SQFT Knowledge Services

MOBILE COMPUTING SECURITY POLICY

Document Revision History

Version	Document No:	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/MCS/POL/027	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/MCS/POL/027	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/MCS/POL/027	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/MCS/POL/027	13-Mar-2021	Change Laptop/systems	K.Gokhul	S.Nandhini
1.1	SQFT/MCS/POL/027	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.2	SQFT/MCS/POL/027	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.2	SQFT/MCS/POL/027	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.2	SQFT/MCS/POL/027	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 of SQFTKS while using mobile computing facilities (Laptop/systems, PDAs).

A mobile computing device is a small, portable computer that allows a user to store, organize, and access information. Mobile computing devices can be referred as Laptop/systems, PDA (Personal Digital Assistant) and any such devices.

The biggest difference between desktop computers and Laptop/systems is that, in most cases, desktops are used in a controlled environment where the local LAN can be monitored and protected with a network security policy. Laptop/systems are constantly being plugged into various environments. Hence extra security measures need to be taken on Laptop/systems for the physical protection of Laptop/systems and the Confidentiality and Integrity of Information stored on Laptop/systems.

2 SCOPE

The SQFTKS Mobile Computing Policy applies equally to all employees utilizing Portable Computing devices and access the Information System (IS) Resources. It is important that all users are aware of this requirement while using portable devices to access the IS resources.

3 POLICY

It shall be ensured that the **Confidentiality, Integrity, Availability & Legality** of Business Information of SQFTKS is not compromised due to mobile computing facilities used by employees.

Systems & procedures shall be developed containing technical and process measures to achieve the above. The salient features of this Policy are listed below:

- Any device brought in to the LAN environment of SQFTKS, including that of visitors who desire to connect to the LAN, should always be scanned using the official Anti-Virus Scanner s/w before being allowed to connect.
- Executable software must, whenever possible be validated and approved by IT before being installed onto the Laptop/system. Unauthorized installations can compromise the IT operating environment and also constitute a security risk, including the intentional or unintentional spreading of software viruses and other malicious software.
- Employees shall be allotted Laptop/systems based on the business need for mobile computing with due approval.
- All Laptop/systems acquired for or on behalf of SQFTKS shall always remain SQFTKS property. Each employee provided with a Laptop/system is responsible for the security of that Laptop/system, regardless of whether the Laptop/system is used in the office, at his/her residence, or in any other location such as a hotel, conference room, car or airport.

- Laptop/system users must sign an acceptance form, accepting responsibility for loss or damage to the laptop/system.
- Usage of wireless technologies including Bluetooth, Wi-Fi, Infrared and related technologies is restricted for mobile devices and shall be permitted only on selected basis with due approval from COO. Risk assessment shall be carried out in such cases.
- No personal owned Laptop/systems or data storage device that is not authorized by the COO should be brought inside the office premises. Usage of personal mobile computing devices shall be approved by the Chief Operating Officer.

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.

The respective Department / Group heads shall be responsible for implementing and executing the policy mentioned in this document as well as the procedures in the related documents.

The implementation 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	Employees/ Authorised users	COO	Head	Admin
1	Allotment of Laptop/systems	P	N/A	N/A	N/A	N/A
2	Antivirus Configuration/Scanning	P	•	N/A	N/A	N/A
3	Appropriate usage	•	P	N/A	•	N/A
4	Implementation of the policy	•	•	N/A	P	•
5	Monitoring the implementation of the policy	•	N/A	P	•	•

6 DEFINITIONS

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

7 ASSOCIATED DOCUMENT

- Mobile Computing Security Procedure (SQFT/MC/PRO/081)

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