

Backup and Data Security Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Version: 1.2

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Document Revision History:

VERSION NO.	REVISION DATE	AUTHOR	REVIEWED BY	APPROVED BY	DESCRIPTION
1	28/6/2022	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed
1.1	28/6/2023	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed
1.2	28/7/2024	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed

1. Purpose

The purpose of this Backup Policy is to establish standardized procedures for backing up critical company data to ensure business continuity, data recovery, and compliance with data protection regulations. This policy ensures that backup processes are implemented, maintained, and tested to minimize data loss in the event of system failures, disasters, or other disruptions.

2. Scope

This policy applies to:

- All critical data stored on company systems, servers, and cloud-based platforms.
- All employees, contractors, and third parties are involved in the management and execution of data backups.
- All types of backup media, including physical and cloud-based storage.

3. Definitions

- Backup: A copy of data stored separately from the primary system to protect against loss, corruption, or disaster.
- Critical Data: Any data deemed essential for business operations, including databases, customer information, financial records, and intellectual property.
- **Backup Types:**
 - Full Back up: A complete copy of all data.
 - Incremental Backup: Only the data that has changed since the last backup is saved.
 - Differential Backup: All data that has changed since the last full backup is saved.

- **Backup Retention:** The length of time a backup is retained before being overwritten or deleted.

4. Backup Strategy

- **Frequency of Backups:**
 - Critical Data will be backed up daily to ensure minimal data loss.
 - Non-Critical Data will be backed up weekly or as deemed necessary.
 - System Backups will be performed at regular intervals (e.g., weekly full backup, daily incremental backup).
- **Backup Methods:**
 - Onsite Backup: Backup copies stored in physical locations (e.g., external drives, local servers).
 - Offsite Backup: Backup copies stored remotely in a secure cloud service or secondary physical location.
 - Cloud Backup: Backup copies using cloud-based storage services with strong security protocols (e.g., encrypted cloud services like AWS, Azure, Google Cloud).

5. Backup Procedures

- **Backup Process:**
 1. Identify the critical systems and data that require backup.
 2. Schedule regular backups based on the backup frequency defined above.
 3. Perform manual or automated backups using approved software tools.
 4. Verify that backup operations are successfully completed by reviewing logs and reports.
- **Testing of Backups:**
 - Regularly test backups to ensure they can be restored properly in the event of a data loss scenario.
 - Perform **quarterly restore tests** on a selected sample of backups to validate the integrity and accessibility of backup data.
- **Backup Storage:**
 - Store backups in secure locations, with offsite backups located in geographically separated data centers to mitigate the risk of localized disasters.

- Maintain a clear inventory of backup media, including their location and retention schedule.

6. Backup Retention and Disposal

- **Retention Period:**

- Full backups will be retained for [X] weeks/months before being overwritten.
- Incremental and differential backups will be retained for [Y] days/weeks/months.
- Long-term retention backups (e.g., archives) will be kept for [X] years as required by regulatory standards.

- **Backup Disposal:**

- Once a backup has reached the end of its retention period, it will be securely disposed of through methods such as data erasure or physical destruction of media.
- Ensure that any backup containing sensitive or classified data is destroyed securely to prevent unauthorized access.

7. Backup Monitoring and Reporting

- **Monitoring:**

- Backup processes will be continuously monitored for failures or irregularities.
- Backup status and performance reports will be reviewed regularly by IT administrators to ensure that backup procedures are effective.

- **Reporting:**

- A backup report will be generated after each backup cycle, detailing success/failure, data volume, and other relevant metrics.
- Any failures or anomalies must be reported immediately to the IT department for investigation and corrective action.

8. Roles and Responsibilities

- **IT Department:**

- Responsible for implementing and maintaining backup procedures, ensuring that backups are executed on schedule and verifying that backup data is recoverable.
- Manage backup storage, including the encryption, retention, and disposal of backups.

- **Employees:**
 - Follow the organization's data management policies and ensure that critical data is saved to the appropriate systems for backup.
- **Management:**
 - Oversee compliance with backup policies and ensure that necessary resources are allocated for backup processes.

9. Exceptions

Any exceptions to this policy, such as alternative backup strategies or custom retention periods, must be documented and approved by the IT department and senior management. Exceptions should be reviewed regularly for compliance.

10. Existing Setup

To ensure data integrity and availability, we have implemented a robust backup strategy that includes cloud storage, scheduled transfers, and critical backup solutions.

1. Cloud Dialer Backup

- **High Availability Mode:** All call recordings and reports are stored on the cloud in HA mode, providing redundancy and security against server failures.
- **Data Continuity:** In case of a server fault, the database remains intact and accessible.

