INCIDENT MANAGEMENT SYSTEM POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/IMS/POL/014	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.1	SQFT/IMS/POL/014	15-Apr-2019	Update the Incident Reporting template	K.Gokhul	S.Nandhini
1.1	SQFT/IMS/POL/014	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/IMS/POL/014	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/IMS/POL/014	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.2	SQFT/IMS/POL/014	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.2	SQFT/IMS/POL/014	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.2	SQFT/IMS/POL/014	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

Information and Privacy security related threats are increasing and also becoming complex with potential business risk. New types of security related incidents emerge frequently.

An incident response capability is, therefore, necessary for rapidly detecting incidents, minimizing loss of data/business, mitigating the weaknesses that were exploited and restoring the disrupted systems. This policy provides general guidelines for incident handling, particularly for analyzing incident related data and determining the appropriate response to each incident.

2 SCOPE

This policy shall comprise of general incident response, reporting and management guidelines that are independent of specific hardware platforms, operating systems and applications. However, it includes general guidelines for detecting, analyzing, prioritizing and handling incidents. This policy addresses the adverse events that are failure of the Business which is system security, failure and Disciplinary related.

This policy is a supplementary to ISMS manual of SQFT KS. The terms and definitions of SQFT KS ISMS Manual are applied in the same context and meaning, in this document.

3 POLICY

All Information and Privacy Security incidents shall be managed to ensure unhindered business operations. Procedures shall be developed to address the Information and Privacy Security Incidents and also to spread awareness of Incident Management amongst all those associated with SQFT KS Business Operations.

A security incident is defined as an event of violating an explicit or implied security policy.

Such acts include but are not limited to:

- Attempts (either failed or successful), to gain unauthorized access to a system or its data;
- Unwanted disruption, denial of service or Impact on Business;
- Unauthorized use of a system for the processing or storage of data;
- System access violation;
- Changes to system hardware, firmware or software characteristics without the owner's knowledge;
- Computer network intrusion;
- Network integrity violation;
- Privacy violation;
- Installation or use of pirated computer software;
- Offensive electronic mail message;
- Off-site hardware or software damage or loss;
- Any other criminal act where the computer is a major factor in committing the offence.
- Any unauthorized use of SQFT KS resources.

Incident is defined as an event of violating an explicit or implied to the Disciplinary Policy.

Such acts include but are not limited to:

- Confidentiality/ Secrecy
- Any willful company property damage to work in process or any property of the establishment by employee
- Employee will be subject to checking's that may be conducted either before or after the date employment and any incorrect information produced, it may lead to disciplinary action

Other areas accounted under disciplinary standards:

- Negligence of duties or neglect of work and / or Loitering, gossiping in department during working hours
- Willful insubordination or disobedience of any lawful and reasonable order of a superior
- Going on legal strike or abetting, inciting, instigation
- Willful slowing down in performance in work or instigation there of.
- Theft, fraud or dishonesty in connection with the employer's business or property which leads to termination
- Taking or giving bribes or any illegal gratification
- Habitual breach of any standing order or any law applicable to establishment
- Engaging in trade / Gambling within the premises of establishment. Distributing or exhibiting within the premises of establishment and bills, pamphlets and posters
- Drunkenness, Riotous, Disorderly or indecent behavior on the premises of the establishment. Smoking or spitting on the premises of the establishment, where it is prohibited
- Commission of any acts subversive of discipline or rude behavior on the premises of the establishment
- Holding meetings inside the premises of establishment without the permission of the manager
- Disclosing to any unauthorized person any information in regard to the processes of the establishment
- Failure to observe safety instructions notified by the employer or interference with the safety devices
- Refusal to accept a charge sheet order or other communication served in accordance with the standing orders
- Unauthorized possession of lethal weapon in the establishment. Not following the access procedure of bio-metric.

Furthermore, these acts could also be considered cybercrime if they involve deliberate misrepresentation or alteration of data in order to obtain something of value.

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			
		COO	IT TEAM	Users	Head
1	Identifying and Reporting incidents	N/A	N/A	P	N/A
2	Respond to Security Incidents reported and Incident closure	N/A	P	N/A	•
3	Analysing the incident and take decisions	N/A	•	N/A	P
4	Executing and implementing the policy	N/A	N/A	•	P
5	Monitoring the implementation of the policy	•	N/A	N/A	N/A

6 DEFINITIONS

IT TEAM	Infrastructure 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

- Incident Management Procedure (SQFT/IM/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.

SQFT Knowledge Services

Leading player in Real Estate back office support

Incident Reporting		
Name:	**Designation:**	**Employee ID:**
Response Time:	**Classification:**	**Priority:**

Incident information

Date/Time of incident:	
Location/system/Network where the incident has occurred	
Nature of incident: (please Tick Appropriate)	
☐ Virus	
☐ System impairment/denial of resources	
☐ Password Misuse/unauthorized change in password	
☐ Unauthorized access	
☐ Compromise of system integrity	
☐ Theft	
☐ Damage	
☐ Others	
Description of the Incident:	

	Y	N
Did you witness the incident yourself?	☐	☐
Did others witness the incident? (if yes specify below the details)	☐	☐

To your knowledge was any of the following involved?

Telephone	☐	Theft	☐
Fax	☐	Fraud	☐
Photocopier	☐	Unauthorized Access	☐
Computer Hardware	☐	Customers	☐
E-mail	☐	Third Parties	☐
Internet download	☐	Copyright	☐
Virus	☐	Other (specify below)	☐

Initiated By:	Date:

SQFT KS Incident Reporting Form Page 1 of 1

End of Document