LOGICAL ACCESS CONTROL POLICY

Document Revision History

Version	Document No:	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/LAC/POL/023	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/LAC/POL/023	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/LAC/POL/023	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/LAC/POL/023	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/LAC/POL/023	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/LAC/POL/023	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/LAC/POL/023	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

This policy covers user access to computer systems at various levels like operating system, database and application. This document covers policy for access control to computer systems at the three above-mentioned levels.

2 SCOPE

This policy is limited to controlling access to Information Systems resources like operating system; database and application so as to restrict access to authorized users only. The policy does not include physical access control of desktops/servers hosting the Information security and Privacy resources. This policy is applicable to all employees, third parties and Exclusive Consultants accessing the above mentioned IS resources of SQFT KS.

3 POLICY

- Logical Access to all information-processing facilities of SQFT KS shall be controlled based on "Least Privilege" and "Need to know" basis
- There shall be appropriate approval process to access the information processing facilities of SQFT KS
- Segregation of duties shall be maintained in critical information processing roles
- Software development, test and production facilities shall be separated to reduce the risks of unauthorized access to the operational, application and database systems
- Appropriate procedures shall be evolved to cover the logical access to various Information processing facilities of SQFT KS.

4 EXECUTIVE OWNER

- The 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 procedures in the related documents.
- 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

Responsibilities	Roles				
	IT TEAM	**Head**	**COO**	**HR**	
Access control matrix	•	P	N/A	N/A	N/A
Creation and control of user ID	P	•	N/A	N/A	N/A
Notifying IT TEAM about any role changes	N/A	N/A	N/A	P	N/A
Implementation of the policy and procedure	P	N/A	•	N/A	N/A
Monitoring the implementation	N/A	N/A	P	N/A	N/A
Segregation of duties	•	P	•	N/A	N/A

6 DEFINITIONS

IT TEAM	Infrastructure Management Group
Head	Group/Department Head
COO	Chief Operating Officer
Users	Employees, third parties, clients etc.
ISPSC	Information Security and Privacy Steering Committee
ISACA	Information Systems Audit and Control Association

7 ASSOCIATED DOCUMENT

- Logical Access Control Procedure (SQFT/LAC/PRO/079)

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