



SQFT Knowledge Services

NETWORK SECURITY POLICY

Document Revision History

Version	Document No:	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/NSP/POL/028	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/NSP/POL/028	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/NSP/POL/028	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/NSP/POL/028	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/NSP/POL/028	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/NSP/POL/028	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/NSP/POL/028	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE 3

2 SCOPE 3

3 POLICY 3

4 EXECUTIVE OWNER 3

5 ROLES AND RESPONSIBILITIES 3

6 DEFINITIONS 4

7 ASSOCIATED DOCUMENTS 4

8 DOCUMENT MAINTENANCE 4

1 PURPOSE

In the complex global IT networking environment, SQFT KS needs to safeguard system network, from various business and environmental threats. Towards this end, systems and procedures shall be developed and implemented by providing network security resources at a level that is appropriate for the nature of the data transmitted in order to protect all business data, related application systems and operating systems software from unauthorized or illegal access.

2 SCOPE

This Policy applies to all employees of SQFT KS, Vendors, Employees of Third Parties affiliated with SQFT KS and Exclusive Consultants accessing any resources of SQFT KS from / within SQFT KS or from remote locations.

3 POLICY

SQFT KS shall develop effective systems and procedures to ensure protection of network infrastructure and also provide secured access to its network services for authorized users only by addressing security issues in the following areas:

- LAN Connectivity and access
- Firewall and Router
- Intrusion Detection System
- Remote Access VPN
- URL Filtering
- Content Filtering

4 EXECUTIVE OWNER

Chief Operating Officer shall 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 procedures in the related documents.

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

5 ROLES AND RESPONSIBILITIES

Abbreviations

P- Primary Responsibility

.- Co-operative responsibility

N/A - Not Applicable

Activities	Roles	
	IT Team	COO
Executing and Implementing the Procedures	P	•
Reviewing and Implementation	N/A	P

6 DEFINITIONS

COO	Chief Operating Officer
IT Team	Information Technology Team
ISPSC	Information Security and Privacy Steering Committee

7 ASSOCIATED DOCUMENTS

- Network Security Procedure (SQFT/NS/PRO/022)

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