SQFT Knowledge Services

DISASTER RECOVERY POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/DR/POL/009	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/DR/POL/009	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/DR/POL/009	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/DR/POL/009	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/DR/POL/009	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/DR/POL/009	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/DR/POL/009	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

Through the adoption of Business Continuity Management best practices SQFT KS will achieve effective business continuity in safeguarding our reputation and public image. This will occur by using best endeavors to meet the needs of, customers, employees, shareholders and suppliers thereby ensuring that business critical products and services are not compromised by a major disruptive event.

The disaster recovery policy for protection of IT assets of SQFT KS forms part of the ongoing Business Continuity exercise at SQFT KS.

2 SCOPE

The scope of the policy covers all critical Information Technology Assets that support the IT related business processes of SQFT KS. All employees and third parties who provide essential services shall also be covered under the policy as supporting personnel.

3 POLICY

SQFT KS shall establish a Disaster Recovery Plan for protection of its Information Technology assets that support the critical business processes at its Office.

The Disaster Recovery Plan shall address both the general management aspects of the recovery and business continuity process.

The following activities shall form part of the Disaster Recovery Preparedness activities of SQFT KS:

- SQFT KS shall annually review the Risk Assessment including annual update of the Business Impact Analysis.
- Update the Disaster Recovery plan annually to ensure that critical assets and current information have adequate recovery strategies in case of a major disaster.
- The disaster recovery plan shall be reviewed for possible updates within 30 days of any major operational or system changes that will have a material effect on the contingency strategy of the IT infrastructure.
- Undertake exercises of the Disaster Recovery Plan for training and evaluation purposes each year or within 30 days of any major operational or system changes that will have a material effect on the contingency strategy of any department / unit.
- SQFT KS shall ensure that critical functions, for which they have responsibility, are able to continue within the defined Recovery Time Objective following credible major disruptive events and that arrangements are in place to achieve this.
- The arrangements include proactive development, maintenance and devolution of business continuity / disaster recovery planning within their areas.
- Managers shall encourage the active participation of employee in business continuity / disaster recovery issues and must ensure that key personnel are able to perform competently during a major disruptive event.

4 EXECUTIVE OWNER

Chief Operating Officer will be the executive owner of the policy.

The policy shall be approved by the Chairman of the Information Security and Privacy Steering Committee after review by COO.

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

All departments shall coordinate with IT in establishing a practical and live Disaster Recovery Plan.

Users shall understand and comply with the guidelines and be prepared to react properly in the event of any disaster.

The execution shall be monitored and reviewed by the Chief Operating Officer.

5 ROLES AND RESPONSIBILITIES

Abbreviations

P – Primary Responsibility

• - Cooperative Responsibility

N/A - Not Applicable

Responsibility

	IT TEAM	COO	Head of Department	User
Identification of Critical IT Assets	P	N/A	•	N/A
Establishment of DR Plan	P	N/A	•	N/A
Identification of Recovery Time objective	N/A	•	P	N/A
Compliance with the DR guidelines	•	•	•	P
Execution of the DR Plan	P	•	•	N/A
Monitoring and review of the Policy	N/A	P	•	N/A

6 DEFINITIONS

Business Continuity:

Business continuity is the uninterrupted availability of all key resources supporting essential business functions.

Business Continuity Plans:

A collection of procedures and information that is developed compiled and maintained in readiness for use in the event of an emergency or disaster.

(Associated terms: Business Recovery Plan, Disaster Recovery Plan, Recovery Plan)

Business Continuity Management:

Business Continuity Management provides for the availability of processes and resources in order to ensure the continued achievement of critical objectives.

Business Impact Analysis:

A management level analysis, which identifies the impacts of losing organizational resources. The BIA measures the effect of resource losses and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on continuity management.

Disaster:

An event that creates substantial damage stopping business services completely. The event may be natural (e.g. flood, earthquake), accidental (e.g. fire), commercial (e.g. loss of supply of critical services) or willful (e.g. sabotage, vandalism, arson, terrorism). Associated terms: "major crisis'.

Disaster Recovery:

Responding to a disaster and restoring critical operations to the point of normal functioning in the event of a disaster.

Risk Assessment:

Overall process of risk analysis and risk evaluation.

Stakeholders:

Persons and organizations that may affect, or be affected, or perceive themselves to be affected by a decision or activity.

IT TEAM	Information Technology Team
COO	Chief Operating Officer
ISPSC	Information Security and Privacy Steering Committee
User	Users of Critical Service information Assets

7 ASSOCIATED DOCUMENT

- Disaster Recovery Plan (SQFT/DR/PRO/010)

8 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