
# BACKUP POLICY

# Document Revision History

| Version | Document No | Date | Brief summary of changes | Prepared By | Approved By |
|---|---|---|---|---|---|
| **1.0** | SQFT/BP/POL/003 | 1-Mar-2019 | Initial version created | K.Gokhul | S.Nandhini |
| **1.0** | SQFT/BP/POL/003 | 1-Mar-2020 | Reviewed and no changes done | K.Gokhul | S.Nandhini |
| **1.0** | SQFT/BP/POL/003 | 1-Mar-2021 | Reviewed and no changes done | K.Gokhul | S.Nandhini |
| **1.0** | SQFT/BP/POL/003 | 1-Mar-2022 | Reviewed and no changes done | K.Gokhul | S.Nandhini |
| **1.1** | SQFT/BP/POL/003 | 03-Jan-2023 | Reviewed and updated the policy for Privacy management systems | K.Gokhul | S.Nandhini |
| **1.1** | SQFT/BP/POL/003 | 01-Mar-2023 | Reviewed and no changes done | K.Gokhul | S.Nandhini |
| **1.1** | SQFT/BP/POL/003 | 29-Feb-2024 | Reviewed and no changes done | S.Nandhini | K.Gokhul |

# TABLE OF CONTENTS

## 1 PURPOSE

The purpose of this policy is to provide means to:

i. restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster; and
ii. provide a measure of protection against human error or the inadvertent deletion of important files

## 2 SCOPE

This Policy applies to all employees of SQFT KS, Vendors, Employees of Third Parties affiliated with SQFT KS and Consultants accessing any resources of SQFT KS.

Further this Policy applies to the following information resources.

- All data residing in Critical Servers including the Operating System files and application software files
- All business data managed and handled by various departments / Groups
- Data on critical Desktops/Laptops and other devices
- Configurations and Registry information of all servers
- Configurations and Operating system files of all network devices, Security products, communication equipment's
- All kind of logs generated from all critical servers, devices and communication equipment's etc
- Software / Utilities / scripts, manuals developed In house, provided by external vendors

## 3 POLICY

SQFT KS shall develop a documented methodology

- To evolve appropriate procedures for backing up information required for business functions on a predefined and regular basis
- All user-level and system-level information maintained by SQFT shall be backed up periodically. The backup media shall be stored with sufficient protection and proper environmental conditions.
- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- The Information Resources backup and recovery process for each system must be documented and periodically reviewed.
- Backup copies of operating systems and other critical information system software shall not be stored in the same location as the operational software.
- The system backup information shall be provided with protection from unauthorized modification and environmental conditions.
- Backups must be periodically tested to ensure that they are recoverable. To confirm media reliability and information integrity, the back-up information shall be tested at some specified frequency.

- Backup information shall be selectively used to restore information system functions as a part of the business continuity process
- To ensure all backup media classified and labeled according to Information Classification Policy
- To have the documented process in place to achieve the above requirements

## 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.

Infrastructure Team will be responsible for implementing and executing the policy mentioned in this document as well as the procedures in the related documents.

Implementation and execution shall be monitored and reviewed by the COO.

## 5 ROLES AND RESPONSIBILITIES

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

Responsibility

| | IT TEAM | COO | User |
|---|---|---|---|
| Requesting for backup | N/A | N/A | P |
| Identifying and segregating critical backup files in local systems | N/A | N/A | P |
| Planning for backup for critical servers and connectivity equipment's | P | • | N/A |
| Taking of backup as per the guidelines | P | N/A | • |
| Implementing the policy | P | N/A | • |
| Monitoring the Implementation and review | N/A | P | N/A |

## 6 DEFINITIONS

| | |
|---|---|
| IT TEAM | Infrastructure Team |
| COO | Chief Operating Officer |
| ISPSC | Information Security and Privacy Steering Committee |
| User | Users of SQFT KS having business important information to be backed up |

## 7 ASSOCIATED DOCUMENT

- Backup Procedure (SQFT/BP/PRO/003)

## 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**