SQFT Knowledge Services

TELEWORKING SECURITY POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/TWS/POL/032	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/TWS/POL/032	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/TWS/POL/032	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/TWS/POL/032	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/TWS/POL/032	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/TWS/POL/032	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/TWS/POL/032	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

The objective of this policy is to protect security of information assets of SQFT KS when its information assets are accessed from external networks.

Business requirements of the SQFT KS operations require that the information need to be accessed and used, in selected cases, from remote networks. In such cases, the information resources of SQFT KS are subjected to risks that are not under its direct control. Effective risk assessments and agreements for issues including the levels of access and usage need to be adequately addressed in protecting the interests of the company.

2 SCOPE

The policy applies to all users who access and use the information resources of SQFT KS from external networks.

3 POLICY

SQFT KS shall provide restricted access to its information resources from any external networks.

Access from external networks will be permitted only to authorized users on complete business needs and such access will be logged and monitored.

SQFT KS shall take adequate preventive measures to protect its information assets from the risks associated with such external access.

Users shall access the information resources of SQFT KS from secured external networks only, for absolute business needs and exercise due care and prudence to protect the information resources of the company.

4 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 Security and Privacy 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.

5 ROLES AND RESPONSIBILITIES

Abbreviations

P – Primary Responsibility

• - Cooperative Responsibility

N/A - Not Applicable

Responsibility

S.No	Activity	Roles			
		IT TEAM	Users	COO	Department Head
1	Authorization of user for Teleworking on business requirements	•	N/A	N/A	P
2	Granting Access to users for Teleworking	P	N/A	N/A	•
3	Logging and monitoring of Access from External networks	P	N/A	•	N/A
4	Exercising adequate care when accessing network from external networks	•	P	N/A	•
5	Executing and Implementation of the policy	•	•	N/A	P
6	Monitoring and review implementation of the policy	•	N/A	P	•

6 DEFINITIONS

IT TEAM	Infrastructure Team
Head	Group/Department Head
COO	Chief Operating Officer
Users	Employees, third parties, clients etc.
ISPSC	Information Security and Privacy Steering Committee

7 ASSOCIATED DOCUMENT

- NiL

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