING, MEASUREMENT, ANALYSIS AND EVALUATION

The following sources of information will be used to evaluate information security performance and the effectiveness of the information security management system. It shall be the responsibility of the CISO and TISO to ensure that appropriate evidence of monitoring, measurement, analysis, and evaluation are available:

- The effectiveness and degree of compliance with information security controls as monitored through internal audits, external audits, and penetration testing – all of which will be conducted on at least an annual basis.
- Number of security incidents, breaches, and vulnerabilities – all of which will be monitored proactively and reported upon at least quarterly.
- Degree of compliance with appropriate legislative requirements – which will be monitored at least annually.
- Adherence to security management controls such as patch management schedules, antivirus, and malware updates.

All of the above sources of information will be analysed and evaluated at the Management Review Meeting and also at other internal management and information security forum meetings.

9 CONTINUAL IMPROVEMENT

The CISO, TISO in conjunction with the Management Team will be responsible for ensuring that the suitability and effectiveness of the Information Security Management System are continually improved, this will be achieved via:

- Information security forums.
- Management review meetings.
- Risk assessments and risk treatment plans.
- Identification and resolution of non-conformities.
- Feedback/suggestions from staff and other interested parties.
- Technological advancements.
- Internal and external audit findings.

10 POLICY REVIEW

This Policy is to be reviewed on an annual basis by the Executive Leadership Team to take account of changing circumstances, legislation, technology, and security risks.

Any revisions to the Policy are to be approved by the Executive Leadership Team prior to implementation.

11 LEGAL OBLIGATIONS

11.1 GENERAL

FISCAL accepts its obligations to comply with the laws of the United Kingdom. All members of the team must be aware that there are legal requirements relating to information that must be met.

The principles of these are detailed below.

11.2 DATA PROTECTION ACT 2018

This legislation updates the previous UK Data Protection Act and enshrines the General Data Protection Regulations (GDPR) into UK law. It places obligations on those who record and use personal data and the organisation for which the work.

CISO/TISO is responsible for registration matters with the Office of the Data Protection Registrar, application of the Data Protection Principles and the briefing of all Data Users within the team.

11.3 PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS (PECR)

The e-privacy Directive complements the general data protection regime and sets out more specific privacy rights on electronic communications. It adopts the GDPR definition of 'consent' and provides rights to individuals regarding the data stored about them for tracking or marketing purposes including the requirement for explicit consent for the data to be held and the right for the data to be deleted.

11.4 SOFTWARE COPYRIGHT

Software is protected by the Copyright, Designs and Patents Act 1988, which state that 'the owner of the copyright has the exclusive right to copy the work'.

It is illegal to make copies of software without the owner's permission. Penalties include unlimited fines and up to two years in prison.

11.5 COMPUTER MISUSE ACT

The Computer Misuse Act 1990 established three prosecutable offences against unauthorised access to any software or data held on any computer.

The offences are:

- Unauthorised Access to Computer Material
- Unauthorised Access with intent to commit or facilitate the commission of further offences
- Unauthorised Modification of Computer Material

ANNEX A - INFORMATION SECURITY POLICIES

FISCAL Technologies' Information Security Policy is supported by additional policies which address the specific requirements of information security areas and form the base of a robust information security posture across the organisation.

1. Risk Management Policy

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

Reference: Refer to ***Risk Management Policy***.

2. Acceptable Use Policy

The purpose of this policy is to outline the requirements and acceptable use of FISCAL Technologies's information and IT assets.

Reference: Refer to ***Acceptable Use Policy***.

3. Asset Management and Information Classification Policy

The purpose of this policy is to outline FISCAL Technologies's asset management processes, including the classification of information to establish the appropriate levels of protection for assets.

Reference: Refer to ***Asset Management and Information Classification Policy****.*

4. Access Control Policy

The purpose of this policy is to prevent unauthorised access to FISCAL Technologies's information in order to protect it from unauthorised disclosure, deletion, or modification.

Reference: Refer to ***Access Control Policy***.

5. Secure Development Policy

The purpose of this policy is to ensure that information security controls are designed and implemented within FISCAL Technologies's software and system development lifecycle and in accordance with industry standards.

This policy sets out the principles to be followed during the software development lifecycle to manage the risks related to threats such as cyber-attacks to the organisation.

Reference: Refer to ***Secure Development Policy***.

6. Supplier Security Policy

The purpose of this policy is to protect FISCAL Technologies's information assets that are accessible to or affected by suppliers through the deployment of adequate and appropriate supplier-related security controls.

Reference: Refer to ***Supplier Security Policy***.

7. Incident Management Policy

The purpose of this policy is to design and implement a consistent and effective incident management process to ensure the timely and appropriate response to actual or attempted incidents and security breaches.

Reference: Refer to ***Incident Management Policy***.

8. Business Continuity Management Policy

The purpose of this policy is to define the objectives and rules for business continuity management. Business continuity management aims to identify possible threats to critical assets and processes in the organisation and the impact they may have on its operations, implementing a framework of organisational resilience, plans and actions to effectively respond.

Reference: Refer to ***Business Continuity Policy***.

9. Mobile Device Policy

The purpose of this policy is to ensure that the information stored on mobile devices is securely managed and protected and that the risks of working with mobile devices in unprotected environments are managed.

Reference: Refer to ***Mobile Device Policy***.

10. Information Management Policy

The purpose of this policy is to ensure that information transfers take place via secure, authorised mechanisms and that sensitive information is protected from unauthorised access or disclosure.

Reference: Refer to ***Information Management Policy***

11. Physical and Environmental Security Policy

The purpose of this policy is to mandate the physical and environmental security requirements for the protection of the information and related assets of FISCAL Technologies. The objective is to prevent unauthorised physical access, damage and interference to the organisation's information and facilities.

Reference: Refer to ***Physical & Environmental Security Policy***

12. Change Management Policy

The purpose of this policy is to establish management direction and high-level objectives for change management and the related controls. To ensure that changes to information resources are managed and executed according to a formal change control process.

Reference: Refer to ***Change Management Policy***

13. Network Security Policy

The purpose of this policy is to provide guidance on the network management controls which shall be implemented to protect FISCAL Technologies's network, network devices, computers etc., from unauthorised access, misuse, malfunction, modification, destruction, or improper disclosure from within the organisation or outside.

Reference: Refer to ***Network Security Policy***

14. Encryption Policy

The purpose of this policy is to ensure proper and effective use of cryptography controls to protect the confidentiality, authenticity and/or integrity of information.

Reference: Refer to ***Encryption Policy***