SL No	Description	Rev	Created On	Remarks
1	Initial Release	1.0	30.11.2020	

Prepared By:	Sajin K S	Dept.	IT
Reviewed By:	Shyam	Dept.	IT
Approved By:	Sanil	Dept.	IT

1. INTRODUCTION

It is vital that SFO Technologies adopt consistent policies, appropriate and cost effective strategies and good practice to ensure that all electronic information resources on which SFO depends, and the IT infrastructure on which they reside, are protected against loss of data or corruption. This policy will support and strengthen the implementation of SFO's Information Systems and Information Technology Strategies.

2. OBJECTIVES

- Maintain business continuity within the organization in the event of disaster.
- To protect the institution against the loss of data in the event of other minor incidents which may lead to the loss of data (e.g. data corruption).
- To further develop and maintain a high level of resilience over the institutions Information systems.

3. SCOPE

- This policy applies throughout SFO. It applies to all staff within SFO who create, manage or use data that is owned, managed or stored by SFO. The policy also applies to anyone, including third parties, who manage or have responsibility for systems or data stored on systems within SFO.

- Additionally, in recognition of movement within the institution to use cloud base services the policy applies to all those within the institution having responsibility for management and/or co-ordination of services which may be provided externally by a third party in a cloud based environment.

- The scope of the individual supporting documents is specified within the list of those documents.

4. PRINCIPLES

The principles of this policy are:

- The key purpose of this policy is to define minimum controls required for the backup of SFO IT systems and data to meet the institutions objectives.
- To safeguard against the loss of data that may occur due to hardware or software failure, physical disaster or human error.
- To have a risk aware approach that identifies and addresses unacceptable risks, while maintaining a knowledgeable and reasoned acceptance of other risks.

Responsibilities:

- Formulation and review of the SFO IT Backup & Recovery Policy is the responsibility of the Site IT Manager, reporting to Group CIO. The CIO is responsible and accountable for ensuring that objectives for SFO Backup and Recovery are achieved. Approval of the policy lies with the SFO Executive Group.

- The SFO IT team are currently responsible for the management of all SFO IT department backup systems and associated documents relating to such backup systems.

- Data custodians are responsible for ensuring that appropriate backup schedules are arranged with The SFO IT department. Additionally SFO staff with responsibility for production and management of data must ensure important institutional data under their control is included in the SFO Backup plan.

- All users within SFO have responsibility for the management of institutional data under their control. Staff should ensure that all valuable data both organisational and personal is stored on a recognised SFO data server. End users should not store data on personal computers and/or external devices such as removable hard drives which are not protected by backup.

- Staff having supervisory responsibility are required to coach and encourage best practice amongst their supervised staff or students.

- Data backups are not intended to serve as archived copies of data or to meet requirements relating to institutions record keeping.

- This policy is applicable to all staff within the institution and third parties who process and/or store Institutional data.

- The SFO backup and recovery process is applied to all data held within the Institutions recognised servers/data centres. Responsibility for backup of data held on any computer or device out with these recognised locations, regardless of ownership, falls entirely on the owner/user of the device.

Definitions:

IT (Information Technology) is the SFO department responsible for the provision of backup and recovery services for data held in the Institutional Data Centre.
SFO Data centres are defined as the key physical locations within the institution which hold the institutional Information systems and provide the institutions information technology services. Currently these centres are in the Regional Corporate office Building, Stamping Division at Bangalore and HQ at Cochin.

Granularity is the frequency with which data is backed up. Data that is present for less than this time period may not be captured by the backup process and hence may not be recoverable.

Retention is the length of time a backup is kept. At the end of the retention period the backup is deleted.

RPO- Recovery point objectives refer to data loss tolerance, the amount of data that can be lost before significant harm to the business occurs. The objective is expressed as a time measurement from the loss event to the most recent preceding backup

RTO- Recovery Time Objective refers to how much time an application can be down without causing significant damage to the business.

DC Data Centre

Structure :

The SFO IT Backup and Recovery Policy consists of this high-level overarching document and a number of supporting documents.

