**Data Backup Policy and Procedure**

Doc ID: POL/0.1

Document Classification: Internal

July 2022

**Document Control Information**

| Document Name | Data Backup Policy and Procedure |
| --- | --- |
| Document ID | {Company}/POL/0.1 |
| Document Owner | Information Security Officer |
| Classification | Internal |
| Approved By |  |

| **Authorization** | | | |
| --- | --- | --- | --- |
| **Stakeholders** | **Read Access** | **Write Access** | **Media Type** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

| **Amendment Log** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Modification Date**  **DD MMM YYYY** | **Author (s)** | **Reviewed By** | **Approved by** | **Brief description of the change** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**TABLE OF CONTENTS**

1.0 Policy Statement [4](#_heading=h.1fob9te)

2.0 Purpose [4](#_heading=h.3znysh7)

3.0 Scope [4](#_heading=h.2et92p0)

4.0 Policy [5](#_heading=h.tyjcwt)

4.1 Responsibility [5](#_heading=h.3dy6vkm)

4.2 Documentation and Records [5](#_heading=h.1t3h5sf)

4.3 Backup Media and Storage [6](#_heading=h.4d34og8)

4.4 Restoration Testing [6](#_heading=h.2s8eyo1)

5.0 Backup Requirements [7](#_heading=h.17dp8vu)

5.1 Backup Plan [7](#_heading=h.3rdcrjn)

5.2 Backup Medium and Mechanism [7](#_heading=h.26in1rg)

5.3 Backup Operations [7](#_heading=h.lnxbz9)

6.0 Storage of Backup [8](#_heading=h.35nkun2)

6.1 On-Site Backup [8](#_heading=h.1ksv4uv)

6.2 Off-Site Backup [8](#_heading=h.44sinio)

7.0 Procedure [9](#_heading=h.2jxsxqh)

7.1 Creation of backup schedule [9](#_heading=h.z337ya)

7.2 Backup Procedure [9](#_heading=h.3j2qqm3)

7.3 Tape Labeling [9](#_heading=h.1y810tw)

7.4 Backup Operations [9](#_heading=h.4i7ojhp)

7.5 Restoration Plan [11](#_heading=h.2xcytpi)

7.6 Backup Restoration [11](#_heading=h.1ci93xb)

7.7 Backup Restoration Testing [11](#_heading=h.3whwml4)

7.8 Backup, Storage, Restoration Review [12](#_heading=h.2bn6wsx)

8.0 Reference Documents [12](#_heading=h.qsh70q)

# 

# Policy Statement

Electronic Information Systems and the Business information stored and communicated via these systems, are essential resources for accomplishing {Company}’s business activities.

These resources and information are valuable and it is imperative to ensure continuity of the operations in case of hardware faults or other disasters. This policy relates to the backup, storage and restoration of the application systems and the data on an ongoing basis.

# Purpose

The purpose of this policy is to:

* Ensure continuity of operations in spite of hardware failures and other disasters
* Identify the critical components to be backed up and define the procedures for taking backup
* Define the mechanism to store the backup media in a manner ensuring reliable and safe location
* Provide guidelines for restoration testing of the backed up media
* Define an offsite backup mechanism to ensure disaster recovery

# Scope

This policy is applicable to Business systems and information stored in {Company}'s Electronic Information Systems

**Note:** IT systems (hardware / software) owned or under the custody of {Company} include but are not limited to systems at {Company} office premises in India / abroad, VSNL and Reliance data-centers and data-centers elsewhere, and also systems leased out to vendors.

# Policy

## Responsibility

* Application / information owner or respective Department Head shall identify the data which should be backed up along with the frequency and the retention period. System administrator from IT shall ensure that backups are taken as per the schedule. The primary responsibility of data backup process and execution shall remain with IT Team. Similarly the operating system files and database configuration files shall be identified by the respective system / database administrators.
* Application owner with the help from system administrators and database administrators shall decide appropriate backup plan for each type of data identified taking into consideration importance of data, legal requirements, technology available, application requirements, nature of transactions etc.
* The Head – IT shall delegate the task of regular backups to the members of the IT Team. The delegated persons (backup team) shall test the ability to restore data from backups as per the data restoration request raised by the project / support team. IT team shall test the ability to restore data of server’s backup on quarterly basis.
* Any changes done to system which affects regular backup should be prior informed to backup team by application owner.
* Users are responsible for backing up any data not stored on file servers. All important data should be copied on file servers to ensure the backup.

