SQFT Knowledge Services

INFORMATION SECURITY AND POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/IS/POL/016	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.1	SQFT/IS/POL/016	9-Sep-2019	Updated Information Security Objectives	K.Gokhul	S.Nandhini
1.1	SQFT/IS/POL/016	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.2	SQFT/IS/POL/016	20-Oct-2020	Updated Objectives and Unit measurement in Security Objectives	K.Gokhul	S.Nandhini
1.2	SQFT/IS/POL/016	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.3	SQFT/IS/POL/016	19-Mar-2021	Updated Objectives and Unit measurement in Security Objectives	K.Gokhul	S.Nandhini
1.3	SQFT/IS/POL/016	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.4	SQFT/IS/POL/016	09-Mar-2022	Combined Location 2 and Updated Objectives	K.Gokhul	S.Nandhini
1.5	SQFT/IS/POL/016	26-Sep-2022	Changes done in clause 12 of Objectives measurements	K.Gokhul	S.Nandhini
1.5	SQFT/IS/POL/016	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.5	SQFT/IS/POL/016	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 INFORMATION SECURITY AND POLICY - OVERVIEW

A safe and secure working environment is fundamental to business success and we seek to protect our personnel, physical, assets, information, Company and customers' reputation from harm.

2 PURPOSE

This document outlines SQFT KS commitment to information security. It outlines our approach, implementation of the Information Management System and how this is verified by our Information Security Officer.

3 SECURITY POLICY – IMPLEMENTATION – WE WILL

- Identify and regularly assess security threats to business operations and manage associated risks.
- Define and implement specific controls and procedures to ensure the confidentiality, availability and integrity of all forms of business and personal data.
- Develop and maintain effective Security Management processes to mitigate or minimize identified risks by the use of proactive and cost effective measures and procedures.
- Protect all company assets, including Information, Paper, physical assets , Application / software asset, Service asset, People asset, Hardware asset, Reputation, Site, business information and systems, physical property and key business processes from harm.
- Record, analyze and investigate all reported security incidents and irregularities to develop improvements to prevent their recurrence.
- Consider security in all aspects of business operations and planning.
- Expect a positive commitment to security by all levels of management and provide sufficient resources commensurate with the assessed risks.
- Conduct security operations in compliance with SQFT KS business principles, national legal requirements and international standards. Where practical we will improve on the performance standards specified.
- Produce and test response, contingency and business interruption plans to cover all foreseeable events to minimize the impact of any incident or emergency and train personnel in their effective and efficient implementation.
- Introduce and maintain active programs to develop security awareness and responsibility among all employees and Exclusive Consultants.
- Ensure compliance with this policy through a process of education, training, review and audit

This Security Policy will be made available to employees, customers, suppliers and the public.

4 ASSET MANAGEMENT POLICY

Asset Management aims to classify and maintain appropriate protection or organizations assets. Information asset classification ensures that individuals who have legitimate right to access piece of information can do so while ensuring that the information is protected from others who do not have right to access them.

At SQFT KS, assets are classified into the following categories:

- Public: May be viewed by anyone anywhere in the world.
- Internal: Access is available only to SQFT KS employees.
- Restricted: Access is limited to specific members with appropriate authorization.
- Confidential: Access is controlled and restricted strictly to a small number of named individuals.

This involves:

- Identification and categorization of all information assets.
- Maintenance of assets inventory/information asset register.
- Identification of the owners and custodian of information assets.
- Identification of responsibilities of owners and custodians.
- Protection of Information assets through appropriate access control.

4.1 POLICY STATEMENT:

- New Assets: When a new Asset will be commissioned to SQFT KS, appropriate tags will be created and the same will be recorded in the Assets register.
- Asset Movement: Concerned official shall submit the request to the IT team and IT team approves the request after due diligence of the request. Any asset movement shall be logged and reviewed periodically.
- Asset Disposal: Any asset deemed to be ready for disposal shall be reviewed by IT team whether the asset can be recycled/dead.

5 INCIDENT MANAGEMENT POLICY

Accidental or malicious incidents caused by employee or non-employee leads to significant disruption of the mission-critical business process. These incidents can severely disrupt computer supported operations, compromise the confidentiality of sensitive information and diminish integrity of critical data. This policy is designed to help mitigate the disruptive short and long-term effects of security incidents and thereby prevent nonoccurrence at SQFT KS.