5. POLICY

1. Backup & Recovery Policy

SFO requires that all institutional data is backed up according to the following policy:

1.1 Complete records must be kept as to what data and systems are being backed up.
1.2 All Schedules for backup must be recorded and maintained.
1.3 All Backup media must be clearly labelled.
1.4 Where tape media is placed or held within a data centre tape library tapes must be bar coded (If Tape media is used).
1.5 Backups should not be stored in the same building as the live data or system. SFO should strive to ensure geographically diverse locations between the primary data/systems and their backup.
1.6 Data and system recovery processes must be tested frequently. The maximum period between tests should not exceed three months. Testing of recovery procedures must be undertaken to ensure that backup data can be used re-instate data in an emergency or disaster situation. A record of backup testing must be maintained. Where a natural data or system recovery is required this can be used to contribute towards the testing process, provided details of the recovery are recorded.
1.7 Recovery procedures for the restoration of data must be maintained and up to date.
1.8 Records pertaining to points 1.1 – 1.6 above must be managed and retained for audit purposes.
1.9 All users must ensure that important organisational and personal data is stored on a recognised SFO data server and not on personal computers or workstations as these are not backed up.

2. Backup Schedules

SFO requires that the institutions systems and data are backed up in line with the following schedules:

2.1 Backup of data (Staff data, commercial/project/customer data and application data).

- A data backup is taken every day and retention period of each data set is mentioned in below table.
- The first Backup in each cycle must be a full Backup.
- For subsequent backups in each cycle backup type (Full, Differential, or Incremental) must be defined and recorded.
- Data created or deleted less than 24 hours between backups or data deleted more than 30 days before the backup was created cannot be recovered.

The following schedule provides for data to be restored with at most one working days data missing.

Data Set	Type of Backup	Granularity (Duration between backups)	Retention Period	Location
Application & Databases	Incremental	4 Hrs	30 Days	Secondary DC
	Full	Weekly	8 weeks	
	Full	Monthly	12 months	
	Full	Yearly	5 Years	
Staff/User Documents and files Commercial Data Customer's/Project Data	Incremental	Daily	30 Days	
	Full	Weekly	8 weeks	
	Full	Monthly	12 months	
	Full	Yearly	15 Years	

2.2 Backup of Systems

Backup for SFO systems is required to protect the organisations vital business and operational systems. System backup must be provided for all infrastructure, business and data systems to ensure that in the event of any significant disaster, such as loss of data centre or system, business critical systems can be restored within a reasonable time frame.

To facilitate quick recovery of systems SFO must maintain the following types of backup:

- Backup copies of systems in the form of images which can be restored to any location or platform.
- Replicate all virtual key systems adhering to this Backup Policy, particularly with regard to location.
- Ensure additional backup of data and system configurations are in place for all systems.

2.2.1 Backup of Systems (hardware platform)

- All system image backups must be full backup.
- Changes to systems less than 7 days between backups must be captured daily using configuration backup
- Additional database backup process must be applied to all systems holding databases.

The following table provides the backup schedule for imaging of SFO Systems. This schedule dictates the frequency for full system images based directly on hardware platforms (not virtualised).

Data Set	Target	Type of Backup	Granularity (Duration between backups)	Retention Period	Backup Storage Location
Bare Metal Image	Domain Controller Exchange Servers ERP Server ERP Development Server File Server	Incremental	Daily	30 Week	Primary DC Secondary DC
		Full	Weekly	8 weeks	
		Full	Monthly	12 months	
		Full	Yearly	5 Years	
Active Directory	Domain Controller	Incremental	Daily	30 Week	Primary DC Secondary DC
		Full	Weekly	8 weeks	
		Full	Monthly	12 months	
		Full	Yearly	5 Years	

2.2.2 Backup of Systems (Virtual platform)

With a few exceptions SFOs infrastructure and application systems are homed in a virtual environment using VMware ESXi and Hyper-V. In order for SFO to maximise benefit from this type of deployment these systems must be replicated frequently to provide an additional level of resilience in event of a hardware failure or local disaster. The schedule below indicates frequency for replication of all virtual servers. This replication must observe backup policy by ensuring that replicas are housed in a different physical location to the original virtual server.