## Documentation and Records

* Detailed backup plan and procedures for each application under IT custody / control shall be documented by the IT team. For applications under project team the detailed backup plan and procedures shall be documented by the project team and IT team together. This shall include details like data to be backed up, type of media, backup application, type of backup, storage location, rotation and archival schedule, restore procedures, restoration testing frequency, labelling standards, etc.
* Backup procedures should provide the following information:
* Files and applications to be backed up
* Inventory of backup media including the location of their storage and contents
* Record of blank (unused), discarded and destroyed media in a manner that complete history of media usage is available

## Backup Media and Storage

* Backup media shall be clearly and distinctly numbered. The details of the backup media such as number of the backup media, the number of times it is used shall be obtained from the backup software.
* All data stored on the backup media shall be classified. Removable media shall be treated with the same or greater security precaution warranted by the classification of data it holds.
* External labels of tapes / cartridges / floppies / CDs etc. shall mention the name of the backup.
* Backup media must be selected depending on the quantum of data, type of application software package, speed of backup and restoration, life of storage of the data, reliability requirement, efficiency, available technology and the guidelines in force.
* The backup media must not be kept for storage in the same place where original data resides. A backup copy of all data must be maintained at an identified off-site location. Offsite backup must be maintained in fire resistant cabinet and must be provided with appropriate physical security.
* All movement of backup media to the onsite backup storage room or to the offsite backup storage area must be controlled and logged for future reference.
* Access to backup media will be restricted on a ‘need to know’ basis. Access shall be provided only after approval from backup administrator / Head – IT. The ad-hoc backup request / project archival backup is performed on the tape which will be in the custody of the IT team. The CD backup (backup example: such as outlook mails) will be in the custody of the project manager and /or the personnel who requested the backup.
* Storage media will be destroyed based on the restoration period and / or when not needed.
* The media containing the backups shall be preserved and retained to a minimum period of as required under any relevant regulations or as mentioned in the Backup Register.
* In case the backup media is to be changed with a new technology, the latest backup must be converted to the new media in one copy. The backup software also must be backed up into another media and kept or have compatibility with the new system.
* Monthly (one-month older tapes) backup tapes shall be couriered to alternate sites.

## Restoration Testing

* Restoration test shall be carried out as per the data restoration request raised by the project / support team. IT team shall test the ability to restore data from backup of the servers as per the restoration test plan document. The recommended frequency for backup restoration testing is once in 6 months.
* Restoration logs shall be maintained as records for the restore results.
* Recovery procedures as defined by application owners should ensure the relevant files are restored in order to ensure full application functionality is restored.
* Logging of restore operation should be enabled and logs screened to check errors during the restore operation and if the files have been completely restored.
* The restored data shall be removed from the test machine after the activity is concluded. All media with unsuccessful test shall be disposed appropriately. The application / information owner shall be informed of the same and fresh backup taken accordingly.

# Backup Requirements

## Backup Plan

The backup of IT resources at {Company} shall be as per the **Backup Plan**. The backup plan and the backup operations would be as per the following:

* Each IT application in live operations at {Company} and the components in these applications to be backed up shall be identified in the backup plan.
* The components that are static in nature (software, configurations, etc.) and the dynamic components (application data) shall be identified. The frequency of the backup of such components may thus be determined.
* The mechanism and frequency of backing up of these shall also be laid out in the plan.
* A role / person shall be identified for each IT system to be backed up, and such person would be responsible for taking the backup of the applications as per the plan.
* The backup plan must also contain the restoration plan. That is, the frequency of restoration testing and the person / role responsible for the same shall be part of the backup plan.

## Backup Medium and Mechanism

For critical applications, the hardware must have adequate redundancy built in to take care of disk failures etc. Typically, RAID configured servers that support hot swappable disks should be used for such applications.

Backup media as defined in the **backup plan** shall be used for backing up the various components of the IT applications. Typically, backup medium may include Version Control System (CVS) for software, hard disks for replicated data backup, tapes for data backup and storage on-site and off-site.

In cases where backup is to be taken on hard disk media, the same shall be automated by means of backup scripts.

All collation / collection of backup data must be done through scripts to avoid manual errors. Copying of backed up files / archives onto offsite media shall be done manually.

## Backup Operations

As per the backup plan, backup must be performed by the System Engineer designated for the purpose (backup operator).

