LOGGING AND MONITORING POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/LM/POL/022	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/LM/POL/022	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/LM/POL/022	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/LM/POL/022	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/LM/POL/022	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/LM/POL/022	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/LM/POL/022	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

Networked Computing Environment is prone to various types of threats both from internal and external sources. Unless effective event logging and monitoring mechanisms are formulated and implemented to address the threats, the risk remains high. Event logging and monitoring of critical system and security activities provides avenue for effective reduction of the associated risks. This policy and associated procedure will provide a methodology for recording and monitoring system and security related activities of SQFT KS.

The objective of this policy is to ensure that SQFT KS detects unauthorized access of information assets and provides the necessary input to mitigate the associated risks.

2 SCOPE

This policy applies to all computing and network resources that are used for information processing of SQFT KS. Logging activities of physical security control activities like electronic entry Access Control and CCTV activities shall be addressed as environment controls

3 POLICY

- SQFT KS shall develop a methodology to record and monitor the activities to ensure that errors, exceptions, privileged & unauthorized access with respect to the computing and network resources are recorded and monitored with time synchronization.
- The logging and monitoring activities shall ensure the following
- Audit logs recording exceptions are produced for critical systems and kept for an agreed period to assist in future investigations and access control monitoring.
- Procedures for monitoring usage of information processing facilities are established and the results of the monitoring activities are reviewed periodically.
- Controls are implemented to protect logging facilities and log information against tampering and unauthorized access.
- Suitable actions shall be initiated based on the system and security logs to protect all information systems and network infrastructure from external and internal attacks.

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 will be responsible for implementing and executing the policy mentioned in this document as well as the procedures in the related documents.
- Execution of the policy shall be monitored and reviewed by the COO.

5 ROLES AND RESPONSIBILITIES

Abbreviations

P – Primary Responsibility

- - Cooperative Responsibility

Responsibility

S.No	Activity	COO	IT TEAM
1	Implementation of the Policy	•	P
2	Review and Audit	P	•

6 DEFINITIONS

IT TEAM	Information Technology
COO	Chief Operating Officer
ISPSC	Information Security and Privacy Steering Committee

7 ASSOCIATED DOCUMENT

- Logging and Monitoring Procedure (SQFT/LM/PRO/019)

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