-

SQFT Knowledge Services

VULNERABILITY MANAGEMENT POLICY

Document Revision History

Version	Document No	Date	Brief summary of changes	Prepared By	Approved By
1.0	SQFT/VAPT/POL/045	04-Mar-2024	Initial version created	S.Nandhini	K. Gokhul

TABLE OF CONTENTS

1.0 PURPOSE **3**
2.0 SCOPE: **3**
3.0 DEFINITIONS **3**
4.0 POLICY **3**
5.0 ASSOCIATED DOCUMENT ..... **ERROR! BOOKMARK NOT DEFINED.**
6.0 DOCUMENT MAINTENANCE ..... **ERROR! BOOKMARK NOT DEFINED.**

1.0 Purpose

This document details the vulnerability management policies and controls required to maintain high levels of system and application security in a diverse IT environment. It outlines the technology and procedures necessary for implementing a comprehensive, integrated program to detect and remediate vulnerabilities in operating systems, applications, mobile devices, cloud resources, and network devices to maintain maximum levels of security.

2.0 Scope:

This policy and supporting procedures encompasses all system resources that are owned, operated, maintained and controlled by SQFTKS and all other system resources, both internally and externally, that interacts with these systems.

Internal system resources are those owned, operated, maintained and controlled by SQFTKS and include all network devices (firewalls, routers, switches, load balances, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources.

External system resources are those owned, operated, maintained and controlled by any entity other than SQFTKS but for which these very resources may impact the confidentiality, integrity and availability (CIA).

3.0 DEFINITIONS

IT TEAM	Infrastructure Management Group
COO	Chief Operating Officer
Users	Employees, third parties, clients etc.
ISPSC	Information Security and Privacy Steering Committee

4.0 Policy

4.1 Vulnerability Scan Frequency / Schedule

All devices are scanned on a consistent scan schedule and also on a by-request or as-needed basis

Sl no	Type of Scan	Frequency	Conducted by	Scope
1	Internal VA	Yearly Once	IT Team	All infrastructure devices/IPs
2	External VA	Yearly Once	External vendor	All Externalized devices/IPs

4.1 Vulnerability Management Solution

The primary vulnerability solution is Nessus professional, Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. It will perform scheduled and on-demand scans on network and server infrastructure and generate reports for the identified vulnerabilities.

Upon receipt of the reports, the Compliance Team and IT team are responsible for:

- Reviewing the results
- Providing a remediation via configuration changes or deploying security patches
- Implementing other mitigating measures
- Properly documenting any exceptions

4.2 Types of Scans

At SQFTKS , we perform the below scans.

4.2.1 Credential / Authenticated scan

Credentialed scans are scans in which the scanning computer has an account on the computer being scanned that allows the scanner to do a more thorough check looking for problems that cannot be seen from the network. Credentialized scan is being done for all sensitive hosts like Firewall or production servers.

4.2.2 Credential / Authenticated scan

a) For external parties, remote access should be provided only if there is a business requirement.

b) The risks for such access privileges should be analyzed and appropriate controls applied.

c) Limitation to connection time should be considered for access in case of external parties such as during office hours.

4.2.3 Non-Credential / Authenticated scan

Non-credentialed scans provide a quick view of vulnerabilities by only looking at network services exposed by the host.

4.3 Remediation Service Level

Vulnerability remediation's are to be classified as per their severity levels and treated accordingly as per the following guidelines:

No	Severity Level	Description	SLA
1	Critical	Critical vulnerabilities have a CVSS(Common Vulnerability Scoring System) score of 8.0 or higher. They can be readily compromised with publicly available malware or exploits.	Immediate
2	High	High-severity vulnerabilities have a CVSS (Common Vulnerability Scoring System) score of 8.0 or higher, or are given a High severity rating by PCI DSS v3. There is no known public malware or exploit available.	Within 3 days
3	Medium	Medium-severity vulnerabilities have a CVSS(Common Vulnerability Scoring System) vulnur score of 6.0 to 8.0 and can be mitigated within an extended time frame.	No action taken - IT Team will analyze
4	Low	Low-severity vulnerabilities are defined with a CVSS (Common Vulnerability Scoring System) score of 4.0 to 6.0. Not all low vulnerabilities can be mitigated easily due to applications and normal operating system operations. These should be documented and properly excluded if they can't be remediated.	No action taken - IT Team will analyze

4.4 Remediation Service Level

All devices connected to both public and private segments of the network are scanned. Device scans are organized by the individually defined address spaces, active directory queries, cloud resources, and locally installed agents.

5.0 ASSOCIATED DOCUMENT

1. Vulnerability Management Policy (SQFT/VAPT/POL/045)

5.1 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