Where the backup is being run automatically by means of scripts, the backup operator must ensure that the scripts have run properly without error.

Where the backup is to be taken on offsite medium like tapes, the same must be clearly labeled.

The backup operator must fill up the **backup check list** at the end of the backup operation that identifies the label of the medium (if tape), the number of files backed up, the size and such information as mentioned in the backup check list.

The backup operator would ensure that the backed up data medium is handed over for safe storage to the person in charge of storage of the backup medium.

# Storage of Backup

## On-Site Backup

The backed-up media must be stored in a secure and environmentally safe location.

Backup media is stored in an organized way, by means of labels and the backup date, to ensure that the backup for the specified number of days is easily accessible.

Backup media may be released for reuse after ensuring that the backup for 7 days is available. That is, the storage may contain 7 sets of the latest backed up media. The tapes shall be labeled in a manner that shall ensure that there is no confusion for using the tape. The older ones may be rotated for reuse. Such release of backup media must be duly recorded in a **backup media release list**.

Whenever new media is added to the backup media repository, the labeling is done so as to not create confusion in the organization of stored backup media.

## Off-Site Backup

At regular intervals as identified in the **backup plan**, the backup media must also be handed over to custodians who would store the same in a different location than the location of the data source. These offsite backup custodians must store the same in a safe and secure location, such as a fire-resistant cupboard.

The offsite backup shall be maintained for a period of 7 years. Tapes older than that can be recycled. Any such reuse / recycling must be duly recorded in the **backup media release list.**

# Procedure

## Creation of backup schedule

* Application / information owners will intimate IT about their backup requirements for the File Servers.
* The backup administrator will create the backup schedule for all critical systems and File Servers being used by {Company} and the same would be validated by Head - IT.
* The backup schedule will mention the frequency (regular backup or achoo) and the data that is going to be backed up.
* The backup schedules would be validated by the Head – IT.
* Any changes to the backup schedule will be subject to approval from Head - IT.
* Once validated, the backup schedule will be conveyed to backup team. Backup team would then follow the schedule and take backups accordingly.

## Backup Procedure

* Instruction / Guidelines for taking backup of data will be issued by Head – IT.
* During the regular backup routine, the backup team will take the backup as per the Backup Schedule.
* In addition to the scheduled backups, backups shall also be taken and stored at a centrally located space in case any of the following events occurs:
* Configuration change in an IT / IS asset
* Upgrade of any OS / Firmware / Application system etc.
* The backup activity will be closely monitored and logged by the IT department.
* The backup tapes will be rotated as per the retention period.
* The backup team shall take care in using the right tape and label the tapes appropriately as detailed in the backup register.
* If the backup team personnel have started the backup and the backup has failed then the verbal instructions from the Head - IT or the backup administrator shall be provided to the next shift person. The event of failed backup would be logged as an incident in the Service Desk and appropriate actions taken to ensure successful backup would be recorded.

## Tape Labeling

* All backup media must be appropriately labelled and numbered automatically by the backup system or manually by the operators taking the backup. The monthly (one month older tapes) backup tapes would always be kept offsite for any disaster management.
* The backup media shall be rotated based on the Backup Plans and Backup Schedule. Backup media shall be replaced with a new one after the stipulated number of usages as per backup media technical specification.
* Backup media shall be replaced immediately after encountering the error or at predefined time intervals whichever is earlier.

