PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/PES/POL/030	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/PES/POL/030	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/PES/POL/030	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/PES/POL/030	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/PES/POL/030	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/PES/POL/030	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/PES/POL/030	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

Physical Security is one of the most important aspects of Information Protection. In this policy, the Physical Security aspects of Information resources of SQFT KS are addressed. Also mentioned are the environmental security issues pertaining to Information Security and Privacy. Further this policy also addresses the Physical Security requirements when Third Parties access SQFT KS.

2 SCOPE

This Policy applies to all employees of SQFT KS, Employees of Third Parties affiliated with SQFT KS, consultants and other external parties accessing the resources of SQFT KS. Resources include any type of resources that belongs to SQFT KS or available on SQFT KS premises or networks.

3 POLICY

All Information Resources of SQFT KS shall be physically protected by suitable security measures against any kind of unauthorized or illegal Access.

Procedures shall be developed and implemented to ensure the following.

- The premises shall be well planned and sited with adequate security precautions to protect the critical IT resources.
- To distinguish employees and non-employees through different identity cards.
- To record and maintain movement of company properties in the Asset Movement Register.
- To ensure employee belongings are safe and secured inside the premises by providing cupboards with lock and key to the employees.
- CCTV cameras shall be deployed in critical areas and all movements shall be monitored and recorded.
- Manager (Administration) shall be reviewing the CCTV activities periodically.
- The records shall be maintained for a minimum period of 15 days before recycling.
- CCTV tapes/recording shall be reviewed on a monthly basis and the details of review shall be recorded.
- To empower the security personnel to conduct security checks in the interest of the company.
- To make sure critical devices are placed in a controlled access environment.
- All Information Resources shall be environmentally protected as per the best practices and recommendations from respective vendors, consultants & experts, to derive the maximum benefit out of it towards achieving the business goals.
- All IT related equipment's shall be protected with adequate maintenance and controlled movement.

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 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				
		Admin	HR	Head Dept/ Group	Security Guards	Employee
1	Issuing ID Cards (Access Control cards)	P	•	•	N/A	N/A
2	Reviewing of Physical access logs	•	P	N/A	N/A	N/A
3	Reviewing of CCTV	•	N/A	N/A	P	N/A
4	Asset Movement	P	N/A	•	N/A	N/A
5	Reporting of loss of ID cards	•	N/A	N/A	N/A	P
6	Personal belongings		N/A	N/A	•	P
7	Company belongings	•	N/A	N/A	•	P

6 DEFINITIONS

IT TEAM	Information Technology 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

- Physical & Environmental Security Procedure (SQFT/PES/PRO/024)

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