Encryption Policy

Reference: FPD0101-2022

Version: 1

Owner: James Pobgee

First Issued Date:

Revision Issued Date:

To outline the rules for the use of encryption technologies to protect the confidentiality, integrity, and availability of FISCAL Technologies systems and data.

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

1 CONFIDENTIALITY 1

2 DOCUMENT CONTROL 2

2.1 DOCUMENT PUBLICATION HISTORY 2

3 PURPOSE AND SCOPE 3

3.1 PURPOSE 3
3.2 SCOPE 3

4 ROLES AND RESPONSIBILITIES 3

5 ENCRYPTION POLICY 3

5.1 ENCRYPTION REQUIREMENTS 3
5.1.1 Data encryption 3
5.1.2 Encryption key management 3
5.2 ENCRYPTION IMPLEMENTATION 4
5.2.1 Encryption for personal & mobile devices 4
5.2.2 Email encryption 4
5.2.3 Third party encryption 4
5.3 INCIDENTS 5
5.4 COMPLIANCE 5

6 ENFORCEMENT AND VIOLATIONS 5

6.1 ENFORCEMENT 5
6.2 VIOLATIONS 5

2 DOCUMENT CONTROL

Item	Description
Document Title:	Encryption Policy
Associated Controls:	5.3 B.5.10 B.5.12 B.5.14 B.5.15 B.5.2 B.5.26 B.5.3 B.5.31 B.5.33 B.6.4 B.8.1 B.8.20 B.8.24 B.8.26 B.8.3
Reference ID:	FPD0101-2022
Version:	1
Status:	Draft
Approver:	
Approval Date:	
First Issued Date:	20/07/2023
Revision Issued Date:	
Reference Documents:	Linked Policies: • Acceptable Use Policy • Information Security Governing Policy • Mobile Device 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 Encryption Policy is to outline the rules for the use of encryption technologies to protect the confidentiality, integrity, and availability of FISCAL Technologies systems and data. This policy is intended to ensure that encryption is used appropriately and consistently throughout the organisation, and that all encryption controls are managed and monitored effectively.

3.2 SCOPE

This policy applies to all FISCAL Technologies employees, contractors, vendors, and any other individuals or entities that have access to FISCAL Technologies systems and data. All encryption technologies used to protect FISCAL Technologies systems and data must adhere to the standards and guidelines outlined in this policy. This policy also applies to any encryption technologies used by third-party vendors or service providers on behalf of FISCAL Technologies.

4 ROLES AND RESPONSIBILITIES

Technical Information Security Officer (TISO): The TISO is responsible for overseeing the implementation and compliance of cryptographic controls within the organization.

Senior Infrastructure Engineers and Lead Developers: The Senior Engineers are responsible for the day-to-day management and enforcement of cryptographic controls.

System Administrators and Developers: System administrators and developers are responsible for configuring and maintaining cryptographic mechanisms on systems and applications.

5 ENCRYPTION POLICY

5.1 ENCRYPTION REQUIREMENTS

The following requirements outline the use of encryption throughout FISCAL Technologies:

5.1.1 Data encryption

All sensitive and confidential data at rest and in transit will be encrypted using approved encryption methods to ensure confidentiality, integrity, and availability.

- **Data at rest:** All data stored on servers, databases, or other storage devices will be encrypted. Encryption must be applied to the entire disk or storage device, rather than individual files or folders. All data shall be encrypted using secure encryption algorithms based on sensitivity of the data it is securing e.g., AES256.
- **Data in transit:** All data transmitted over public networks, wireless networks, or any other network that is not under direct control of FISCAL Technologies must be encrypted using secure protocols, such as SSL/TLS v1.3. Secure key exchange mechanisms (e.g., Diffie-Hellman) shall be used to establish encryption keys during communication.

5.1.2 Encryption key management

Encryption Key Management at FISCAL Technologies will be conducted according to best practices and in adherence to the rules and steps outlined. This ensures the protection of encryption keys, their proper distribution, periodic updates, and secure retirement when necessary. The key points to be considered are as follows:

- **Key generation:** Cryptographically secure random number generators must be used to generate encryption keys of sufficient strength. The key length must be appropriate for the level of data protection required. Only approved algorithms must be used.

- **Key Storage:** Encryption keys shall be stored securely; separate from the encrypted data they protect. Keys must be protected against unauthorised access and disclosure.
- **Key distribution:** Encryption keys must be distributed through secure communication channels or delivered physically in a secure manner. Distribution must be limited to authorised individuals with a legitimate need for access.
- **Key usage:** Encryption keys must be used solely for their intended purpose and protected from unauthorised access, modification, or deletion. They must be securely stored with strong encryption and access controls with regular updates or rotations maintaining their effectiveness.
- **Key backup and recovery:** Encryption keys must be backed up and securely stored to enable recovery in the event of key loss or destruction. Backup keys will be stored separately from primary keys, using strong encryption and access controls. Regular testing must occur to ensure their effectiveness.
- **Key retirement and destruction:** Encryption keys must be retired when no longer needed or at the end of their useful life. Retired keys must be securely destroyed to prevent unauthorised access or use.
- **Key management audit:** Annual audits must be conducted to ensure compliance with organisational policies and industry standards. Key management activities must be documented, and regular reviews of key management logs be performed to identify any unauthorised or suspicious activity.

5.2 ENCRYPTION IMPLEMENTATION

5.2.1 Encryption for personal & mobile devices

All personal and/or mobile devices used by FISCAL Technologies employees to process or store organisational data must have encryption enabled and comply with the requirements set out in the **Mobile Device Policy**.

The IT team is responsible for ensuring encryption on all mobile and personal devices and meeting the specific standards and requirements. Third-party encryption applications used on mobile devices must be approved by the IT department and evaluated for compatibility.

Please refer to the **Mobile Device Policy** for detailed instructions.

5.2.2 Email encryption

FISCAL Technologies must ensure that all emails containing sensitive or confidential information are encrypted both in transit and at rest, following industry best practices. The highest standards of encryption will be applied to safeguard the confidentiality and integrity of the information transmitted.

5.2.3 Third party encryption

Any use of third-party encryption software or services must be approved by the CISO or TISO and the IT Department. When evaluating third-party encryption solutions, the following criteria must be considered:

- The strength and reliability of the encryption algorithm
- The trustworthiness and reputation of the vendor
- Compliance with relevant laws and regulations
- Compatibility with FISCAL Technologies' existing encryption infrastructure
- Ease of use and manageability
- Availability of support and maintenance services

The organisation will periodically review and update the encryption policy to ensure it remains effective and compliant with industry standards and best practices. Any changes to the encryption policy will be communicated to all relevant personnel, and appropriate training must be provided as needed to ensure that personnel are aware of the changes and understand how to implement them.

5.3 INCIDENTS

In the event of a cryptographic security incident, such as a suspected key compromise, the incident response plan shall be activated promptly to contain the incident, investigate its root cause, and implement corrective actions.

5.4 COMPLIANCE

The company is committed to complying with all relevant laws, regulations, and standards related to encryption, including but not limited to:

- General Data Protection Regulation (GDPR)
- The Data Protection Act 2018
- The Investigatory Powers Act 2016
- The Computer Misuse Act 1990
- The Electronic Communications Act 2000
- The Privacy and Electronic Communications Regulations 2003 (PECR)
- The Cyber Essentials Scheme
- The ISO/IEC 27001 Information Security Management System Standard
- The National Cyber Security Centre (NCSC) Security Principles for Cloud Providers

The company will regularly review and update this Encryption Policy to ensure that it remains in compliance with any changes to applicable laws, regulations, and standards.

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.