IRDAI REGISTERED INSURANCE BROKER

Backup Policy and Procedure

Document Number: SMCInsurance/PO & PR- 03

SMC INSURANCE BROKERS PVT. LTD.

Document Details

Title	Backup Policy and Procedure
Version	0.1
Author	IT-Team
Classification	Internal
Reviewer & Custodian	Director
Approved By	Director

Distribution List

Name
Internal Distribution Only

Version History

Version Number	**Version Date**	**Change Description**
3.1	8.06.2020	New policy creation

Table of Contents

Contents

1. *Overview* 5
2. *Purpose* 5
3. *Scope* 5
4. *Policy Review, Revision and Communication* 5
5. *Definitions* 5
6. *Guidelines* 5
7. *Procedure* 6
8. *Responsibility* 6
9. *Testing* 7
10. *Restoration* 7
11. *Task* 7
11.1. Validation and Verification 7
11.2. Exist Criteria 7
12. *Non- Compliance* 7
Annexure 1 8
Back up Procedure 8
- **Local Server:** 8
- **File Servers etc.** 8
- **Configuration Back up of Network Devices** 8

1. Overview

This policy and procedure defines backup of applications, transactional data created by the applications, systems and configuration backup of critical devices within Smc Insurance Brokers Private Limited (hereafter, SMC) which are expected to have their data backed up. These systems are typically servers, but are not necessarily limited to servers. Servers expected to be backed up include the File servers, AD servers etc.

2. Purpose

Backup policy and procedure is designed to protect data in SMC and to be sure that it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

3. Scope

Backup policy and procedure applies to all equipment and data owned and operated by SMC.

4. Policy Review, Revision and Communication

This policy shall be reviewed and updated once every year to incorporate relevant changes. All subsequent updates to the policy shall be communicated over E-mail and made available on the intranet to all the employees by the end of March every year.

5. Definitions

- **Backup:** Saving of files onto offline mass storage media/ SAN/ Hard disk Storage clusters for the purpose of preventing loss of data in the event of equipment failure or destruction.
- **Retention:** Saving of old or unused files onto offline mass storage media for the purpose of releasing an online storage room.
- **Restore:** Process of bringing offline storage data back from the offline media and putting it on an online storage system such as file server.

6. Guidelines

- The frequency of back up for all critical and important data shall be identified by the asset owner.
- Full back up for critical data shall be performed once a month.

SMC INSURANCE BROKERS PVT. LTD.

- Logs of backups shall be maintained in soft or hard format wherever possible as per availability for all critical information systems.
- Restorations of critical data shall be carried out periodically ascertaining the integrity of the backups taken.
- Backup shall be taken on suitable media favoring ease of restoration and storage. Media shall be labeled for identification. Wherever possible multiple copies shall be maintained for redundancy. Old or damaged media shall be incinerated to avoid misuse.
- A Disaster Recovery (DR) site shall be implemented and maintained. This could be either a hot or a cold site as per SMC business requirements. Periodic checks shall be carried out to ascertain the DR site is in sync with the primary site.
- Backup copy shall be maintained off- site as well.
- Backup media used shall be a reliable and secure one. Backup copies of annual data, monthly data, application files etc. shall be stored under lock and key in a fireproof cabinet. Cabinet shall not place in the Data Center (DC).
- Replication of the entire production data shall be done on the MIS server after each day end.
- Restoration of backed up files shall be ensured as the e- data is regarded as evidence in the Court of Law as per IT Act.

7. Procedure

Data Backup Schedule:

Category	Daily	Weekly	Monthly	Random
Configuration back up of critical devices	No	No	Yes	As and when any change in configuration/topology occurs
Servers	no	No	yes	
Network Devices	No	No	Yes	As and when any change in application occurs
Applications	no	Yes	No	

8. Responsibility

Sr. No.	Role	Responsibility
1	Primary responsibility of ensuring physical and environmental security of DR.	IT- Manager
2	Hardware and networking shall hold operational responsibility in this regard.	Assistant Manager
3	Shall be responsible for the security of the assets placed in their respective locations.	Managers or such Location Heads

9. Testing

The ability to restore data from backups shall be tested at least once in 6- (six-) month.

10. Restoration

Users that need files restored must submit a request to the IT- Admin. End- user system related restore request must go the IT Helpdesk ticketing queue (it@smcinsurance.com; itsupport@smcinsurance.com). Include information about the file creation date, the name of the file, the last time it was changed and the date and time it was deleted or destroyed.

11. Task

11.1. Validation and Verification

Backup data verified by user for restoration and validity. It is user's responsibility to verify the same.

11.2. Exist Criteria

- Backup log is updated.
- Backup directories are updated.

12. Non- Compliance

Failure to comply with this policy may, at the full discretion of Smc Insurance Brokers Private Limited, result in disciplinary action as per the policy.

Annexure 1

Back up Procedure

- **Local Server:**
  - Attendance Server etc.
- **File Servers etc.**
  - Daily Database backup is getting stored on (backup server).
  - Database backup configuration file is scheduled in a (backup server name).
  - Daily database backup is running at time (1 AM midnight) A.M. IST.
  - A current timestamp folder is created for backup on (as per the application) based on schedule time.
  - Backup of 2 months with versioning is retained on (storage server).
  - Database configuration file backup job is scheduled as per policy.
- **Configuration Back up of Network Devices**
  - Backup of all critical network devices (switches, routers, firewalls, applications) are taken as change takes place and when required and put in the backup server. Backup is stored at (remote location and SAN Storage).
  - Restoration of backup is done as and when required.

End of Document