5.1 POLICY STATEMENT

1. A formal information security and incident management procedure shall be defined, documented, implemented and maintained by the information security and information management team.
2. Information security and incidents shall be categorized, classified and prioritized to facilitate monitoring, assigning and reporting.
3. All information security and incidents shall be reported, investigated and resolved to ensure that:
    a. The occurrence of such incidents is minimized or eliminated.
    b. Effective security is strengthened or re-established.
4. Employee and users of Information assets shall report all information security and weakness through the Information Security Management Procedure.
5. Employees and users of Information assets shall not report or discuss information security and Incidents with external persons or Organizations.
6. A formal disciplinary process shall be in place for handling violations of security policies and procedures.
7. Learning's from Information Security incidents shall be captured and disseminated to all relevant groups/users by any employee/user/vendor.

6 CHANGE MANAGEMENT POLICY

Information security and incidents leading to loss of information and reliability can result from poorly managed changes in business environment. This policy is designed to control changes in information and IT resources to ensure the information and IT resources of SQFT KS against improper purchase, modification and disposal.

6.1 POLICY STATEMENT:

Changes in the information and IT environment shall encompass:

- Any implementation of new resource/functionality
- Any modification of existing resource
- Any removal / disposal of existing IT resource

Changes to the Information and IT resources shall be through a formal Change Management Procedure:

- Type of change
- Change authorization
- Change monitoring
- Change deployment
- Change review

The development, test and operational environments shall be kept separate to prevent unauthorized access or change to. The information assets

- All changes shall be tested prior to deployment.
- Asset inventory shall be updated after the change.
- Change shall be communicated to relevant people with operational instructions wherever applicable.

7 INTERNET ACCESS POLICY:

All employees at SQFT KS has access to E-mail facility, World Wide Web Services and intranet. Unauthorized use of these facilities leads to dire consequences in the form of wasted resources, risk arising due to the diminished corporate reputation and compliance issues. To protect against these issues, the policy defines the boundaries of behavior and consequences of violation the defined boundaries. Additionally, this policy also defines acceptable use detailing and protecting user's right, outlining responsible behavior.

7.1 POLICY STATEMENT:

The following activities are strictly prohibited:

- Indulgence by employee that violates the local, state, national and international applicable laws and information security policy of SQFT KS during the tenure of employment.
- Violation of rights of any person or company protected by copyright, trade secret or other intellectual property or similar regulations including but not limited to the installation of distribution or pirated software products which are not appropriately licensed by SQFT KS.
- Introduction of malicious programs into the network or servers.
- Revealing account password or use of personal account.
- Covert information gathering on or of the company assets or business.
- Leaving information assets unattended without appropriate protection or security except those in public domains.
- Violation of acceptable usage procedure at SQFT KS.

8 PASSWORD POLICY:

Password is a secret that claimant memorizes and uses to authenticate the claimant's id. Passwords are the most commonly used authentication mechanism. The policy shall govern creation and protection of passwords in SQFT KS to prevent compromise.

8.1 POLICY STATEMENT:

- All servers/system level passwords must be changed at least on a monthly basis.
- All production system passwords must be part of the operations team only.
- All user level passwords must be changed every 45 days.
- All systems and applications used at SQFT KS should adhere to the password policy.
- Password sharing will be generally prohibited except for legitimate reasons after appropriate authorization.
- Password leakage should be treated as a serious information security violation and dealt with a disciplinary action.
- Employees are expected to assign paramount importance to all aspects of information security and ensure safe and secure usage of credentials provided to perform one's role.
- Poor and weak password have the following characteristic which should be avoided:
    - Password length is less than 8 characters.
    - The password is a word found in dictionary.
    - Password is a commonly used word.
    - Password contains the birthdate or the name of the user.

- Strong password will have the following characteristics:

    - The password contains more than 8 characters.
    - Contains both lower case and upper-case characters.
    - Have digits and punctuation characters.
    - Are not based on personal information

Password should never be written down or stored in a file.

9 E-MAIL POLICY:

Electronic messaging (E-mail) system are designed to improve services to customers, enhance internal and external communication and reduce paper work. E-mail system has different risks than paper communication. The policy is defined to ensure establishment of strict and appropriate controls for secure e-mail communications.