- All system replication backups must be full backup.
- Changes to systems less than 7 days between backups must be captured on a daily using additional configuration backup.
- Additional database backup process must be applied to all systems holding databases.

Data Type	Granularity (Duration in days between backups)	Backup Retention Period	Location
Infrastructure Systems	7	Replica over written on backup.	Secondary DC
Application Systems	7	Replica over written on backup.	Secondary DC

2.2.2.a Backup of System configurations

Replication of SFO servers enhances recovery of systems. In many instances the replication process may not be frequent enough to ensure full recovery of status or configuration of a system in the event of recovery.

In order to mitigate the risk, where this exists, configuration backup must be taken at more regular frequency than full replication or system image.

- All system configuration backups must be full backup.
- Changes to systems less than granularity period cannot be restored.

The following table outlines the schedule for system configuration backups. Details of which data should be backed up must be detailed in the SFO Backup Procedure documentation.

Data Type	Granularity (Duration in hours between backups)	Backup Retention Period	Location
Infrastructure Systems	24	30 Days.	Secondary DC
Application Systems	24	30 Days.	Secondary DC

3. Data Recovery

This section of the policy document outlines the policy for recovery of data relating to SFO Backup.

- Request to recover data or systems should be submitted to the IT Help Desk with appropriate approvals. Requests must be made at earliest possible time following loss of data or system.
- The SFO IT department cannot accept responsibility for delay by a member department or individual to register requests for data or system restoration.
- Data restoration from backup is subject to the retention and granularity periods defined within this backup policy (Backup schedules section 2).
- All the requests to recover data from backup (data mentioned in section 2 of this policy) are processed the SFO IT department must endeavour to process such request as soon as possible following receipt. The following table summarises recovery schedules for types of backup carried out by the SFO IT department and required approval levels.

Data Type	**Recovery Period (Hours from request receipt)**	**Type of Recovery**	**Potential data loss (The period of potential difference [hours] between loss of data & last backup).**	**Required Approval**
Commercial/customer/Project/ Personal Data files stored on SFO data servers (Not exceeding5GB).	24 Hrs	Permanent recovery to original data location.	24 Hrs if reported in 30 days	HOD and BU HEAD
Commercial/customer/Project/ Personal Data files stored on SFO data servers (Not exceeding5GB).	48 Hrs	Permanent recovery to original data location.	24 Hrs if reported in 30 days	HOD and BU HEAD
Application Data bases	48 Hrs	Permanent recovery to original data location.	24 Hrs	CIO
Infrastructure servers (Domain Controller)	8 Hrs	Initial recovery using system	No data loss anticipated	CIO

		state backup, Later replicated from Additional Domain Controller		

6. RPO & RTO

Below table outlines the RPO and RTO of critical services.

Services	RPO	RTO
ERP Services	4 HRS	4 HRS
Domain Controllers	NA	4 HRS
File Server	24 HRS	8 HRS
Application Servers	24 HRS	4 HRS

7. POLICY AWARENESS

An electronic copy will be made available on SFO Intranet, SHAREPOINT and IT Help Desk Portal.

8. IT DATA RECOVERY INCIDENT LOG

A record will be maintained within the IT Help Desk software in which all IT Data recovery Incidents will be recorded along with details of any action taken. All staff (from all Departments) will have a responsibility to log with the IT Help Desk any incidents that relate to recovery of Data with necessary approvals.

9. RELATED POLICIES AND DOCUMENTS

The following is a brief summary of documents associated with this backup policy. Full copies of these can be obtained from the SFO Intranet, Sharepoint and IT Helpdesk portal.

Acceptable Use Policy – Information Systems

The reason for this policy is to ensure the proper use of all of SFO's computing and network facilities.

Policy for Data Protection, Data Classification, Information Labelling and Handling Procedures

This policy outlines criteria for categorising importance of data handled by SFO staff. The policy covers the security and use of all information and IT equipment of SFO Technologies Private Limited.

IT Procedure

This procedure outlines control on usage of all Software's & Electronic data to ensure unauthorized use, proper storage and protection.