SQFT Knowledge Services

CRYPTOGRAPHIC CONTROL POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/CCP/POL/037	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/CCP/POL/037	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/CCP/POL/037	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/CCP/POL/037	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/CCP/POL/037	7-Apr-2022	Added Key management	K.Gokhul	S.Nandhini
1.1	SQFT/CCP/POL/037	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/CCP/POL/037	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/CCP/POL/037	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul
1.2	SQFT/CCP/POL/037	15-Mar-2024	Changes done in key management	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

The purpose of the policy is to ensure the customer information, message are concealed and protected as applicable within the SQFTKS's operations and while transmitting the information.

2 SCOPE

This policy applies to all data managed by SQFTKS that are identified as protected information.

3 MAPPING TO ISO27001 CONTROL(S)

Control No	Control Objective
A.10	**Cryptography**
A.10.1	Cryptographic Controls
A.10.3.1	Policy on use of cryptographic controls
A.10.3.2	Key Management

CRYPTOGRAPHIC CONTROLS

- ➢ Identification and implementation of cryptographic solution shall be determined based on a business requirement and risk assessment. Consideration shall also be provided for regulatory restrictions that might apply to use of the identified cryptographic control.
- ➢ SQFT KS shall encrypt sensitive information transported through communication lines.
- ➢ Type and strength of the encryption algorithm to be used in a given situation shall be based on the criticality of the business information handled.

4 POLICY

The policy of SQFTKS is to ensure:

(a) Before cryptography is employed, a business requirement must exist and exact functional requirement must be identified (where required).

(b) Encryption is used to conceal the content of the message where preserving the confidentiality of customer information in electronic form is required during transmission.

(c) Where applicable, cryptographic methods and data encryption products, approved by COO. It should be used in handling critical information that must be protected while in transit or at rest.

(d) Cryptographic methods and data encryption products, recommended explicitly by a regulators/ customers/ any other interested party shall be given highest priority.

(e) Necessary security controls should be considered in order to safeguard the interests of the customer and SQFTKS such as protecting the encryption passwords and keys, wherever applicable. E.g. physical/ logical access controls and awareness on secure handling of keys.

(f) SQFTKS shall use cryptographic controls in compliance with all relevant agreements, laws, and regulations.

(g) When identifying the level of cryptographic protection following shall be taken into consideration (Where Applied / Used)

a. Type/Quality of Algorithm/ encryption
b. Length of Keys
c. Export/Import Controls, if any
d. National regulations, if any

KEY MANAGEMENT

- The length of the cryptographic keys shall comply with any contractual requirements and other regulations.
- The cryptographic keys shall be managed automatically by the applications that are currently used for cryptographic purposes.
- Cryptographic controls shall be implemented in either hardware or software when applicable. SQFT KS, prior to use, shall approve all products (software and hardware), processes, and standards that shall be used for implementing cryptographic controls.
- All the Documents is transmitted via Intranet, then the use of encryption for Intranet shall be implemented. Only users shall be allowed to encrypt mails using other Operations that are approved by COO
- **Key Generation methods:** Keys must be generated by cryptographic algorithms approved by COO.
- **Key distribution and transportation** – Private and symmetric key distribution must be handled securely such as secure email and out of band techniques like conversation through intranet with individuals. Physical transportation of private and symmetric keys will require that they will be encrypted.
- **Key backup** – Keys used for encrypting 'data at rest' must be backed up with documented and proven recovery processes in place.
- **Key usage** – Unique keys (or asymmetric key pairs) should be used for distinct cryptographic processes. Reusing the same keys for different processes may weaken the security provided by one or both of the processes.
- **Key archival** – The integrity and access to the keys must be preserved during the retention period, which often requires the preservation of the software and hardware modules used in the encryption process.
- **Key retention** – Keys must be retained according to the data retention schedule governing the data that those keys are used to encrypt.
- **Key termination** – Symmetric and private keys must be securely erased.

5 EXECUTIVE OWNER

Chief Operating Officer will be the executive owner of the policy.
The policy and revisions shall be approved by the Chairperson of the Information and privacy Security Steering Committee.

IT TEAM shall be responsible for implementing and executing the policy mentioned in this document as well as the guidelines and procedures in the related documents.

Users shall be responsible for exercising adequate care when accessing resources from external networks.

The execution shall be monitored and reviewed by the COO.

6 POLICY ENFORCEMENT

Management reserves the right to monitor the compliance to this policy. All reported incidents related to this policy should be reported to the COO and acted upon based on this policy. All necessary records (emails, etc) for demonstrating the compliance to the enforcement of this policy should be retained as an audit trail.

7 DEFINITIONS

SQFTKS	SQFT KNOWLEDGE SERVICES
COO	Chief Operating Officer
IT	Information Technology Team
ISPSC	Information Security and Privacy Steering Committee

8 ASSOCIATED DOCUMENT

- Cryptographic Control Policy (SQFT/CCP/POL/037).

9 DOCUMENT MAINTENANCE

Chief Operating Officer shall be responsible for document control and any changes.

Updates shall be discussed in the ISPSC under the guidance of COO.

COO shall forward the document to Chairperson of the ISPSC for approval, after review.

End of Document