9.1 POLICY STATEMENT:

Official e-mail Id should be provided to authorized employees of SQFT KS.

SQFT KS reserves the right to:

- Deny an E-mail id to any individual or team.
- Decide E-mail ids to users.
- Access, read, review, copy, intercept, Block and auto forward emails and files on its system for legitimate business reasons.
- SQFT KS IT team will have access to all emails for security reasons.
- User shall abide by copyrights, ethics, rules and other applicable laws while using company e-mail system.
- E-mail sent outside the organization should have appropriate disclaimer attached.

- Violation of Email policy shall invite disciplinary actions.
- Official communication to be executed only through Office email id

10 AUDIT POLICY:

An effective control program for information security and business continuity requires a well-defined monitoring process. A policy shall be in place. authority to perform internal Audit at least every 6 months to ensure adherence for the defined policies.

10.1 POLICY STATEMENT:

The internal audit committee shall be formed with the following members:

Partners

ISO

Audit independence shall be maintained by having cross-functional team members for the internal audit team.

Audit report from the previous audits should be reviewed along with the status of the findings. Audit committee shall submit the report to the ISO after completion of each audit along with the relevant details.

ISO shall review and come up with the action plan for the findings.

11 INFORMATION SECURITY AND INFORMATION MANAGEMENT

SQFT KS defines Information Security as protecting and preserving the confidentiality, integrity, authenticity, availability and reliability of information assets. Assets are both tangible and intangible things that have a value to the organization and/or its interested parties.

The objectives of our Information Management System are based on a continual formal risk assessment process. Having identified and assessed risks to ourselves, and other interested parties, we select and resource specific information security controls. These are summarized in our current Statement of Applicability.

We are committed to meeting the requirements of information security and good practice, satisfying applicable requirements and seeking ways in which we can improve our security to mitigate new risks. To this end, we maintain an Information Management System which is aimed to comply with the requirements of the ISO 27001:2013 standard.

Everyone within SQFT KS has an important role to play in maintaining security of information, each with their own specific tasks, and responsibilities, within the ISMS. We support staff efforts to secure information through continual staff training and awareness activities. The assignment of general and specific responsibilities for the management of the Information Security system is detailed out in the next section.

To oversee Information Security, we have established the Information Security and Information Management Group to manage the implementation, application, improvement

and supervision of the ISMS. Deviations and exceptions will be managed through this team, using the formal corrective actions.

This policy is subject to annual review to ensure that, at a strategic level, it addresses the evolving information security threats and objectives needed for the organization to be successful. It will also be used to demonstrate commitment to the continual improvement of the ISMS.

12 MEASURABLE OBJECTIVES

To ensure the continued suitability and effectiveness of the Information Management System(PIMS) within SQFT KS, a number of measurable objectives have been established. These objectives shall be monitored and reviewed as part of the ongoing measurement and metrics activities, and the Management Review process. These objectives include:

Functional Group Owners; IT --- Head of IT, Security --- Head of Security, HR --- Head of HR (From ISMS Group)

Location 1

Objective Name	Metrics	Unit of Measurements	Relevant Function Names	Domain Names	Formula	Goal
Communication link failure should not be more than 2 hrs per Incident	Communication link failure in minutes	Hours	IT	Communications and Operations Management	Total No. of Hours failed in a month	< 2 hrs
At any point of time greater than or equal to 80 % of the total employee strength shall have undergone training in ISMS.	% of employees undergone ISMS training	Percent	HR	Human Resource Security	No. of employee received training/Total no. of employee *80 (once in 6 month)	80%
Every Incident /Weakness report should be closed with in a 3 Days	# of Incident / Weakness report closed with in a week	Days	IPSSC	Information Security and Incident Management	No. of incidents/Weakness closed in a month*100	3 Days

