SQFT Knowledge Services

ANTI MALWARE POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/AM/POL/001	1-Mar-2019	Initial version created	K. Gokhul	S.Nandhini
1.0	SQFT/AM/POL/001	1-Mar-2020	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/AM/POL/001	1-Mar-2021	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.0	SQFT/AM/POL/001	1-Mar-2022	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/AM/POL/001	03-Jan-2023	Reviewed and updated the policy for Privacy management systems	K.Gokhul	S.Nandhini
1.1	SQFT/AM/POL/001	01-Mar-2023	Reviewed and no changes done	K.Gokhul	S.Nandhini
1.1	SQFT/AM/POL/001	29-Feb-2024	Reviewed and no changes done	S.Nandhini	K.Gokhul

TABLE OF CONTENTS

1 PURPOSE

The objective of this policy is to minimize the impact of malicious code such as Virus, worms & Trojans that can spread in SQFT KS Network. The above terms Virus, worms & Trojans henceforth shall be referred to as "Malicious Codes or Malware".

2 SCOPE

This policy is applicable to all computing resources of SQFT KS including Desktop/Laptop, Servers, Software, Applications, and Communication Equipment's namely Routers etc.

3 POLICY

All IT infrastructure facilities shall be protected against attacks by malicious codes.

Adequate resources shall be provided to prevent malware attacks and contain the damages in case of an attack materializing.

Procedures shall be developed to ensure continuous compliance with the above requirements across all the IT infrastructure of SQFT KS.

The salient features of the policies are listed below:

- All the computing resources shall be adequately protected with anti-virus software and periodically scanned for virus existence by IT TEAM.
- Unless otherwise absolutely required, administrative rights will not be provided to users in Desktops/Laptop. This will help in preventing installation of unauthorized / unlicensed / untested software in systems besides effectively preventing user from disabling anti-virus in system.
- Usage of external USB devices, bootable CDs, floppies etc., shall be strictly restricted. If so permitted, auto scanning shall be enabled for all external devices.
- Ensuring up-to-date virus signature files on Desktop/Laptop & Servers shall rest with IT TEAM. User responsibility shall include checking for existence of up-to-date virus signature files on his/her Desktop/Laptop and reporting to IT department in case of failure of automatic update / signature files.
- Employees shall ensure that their Desktop Network Interface Cable is disconnected from the network in case he/she doubts for virus presence and report immediately to COO
- Employees shall not use and, if found, they are held responsible for the unlicensed and unauthorized software being installed or used by them in their Desktops/Laptops.

- Employees shall refrain from sharing their folders and in case of absolute need, sharing shall be enabled with passwords.
- Employees shall install & use only licensed and approved software on SQFT KS Desktops/laptops and servers.
- Responsibility of conducting periodic software audits on Desktops/Laptops shall rest with COO in coordination with IT TEAM.
- Server operations team should ensure that antivirus software is installed on all servers with latest virus signatures.
- All the incoming mails to the SQFT KS domain should be scanned for malware at the gateway level. The same shall be done for the outgoing mails leaving the SQFT KS domain.

4 EXECUTIVE OWNER

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

The policy shall be approved by the Chairman of the Information Security and Privacy Steering Committee after review by the COO.

IT TEAM shall be responsible for implementing and executing the policy mentioned in this document as well as the procedures and guidelines in the related documents.

The execution shall be monitored and reviewed by the COO.

5 ROLES AND RESPONSIBILITIES

Abbreviations

P – Primary Responsibility

• - Cooperative Responsibility

Responsibility

S.NO	Activity	Roles		
		User	IT TEAM	COO
1	Anti-virus configuration and deployment	•	P	•
2	Anti-virus Management	•	P	•
3	Content filtering	•	P	•
4	Mobile code control	•	P	•

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

- Anti-malware procedure (SQFT/AM/PRO/001)

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