SQFT Knowledge Services

SOFTWARE USAGE & INSTALLATION POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/SWI/POL /040	1-Mar-2021	Initial version created	K.Gokhul	S.Nandhini
1.0	SQFT/SWI/POL /040	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/SWI/POL /040	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/SWI/POL /040	1-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/SWI/POL /040	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

Table of Contents

1. PURPOSE

The purpose of this policy is to ensure all relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements are explicitly identified, documented and kept up to date for each information system and the organization and to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

2. SCOPE

This policy applies to all employees. This policy covers all computers, servers, and other computing devices operating within SQFT Employee.

3. POLICY

3.1 COMPLIANCE POLICY

Compliance team is responsible to identify any legal, regulatory and contractual requirements related to delivery/projects. Compliance Team shall review periodically at least 6 months once in a consultation with all the departments and delivery/projects and identify the legal, statutory, regulatory and contractual requirements applicable to SQFT KS and shall maintain the consolidated list.

3.2 INTELLECTUAL PROPERTY RIGHTS

a. **SQFT KS** shall follow the practice of complying with the Intellectual Property rights as follows:

- Purchasing hardware only from the authorized suppliers.
- Purchasing and installing only the licensed and approved software from authorized suppliers.
- Informing and educating the users that they will not install any unlicensed software.
- Maintaining proof and evidence of ownership of licenses.
- Carry out checks that only authorized software are installed
- Maintaining an Inventory of assets and identifying the requirements to protect IP rights
- Not copying in full or in part books, articles, or other documents other than permitted by copyright law.

3.3 Protection of Organizational Records

a. SQFT KS complies with the legal requirements on documentation and record maintenance. The records are protected from loss, destruction and falsification.
b. Ensure that documents are readily identifiable.
c. Keep documents under safe custody in such a way that they cannot be damaged.
d. Manage version control of ISMS Documents.
e. Ensure withdrawal of obsolete documents and keep them separately till legal and compliance requirements are met.
f. Ensure that the distribution of documents is controlled.
g. A retention schedule shall be drawn up identifying the essential record types and the period of time for which they will be retained.
h. Records of the performance of the security procedures, as required for establishing and managing the Privacy Information Management System(PIMS) and of all occurrences of security incidents related to the ISMS shall be maintained.

3.4 Data protection and Privacy of personal information and regulation

a. COO, in coordination with the legal department will ensure that the controls are implemented for complying with the Privacy legislation (if any) and requirements.
b. The COO will help in identifying controls required for compliance with the data protection and laws.
c. Regular review and audits of SQFT KS Security Practices shall be conducted to check the compliance with SQFT KS Information and Privacy Security and Privacy policy, Standards and Procedures.
d. Internal audits shall be scheduled yearly or as the need arises by the Compliance and Info Sec Forum.

3.5 Ownership and maintenance of Security Policy

a. The ownership of the security policy is with the Info Sec Forum and is responsible for its implementation and maintenance. The COO is the Administrative owner.
b. The Information Security and Privacy Policies will be reviewed by the COO, yearly or at the time any major IS initiatives undertaken or any changes which would affect the areas covered in security policy and procedures document

3.6 Technical Compliance

a. The compliance as per security standards set by **SQFT KS** shall be ensured for operating systems, database, applications, networks, cabling and environmental infrastructure. The COO shall review for Technical compliance of security controls against security policy biannually. The system administrators and information owners shall ensure that the controls implemented are followed and are in compliance with security policy.

b. Technical compliance checking will be performed either manually or through automated tools, which could generate a technical report for remediation. In order to ascertain the strength of network security, periodic penetration testing and vulnerability testing shall be carried out. Likewise manual or automated vulnerability scanning shall be carried out to ascertain the effectiveness of controls implemented in operating systems.

3.6 Software Licensing

a. SQFT KS shall only use software that has been legally purchased or otherwise legitimately obtained and appropriately licensed.
b. SQFT KS shall comply with the terms of all software licenses.
c. Unauthorized or illicitly copied software must not be loaded or used on any of SQFT KS Systems.
d. An up-to-date inventory of software components and their associated licenses must be held centrally at one location and must be capable of audit by either internal or external parties. All software acquisition must be recorded in the inventory.
e. The inventory must be capable of recording all significant details such as period of license, number, names and locations of users as applicable, software name and version number, software license cost and any major usage restrictions.
f. The IS Division shall undertake regular reviews (minimum 6 months) and reconcile software inventory records to software actually installed for and used by each system user.
g. The IS Division shall ensure that any software found to be installed in SQFT KS's Systems that is not appropriately licensed is immediately uninstalled from the system.

3.7 Usage of open source Software

a. Usage of open source/shareware and unauthorized tools are restricted in SQFT KS for all the employees.
b. Only approved and authorized open source/shareware tools shall be installed.
c. Open source /Shareware tools will be installed based on the user request and approval from the Manager IT and COO.
d. IT shall download and install on the test machine and test the tools for malware, spyware and backdoor etc and shall be deployed on the production system.
e. IT shall review the inventory at least six month once.
f. Based on the user request IT shall uninstall the tools and inventory will be updated.

4. ASSOCIATED DOCUMENT

IT List (SQFT/CM/FMT/013)

5. 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

6. 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