## Backup Operations

* Backup Frequency
* Daily Incremental backup for Monday, Tuesday, Wednesday and Thursday and full backup on Friday.
* If for maintenance reasons, backups are not performed on Friday, they shall be done at the earliest after completion of maintenance.
* Every month a monthly backup tape shall be made using the oldest backup tape from the tape set.
* Backup Storage
* There should be a separate set of tapes for each backup day including Monday, Tuesday, Wednesday, and Thursday. There shall be a separate set of tapes for each Friday of the month such as Week 1, Week 2 etc.
* Backups performed on Friday or weekends shall be kept for one month and used again the next month on the applicable Friday. Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week.
* At least one full backup set should be stored offsite. All backups should be stored at secure locations with controlled environment. At least one set should be kept in fire proof safe locker. If the fireproof / waterproof cabinet is not available, they shall be stored in normal lockers.
* A comprehensive record of storage should be maintained. Offsite storage should be carefully planned considering physical access, transportation procedures etc.
* Age of tapes: The date each tape was put into service shall be recorded on the tape. Tapes will be used till the time as prescribed by the manufacturer. The Monthly backup tapes shall be reused after two years.
* Tape drive cleaning: Tape drives shall be cleaned with cleaning tape automatically by the system whenever needed and the cleaning tape shall be changed as per usage and manufacturer specification.
* On-Site
* On-site backup shall be maintained in safe custody in a fireproof and / or water proof cabinet. If the fireproof / water proof cabinet is not available, they shall be stored in normal lockers. Controls shall be in place near the cabinet for protecting the cabinet from fire and water disasters.
* The key to the cabinet shall be available with the Head – IT and / or Backup Administrator.
* Off-Site
* As per the backup schedule, identified backup media shall be stored at an off-site location which shall be at least 5 km from the on-site location, in a fire-proof and / or water proof cabinet. If the fireproof / water proof cabinet is not available, they shall be stored in normal lockers.
* Whenever the backup media is moved to and from off-site location, the engineer in charge shall fill up the offsite backup movement form.
* The movement of backup tapes shall follow the information classification procedure.
* NDA will be signed by the courier company for physical transit of the backup tapes.
* The IT Team shall maintain the backup movement forms for the backups at off-site location.
* Logging
* The IT Team shall maintain the reports generated by the system on the data which has been backed up. The Head – IT shall review the log on a monthly basis.
* The backup movement logs for the backup at off-site location shall be maintained by the IT Team. The Head – IT shall review the log on a monthly basis.
* The backup test metrics shall be maintained by the IT team. The Head – IT shall review the log on a monthly basis.
* Tape Retention
* The tapes used for backup shall be retained as per the table mentioned below:
* Recommended tape retention:

| **Backup** | **Backup Type** | **Retention Period** |
| --- | --- | --- |
| Daily | Incremental | One Week |
| Weekly | Full Backup – Reset Archive Bit | One Month |
| Monthly | Full Backup – Reset Archive Bit | Two Years (24 Months) |

* Data Backed Up
* Data to be backed up include but not limited to the following information:
* File server
* Production Web server
* Production database server
* UAT Servers
* E-mail Servers

## Restoration Plan

The backup plan for various systems also contains a restoration plan. The restoration plan would also identify role responsible for the restoration checking (restoration operator).

## Backup Restoration

* Data recovery for any IT Asset shall be done only after taking the approval of the application / information / asset owner. The request for data recovery for any IT asset being used by projects shall be given using the backup request form.
* Before the data is restored, asset owner shall ensure that the correct version of data is being restored.
* Upon receiving the authorization, the data shall be restored by the IT team. The data restoration request received shall be updated with the status of the request.
* All the backup media, which were used for restoration, shall be returned to the off-site location, if applicable, after the restoration is complete.

## Backup Restoration Testing

* To verify the readability of backup media, restoration tests shall be carried out as per the request raised by the project / support team.
* IT team shall test the ability to restore data of server’s backup as per the restoration test plan document.
* Restoration logs shall be maintained as records for the restore results.
* The IT team will co-ordinate with the restoration requestor to ensure that the data restored is verified and confirmed by him / her.
* All the backup media, which were used for restoration, shall be returned to the off-site location, if applicable, after the restoration is complete.
* It shall be ensured that the restored data is deleted after successful completion of testing.

## Backup, Storage, Restoration Review

Application data backup storage and restoration at Rediff shall be audited on a regular basis, as defined in the **Activity Chart**, to ensure adherence and compliance with this policy. The responsible authority for this audit shall be as identified in the Activity Chart.

The Audit shall be done in the following parts:

* Review of backup procedures as implemented
* Review of backup storage – both on site and off site
* Review of restoration testing from a backup medium (both on site and off site)

The Management Steering Committee of {Company} must at pre-determined intervals, as defined in the **Activity Chart**, review the backup, storage and restoration testing processes. These are to be done by means of:

* Regular reports sent by backup / restoration operators
* Physical inspection of storage media
* Random checks to verify the authenticity of the backup
* Checking of the backup and restoration checklists
* Checking the media release records

Any deviations in these processes from this policy shall promptly be noted by the reviewer and action initiated to cover such deviations / flaws.

# Reference Documents

* ISMS Overview Policy
* ISO 27001:2013
* Statement of Applicability for ISO27001:2013
* Backup Register
* Logical Access Control Procedure
* Restoration Test Plan
* Backup Request Form
* Information Classification Policy