



SQFT Knowledge Services

CORRECTION AND CORRECTIVE ACTION POLICY

Correction and Corrective Policy

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/CCA/POL/008	1-Mar-2019	Initial version created	K. Gokhul	S.Nandhini
1.0	SQFT/CCA/POL/008	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/CCA/POL/008	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/CCA/POL/008	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/CCA/POL/008	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/CCA/POL/008	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/CCA/POL/008	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

Correction and Corrective Policy

1 TABLE OF CONTENTS

1	PURPOSE	3
2	SCOPE	3
3	POLICY ELEMENTS	3
3.1	CORRECTION ACTION	3
3.2	CORRECTIVE ACTION	4
3.3	REVIEW	4
4	EXECUTIVE OWNER	4
5	ROLES AND RESPONSIBILITIES	5
6	DEFINITIONS	5
7	ASSOCIATED DOCUMENT	5
8	DOCUMENT MAINTENANCE	5

Correction and Corrective Policy

1 PURPOSE

The purpose of this Policy is to establish a process to identify the cause of problems encountered and to facilitate action to eliminate and prevent problems in all areas and at all levels of an organization while implementing ISMS.

2 SCOPE

This Policy applies to all employees of SQFT KS, Vendors, Employees of Third Parties associated with SQFT KS for monitoring, maintenance, trouble shooting etc.

3 POLICY ELEMENTS

3.1 CORRECTION ACTION

The Chief Operating Officer (COO) shall:

- Review non-conformance report, incidents reported, malfunctions, security weaknesses and business impact analysis and also violations reported pertaining to Security Policy and Security objectives and determine the type of corrective or preventive actions
- Review the audit reports and incident reporting form. Determine cause of non-conformance / security Incident by brainstorming, data collection, advice from expert, consultation with clients and stakeholders, reviewing legal and regulatory requirements
- Inform the appropriate persons whose work interfaces with the non-conformance or is the cause of the security incident
- Document the cause of the problem on the associated report
- Propose and discuss possible mitigation methods or strategies to correct the problem, which shall include:
 - Evaluating the information
 - Determining level of response and
 - Making recommendations for addition or modification of controls.
- Chalk out an implementation plan and assign responsibility for resolution of corrective action and allocate resources (Team or Process Owners)
- Record outcomes of actions taken
- Review and track the planned actions, to make sure that corrective actions have been implemented
- Ensure that corrective action has not introduced any regression error
- Use causes of non-conformance as an input to identify corrective actions
- Track the corrective actions implemented to judge their effectiveness.

Correction and Corrective Policy

3.2 CORRECTIVE ACTION

The audit team/Incident Response team and all employees shall report to COO on potential weakness and improvements to controls.

COO shall:

- Determine potential non-conformance / security incident happening from corrective action reports, audit reports, employee reports, customer complaints, review of ISMS and availability of new and advanced technologies
- Perform analysis to identify root cause
- Decide the addition or modification of controls to prevent the same problem from occurring in future and chalk out an implementation plan and assign responsibility for implementing corrective action and allocate resources (Team or Department Owners)
- Record outcomes of actions taken
- Implement Preventive Action and verify its effectiveness
- Transfer the learning organization-wide
- Submit Corrective Action Report to members of the Information Security and Privacy Steering Committee for information and review
- Track the Corrective actions to review their effectiveness

3.3 REVIEW

- SQFT KS shall ensure that Correction and Corrective Action is integrated in to the process documents and reviewed periodically.
- The Department In-Charge shall review the root cause of the problems reported and initiate Correction and Corrective Action.
- Also they shall decide on the additional Process, Technical control required to prevent such occurrences.
- A report shall be sent to the COO for information and record.
- Chief Operating Officer will review the Correction and Corrective Actions on a half-yearly basis

4 EXECUTIVE OWNER

Chief Operating Officer will be the executive owner of the Policy.

The Policy shall be approved by the Information Security and Privacy Steering Committee after review by the Chief Operating Officer.

COO shall be responsible for implementing and executing the Policy's and guidelines mentioned in this document.

The records relating to this Policy shall be maintained by the Implementation Team member.

The implementation shall be monitored and reviewed by the Chief Operating Officer.

Correction and Corrective Policy

5 ROLES AND RESPONSIBILITIES

Abbreviations

P – Primary Responsibility

• - Cooperative Responsibility

N/A - Not Applicable

Responsibility

S.No	Activity	COO	COO	Department Heads
1	Correction and Corrective actions	•	N/A	P
2	Recording and follow-up	P	N/A	N/A
3	Review of CCA on half yearly basis	•	P	N/A

6 DEFINITIONS

COO	Chief Operating Officer
ISPSC	Information Security and Privacy Steering Committee
ISPO	Information Security and Privacy Officer

7 ASSOCIATED DOCUMENT

Correction and Corrective action Procedure (SQFT/CCA/PRO/008)

8 DOCUMENT MAINTENANCE

Chief Operating Officer shall be responsible for document control and any changes.

Updates shall be discussed by the Chief Operating Officer and the head of the department who recommends change / update in the Policy document or format to meet specific requirements.

COO shall forward the document to Information Security and Privacy Steering Committee for approval, after review.

End of Document