To reduce the security events from previous year and if possible bring it to near zero	# of security incidents reported every month	Nos	IPSSC	Information Security and Incident Management	No of incidents occurred every month	0
Information security and policy should be reviewed at least once in a year	No. of times policy reviewed per year	Percent	ISMS	Security Policy	No. of times policy reviewed per year	100%
IPSSC meetings should be conducted at least once in a Quarter.	No of times MSF conducted per quarter	Nos	ISMS	Organization of information security	No of times MRM conducted per quarter	4 per year
Admin/IT Incharge should review the assets at least once in a year	No of times Admin Manager has reviewed the assets in a year. (MSF point)	Percent	IT / Admin	Asset Management	No of times Admin Manager has reviewed the assets in a year.	100%
Preventive maintenance should be carried out for all devices every quarterly.	Percentage of servers for which preventive maintenance are carried out in every quarter.	Percent	System Admin	Physical and environmental Security	No. of PM done for devices in quarterly /Total no. of devices	100%
Business Continuity Plans should be tested at least once in a year.To be tested quarterly	Percentage of Business continuity plans tested in quarterly.	Percent	BCP	Business Continuity Management	No. of Plans tested/Total No.of Plans(once in Year)	100%
Internal ISMS Audit	No of times audit conducted per year	Number	ISMS	Internal Audit	No of times audit conducted per year	2 Per Year

Location 2

Objective Name	Metrics	Unit of Measurements	Relevant Function Names	Domain Names	Formula	Goal
Communication link failure should not be more than 2 hrs per Incident	Communication link failure in minutes	Hours	IT	Communications and Operations Management	Total No. of Hours failed in a month	< 2 hrs
At any point of time greater than or equal to 80 % of the total employee strength shall have undergone training in ISMS.	% of employees undergone ISMS training	Percent	HR	Human Resource Security	No. of employee received training/Total no. of employee *80 (once in 6 month)	80%
Every Incident /Weakness report should be closed with in a 3 Days	# of Incident / Weakness report closed with in a week	Days	IPSSC	Information Security and Incident Management	No. of incidents/Weakness closed in a month*100	3 Days
To reduce the security events from previous year and if possible bring it to near zero	# of security incidents reported every month	Nos	ISPSC	Information Security and Incident Management	No of incidents occurred every month	0
Information security and policy should be reviewed at least once in a year	No. of times policy reviewed per year	Percent	ISMS	Security Policy	No. of times policy reviewed per year	100%
IPSSC meetings should be conducted at least once in a Quarter.	No of times MSF conducted per quarter	Nos	ISMS	Organization of information security	No of times MRM conducted per quarter	4 per year

Admin/IT Incharge should review the assets at least once in a year	No of times Admin Manager has reviewed the assets in a year. (MSF point)	Percent	IT / Admin	Asset Management	No of times Admin Manager has reviewed the assets in a year.	100%
Preventive maintenance should be carried out for all devices every quarterly.	Percentage of servers for which preventive maintenance are carried out in every quarter.	Percent	System Admin	Physical and environmental Security	No. of PM done for devices in quarterly /Total no. of devices	100%
Business Continuity Plans should be tested at least once in a year.To be tested quarterly	Percentage of Business continuity plans tested in quarterly.	Percent	BCP	Business Continuity Management	No. of Plans tested/Total No.of Plans(once in Year)	100%
Internal ISMS Audit	No of times audit conducted per year	Number	ISMS	Internal Audit	No of times audit conducted per year	2 Per Year

13 STATEMENT OF SCOPE

Information security covering;

- the management of the storage, handling and delivery of customer products, services, information and data;
- the provision of IT technical field services;
- the management of third party sub-Exclusive Consultants delivering these services;
- key suppliers; and their services as detailed in the Information Security Systems Supplier Log, including their associated risk profiles;
- the provision of IT and HR services;
- Operations based, in accordance with the latest Statement of Applicability.

14 Individuals in Scope

All SQFT KS employees, key suppliers, Exclusive Consultants and sub-Exclusive Consultants.

15 Locations

All SQFT KS locations.

16 Assets and Technology

- Routing, switching and cabling infrastructure.
- Desktop and laptop devices.
- Servers and support systems.
- Mobile devices managed through the operation.
- Information held within the office and used when working remotely.
- Information hosted through key third parties used by the business' operation.
- Applications provided through key third party suppliers.

17 Third parties, covered by SLA

External third---parties with any electronic access or use of confidential customer information, or a critical role to play in service delivery are managed with appropriate Service Level Agreements (SLAs) and associated processes.

Records

The following information will be recorded in a report during the internal audit

- Risk Assessment and Threat Analysis
- Vulnerabilities
- Review of previously identified noncompliance findings

End of Document