2. Scheduled Recording Backup

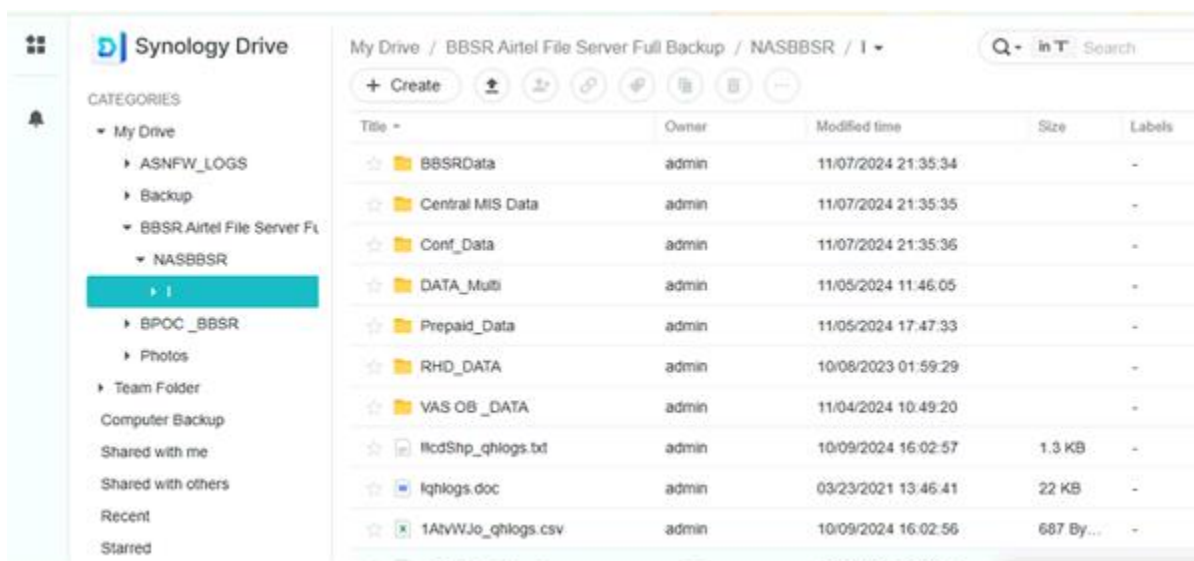
- **Daily Transfers:** Call recordings from both cloud servers are scheduled to back up automatically to the on-premises recording server at 7 PM daily.
- **Seamless Accessibility:** This ensures recordings are readily available locally, enhancing operational efficiency.

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings
```

```
Last login: Tue Nov 5 12:40:09 2024 from 10.14.215.1
ngucc@srrecosvr:~$ sudo su
[sudo] password for ngucc:
root@srrecosvr:/home/ngucc# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            7.7G   0  7.7G   0% /dev
tmpfs           1.6G  165M  1.4G  11% /run
/dev/mapper/ubuntu--vg-ubuntu--lv 915G  820G   57G  94% /
tmpfs           7.8G   0  7.8G   0% /dev/shm
tmpfs           5.0M   0  5.0M   0% /run/lock
tmpfs           7.8G   0  7.8G   0% /sys/fs/cgroup
/dev/loop3      92M   92M   0 100% /snap/lxd/24061
/dev/loop1      64M   64M   0 100% /snap/core20/1828
/dev/loop2      50M   50M   0 100% /snap/snapd/18357
/dev/loop0      41M   41M   0 100% /snap/snapd/20290
/dev/loop4      64M   64M   0 100% /snap/core20/2015
/dev/sdc1       2.0G  108M  1.7G   6% /boot
/dev/sdb        917G  703G  168G  81% /mnt/SDB
/dev/sda        1.8T  1.3T  509G  71% /mnt/SDC
/dev/sde        932G  522G  410G  56% /mnt/SDE
tmpfs           1.6G   0  1.6G   0% /run/user/1000
root@srrecosvr:/home/ngucc#
```

3. NAS Storage for Critical Data

- **Centralized Backup Solution:** Network-Attached Storage (NAS) is in place for storing critical backups, ensuring data redundancy and protection against unexpected failures.
- **Extended Retention:** NAS provides a secure, scalable solution for long-term backup needs.



The screenshot shows the Synology Drive web interface. On the left, the 'My Drive' sidebar is expanded, showing a hierarchy: My Drive > BBSR Airtel File Server Full Backup > NASBBSR > I. The main area displays a table of files and folders.

Title	Owner	Modified time	Size	Labels
BBSRData	admin	11/07/2024 21:35:34	-	-
Central MIS Data	admin	11/07/2024 21:35:35	-	-
Conf_Data	admin	11/07/2024 21:35:36	-	-
DATA_Multi	admin	11/05/2024 11:46:05	-	-
Prepaid_Data	admin	11/05/2024 17:47:33	-	-
RHD_DATA	admin	10/08/2023 01:59:29	-	-
VAS OB _DATA	admin	11/04/2024 10:49:20	-	-
llcdShp_ghlogs.txt	admin	10/09/2024 16:02:57	1.3 KB	-
lqhlogs.doc	admin	03/23/2021 13:46:41	22 KB	-
1AtvWJo_ghlogs.csv	admin	10/09/2024 16:02:56	687 By...	-