IT EQUIPMENT SECURITY POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/ITE/POL /021	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/ITE/POL /021	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/ITE/POL /021	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/ITE/POL /021	13-August-2021	Added Genset Generator in the Scope	K.Gokhul	S.Nandhini
1.1	SQFT/ITE/POL /021	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.2	SQFT/ITE/POL /021	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.2	SQFT/ITE/POL /021	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.2	SQFT/ITE/POL /021	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 the physical equipment used for Information Technology Processing of SQFT KS and to ensure that the IT equipment and associated infrastructure systems function with optimal capacity and maximum efficiency under normal circumstances.

2 SCOPE

The policy applies to all physical IT equipment and supporting infrastructure that are used for Information processing. This policy covers all servers, firewalls, routers, network components, cables, desktops, laptops, peripheral equipment like Printer, Scanner and supporting equipment like Air conditioners, UPS, Genset Generator Electric equipment etc.

3 POLICY

SQFT KS shall protect all its Information Technology equipment and supporting infrastructure to ensure that the equipment fully support optimal capacity utilization and maximum efficiency in processing business information under normal circumstances.
All users of IT equipment shall exercise due care and prudence when using IT equipment to avoid the damage and risk to the property.

In protecting the IT equipment and supporting infrastructure the following security requirements will be considered:

- Critical IT equipment shall be well positioned and sited in secured areas away from direct view and access and segregated based on the level of sensitivity.
- Smooth functioning of IT equipment shall be protected by way of ensuring adequate availability of supporting and infrastructure services like clean, safe and redundant electric supply, continuous and adequate Heat, Ventilation, Air Conditioning and pollution control equipment, fire detection and protection etc.
- Adequate and secured cabling for power, telecommunication and data/ voice transfer shall be commissioned for all IT and supporting systems to ensure smooth, quality and continuous availability of the services and prevent loss due to short circuit, breakage, EMI etc.
- Equipment shall be maintained as per the vendor specifications and maintenance activities shall be carried out only by adequately trained and experienced service personnel.
- Equipment maintenance activities shall be recorded for knowledge and future reference.
- Preventive maintenance shall be carried out periodically.
- Where equipment is insured, the insurer's specifications shall be complied.
- Adequate precautions and care shall be taken for equipment taken offsite. A detailed equipment protection methodology shall be applied for all equipment carried offsite.

- All IT equipment moving out of SQFT KS premises shall be recorded. Returnable equipment shall be followed up.
- Equipment carrying business information shall be given additional protection for transport, storage and use.
- Media and equipment shall be properly sanitized and thoroughly checked before reuse so that the earlier data stored in the media or equipment shall not be available at the time of reuse.
- Equipment and media shall not be carried offsite without prior authorization and shall be checked and recorded before removal from SQFT KS premises.

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 and Admin department 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 adequate care and prudence in handling of equipment as per the specifications.
- 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	Employees	COO	Department Head	Admin	Finance
1	Protection of Computers, Networking equipment	P	N/A	N/A	•	•	N/A
2	Supply of electricity, HVAC	•	N/A	N/A	N/A	P	N/A
3	Equipment Location	•	N/A	N/A	•	P	N/A
4	Adequate Insurance for equipment	•	N/A	N/A	N/A	•	P
5	Executing and Implementation of the policy	•	N/A	N/A	P	•	N/A

6	Monitoring the implementation of the policy	•	N/A	P	•	•	N/A
7	Equipment and infrastructure SLAs and license for usage	P	N/A	N/A	N/A	•	N/A
8	Proper and careful usage of IT equipment	•	P	N/A	N/A	N/A	N/A

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

- Equipment Security procedure (SQFT/ITE/PRO/017)

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