SQFT Knowledge Services

HUMAN RESOURCE SECURITY POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/HRS/POL/012	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/HRS/POL/012	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/HRS/POL/012	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/HRS/POL/012	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/HRS/POL/012	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/HRS/POL/012	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/HRS/POL/012	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

The purpose of this policy is to define the Human Resources activities in SQFT KS for identifying, recruiting, developing and terminating the required Human Resources skills in SQFT KS.

To define, develop, communicate and implement formal process for security in job responsibilities, employee joining, background verification, performance improvement program, Exit process, disciplinary process and Training.

2 SCOPE

This policy is applicable to Human Resource department to manage activities related to Human Resources at SQFT KS in accordance with its corporate values and to comply with the employment legislation and code of conduct and is designed to address Information Security and Privacy with respect to Human Resources Management domain of Privacy information management system(PIMS).

This policy will be implemented in accordance with the Human Resources Management policies of SQFT KS.

3 POLICY

A process shall be in place to manage the Human Resources activities of SQFT KS that include

- Addressing Security at the time of recruitment by way of background checks, screening, professional competence verification etc., for business sensitive roles
- Integrating security with job responsibilities including segregation of duties, monitoring, and specialization wherever applicable
- Including Confidentiality and non-disclosure clause in all employment offers and employment contracts
- Ensuring adequate awareness on Information Security and Privacy as part of employment
- Defining Disciplinary process to respond to violation of policies
- Ensuring that the interest of the organization is addressed with respect to protection of information assets by way of confidentiality and non-disclosure agreements, terms of re-employment, succession planning, professional pursuit etc
- Training Effectiveness and Evaluation should be conducted
- BCP, Health and safety training should be conducted as part of induction training
- Including Information Security and Privacy as part of Service Level Agreements with all contractors and other third party services
- Access authorization for users and monitoring electronic access for better control and time management

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.
- 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 COO.

5 ROLES AND RESPONSIBILITIES

Abbreviations

P – Primary Responsibility

• - Cooperative Responsibility

N/A - Not Applicable

Responsibility

S.No	Activity	Roles			
		HRD	**COO**	**Head**	**Training**
1	Defining job responsibilities	P	N/A	•	N/A
2	Security Awareness & Training	N/A	•	N/A	P
3	Executing and Implementation of the policy	P	N/A	N/A	N/A
4	Monitoring the implementation of the policy	•	P	•	N/A

6 DEFINITIONS

HRD	Human Resources Department
Head	Department / Group Head
COO	Chief Operating Officer
ISPSC	Information Security and Privacy Steering Committee

7 ASSOCIATED DOCUMENT

- Human Resources Security Procedure(SQFT/HRS/PRO/012)

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