SQFT Knowledge Services

CLEAR DESK CLEAR SCREEN POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/CDCS/POL/006	1-Mar-2019	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/CDCS/POL/006	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/CDCS/POL/006	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/CDCS/POL/006	7-Sep-2021	Changes done in Clause 3	K.Gokhul	S.Nandhini
1.1	SQFT/CDCS/POL/006	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.2	SQFT/CDCS/POL/006	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.2	SQFT/CDCS/POL/006	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.2	SQFT/CDCS/POL/006	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

The purpose of Clear Desk and Clear Screen Policy is to prevent the loss of critical and sensitive information, the users shall maintain clear desk and clear desktop (Locked) screen at SQFT KS.

2 SCOPE

This Policy applies to all employees of SQFT KS, Vendors, Employees of Third Parties affiliated with SQFT KS for monitoring, maintenance, troubleshooting etc, Consultants accessing the resources of SQFT KS.

3 POLICY

3.1 SECURE WORK AREA

a. Documents classified as Confidential should be stored in locked cupboards when not in use, especially beyond work hours.
b. Employees should not leave the documents or removable media that may contain business information unattended.
c. Computer terminals should not be left logged and unattended. Users should lock the workstation using Ctrl+Alt+Del key when they are not present in the work area.
d. All active application sessions should be terminated upon completion of the work.
e. Equipment, information in any form or software should not be taken off-site without authorization from the Asset Owner.
f. The respective users should use an appropriately password protected screen saver /auto log off, which should be activated within 5 minutes of inactivity.
g. Confidential/Restricted Information should not be left within Meeting Rooms
h. Any Information written on White Boards or Flip Charts shall be erased at the end of the meeting.
i. Classified material should only be removed from the office when:
   - the material is needed for a declared purpose.
   - the employee removing the material has specific permission.

3.2 PRINTER

a. Confidential/ Restricted information should never be sent to a network printer without an authorized person retrieving it so as to safeguard its confidentiality during and after printing.
b. Documents when printed in the network printer should be cleared/collected by the user immediately.
c. Printers used for the production of output having direct financial value or confidential information must be kept in a secure location

3.3 TELEPHONE

a. Following security safeguards will be observed by users when using Telephones
   - Identify the caller or the recipient destination.
   - Establish a clear need for the information asked.
   - Before sending information classified as Confidential & above, obtain prior approval from Department Head / Process Owners.

3.4 PHOTOCOPIER

b. Personnel using photocopiers must ensure that the documents (both original, copiers and jammed ones) are not left at the photocopier after the copying work.

c. Copying must be made only by persons on need-to-know basis. Reproduced documents must bear the same Security markings/classification as originals. When copies are made using outside facilities, care must be taken to protect the information.

d. When using the photocopiers employees will ensure that they do not make any copies of controlled documents. Any such copies will be made after prior approval and authorizations from the Department head / Process Owners.

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 and Group / Department Heads shall be responsible for implementing and executing the policy mentioned in this document.
- The execution shall be monitored and reviewed by the Chief Operating Officer.

5 ROLES AND RESPONSIBILITIES

Abbreviations
P – Primary Responsibility
• - Cooperative Responsibility
N/A - Not Applicable

Responsibility

SI.No	Activity	Roles				
		IT Team	Admin Team	All Information users	COO	Department Head
1	Secured work Area	•	•	P	N/A	N/A
2	Printer	•	•	P	N/A	N/A
3	Telephone	•	•	P	N/A	N/A
4	Photocopier	•	•	P	N/A	N/A
5	Information Disposal	•	•	P	N/A	N/A
6	Implementing the policy	P	•	•	N/A	•
7	Monitoring the implementation and review	•	•	N/A	P	N/A

6 DEFINITIONS

IT Team	Infrastructure Team

COO	Chief Operating Officer
Users	Employees, third parties, clients etc.
ISPSC	Information Security and Privacy Steering Committee

7 ASSOCIATED DOCUMENT

Clear desk clear screen Procedure (SQFT/CDCS/PRO/006)

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