WIRELESS COMMUNICATION SECURITY POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/WCS/POL/036	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/WCS/POL/036	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/WCS/POL/036	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/WCS/POL/036	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/WCS/POL/036	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/WCS/POL/036	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/WCS/POL/036	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 4
6 DEFINITIONS 4
7 ASSOCIATED DOCUMENT 5
8 DOCUMENT MAINTENANCE 5

1 PURPOSE

Technology development has facilitated access to information resources through non-physical networks. Further, many mobile devices including cellphones, PDAs etc support Wireless Technology.

Wireless connectivity can be in two forms:

1) Controlled connectivity: In this form, wireless connectivity is managed by way of closed wireless circuit like LAN and MAN. Controls can be imposed as per the logical access control policies.
2) Uncontrolled connectivity: Access is feasible through wireless technologies like wi-fi, Bluetooth, infrared etc.

Risks associated with such access include bypassing perimeter controls in the local network, direct exposure of the network, inability to monitor the activities of the wireless network, vulnerability to malicious codes in systems etc.

The objective of this policy is to protect security of information assets of SQFT KS when connectivity is provided through wireless communication.

2 SCOPE

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

3 POLICY

SQFT KS shall provide restricted access to external networks through wireless technologies and access shall be provided only after considering the risks associated with access through wireless technologies.

Usage of wireless technologies using mobile external devices with the IT resources of SQFT KS is strictly prohibited and made available only after proper authorization and risk.

Wireless connection shall be segregated from the physical networks. Access to physical networks through wireless shall be through adequate protection methods.

Users shall exercise adequate care and prudence in using wireless technologies and external devices with wireless technologies and protect the confidentiality and integrity of SQFT KS resources.

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 exercise shall scrupulously follow the policy and exercise due care and prudence when using wireless technology.

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

S.No	Activity	Roles			
		IT Team	**Users**	**COO**	**Department Head**
1	Authorization for using Wireless on SQFT KS	•	N/A	N/A	P
2	Granting Access to users for Wireless	P	N/A	N/A	•
3	Logging and monitoring of Access through wireless devices	P	N/A	•	N/A
4	Exercising adequate care when accessing SQFT KS network through wireless.	•	P	N/A	•
5	Executing and Implementation of the policy	P	•	N/A	•
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

- Wireless Communication Security Procedure (SQFT/WCS/PRO/028)

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