Standard Operating Procedure (SOP): Data Storage and Backup Procedures

This SOP describes **data storage and backup procedures** designed to protect vital information from loss or corruption. It covers guidelines for secure data storage, regular backup schedules, methods for backing up data both on-site and off-site, verification of backup integrity, data recovery processes, and responsibilities of personnel involved. The aim is to ensure data availability, integrity, and confidentiality through consistent and reliable backup practices.

1. Purpose

To establish protocols for secure data storage and comprehensive backup procedures to safeguard information against loss, corruption, or unauthorized access.

2. Scope

This SOP applies to all employees and contractors who manage, store, or access organization data, including servers, workstations, cloud resources, and portable devices.

3. Responsibilities

- **IT Administrator:** Implement, manage, and monitor backup solutions; verify backup integrity; test recovery processes.
- **Data Owners:** Identify critical data requiring backup; request recovery of data when needed.
- **All Employees:** Store data in authorized locations and report any issues or data loss incidents promptly.

4. Data Storage Guidelines

- All critical data must be stored on secured network drives, cloud platforms with proper encryption, or authorized local storage devices.
- Access to data should be restricted based on the principle of least privilege.
- Confidential and sensitive data should be encrypted at rest and during transfer.
- Regularly review and update data storage locations and permissions.

5. Backup Schedule

Data Type	Backup Frequency	Backup Location
File Servers & Shared Folders	Daily Incremental, Weekly Full	On-site & Off-site
Workstations	Weekly Full	On-site
Cloud Storage	Daily Snapshots	Cloud Backup
Databases	Daily Full, Hourly Incremental	On-site & Off-site

6. Backup Methods

- **On-Site Backups:** Use network-attached storage (NAS) devices, local backup servers, or tape drives for physical copy retention.
- **Off-Site Backups:** Transfer encrypted backups to secure off-site storage or trusted cloud backup services to ensure disaster recovery readiness.
- Automate backups where feasible to minimize human error.

7. Backup Integrity Verification

- Perform monthly test restores from both on-site and off-site locations to verify backup completeness and integrity.
- Monitor backup logs daily; address and resolve errors immediately.

8. Data Recovery Procedures

1. Report data loss or corruption to IT immediately.

2. IT Administrator verifies the scope and identifies the latest reliable backup version.
3. Restore data from backup to the original or alternate location as required.
4. Verify restored data integrity and functionality with the data owner.
5. Document the recovery incident and implement preventive measures, if applicable.

9. Security and Confidentiality

- Ensure all backups are encrypted both in transit and at rest.
- Backup storage must be physically secured or access-protected with strong credentials and multi-factor authentication where available.
- Backup media retired or disposed of must be securely wiped or destroyed according to data destruction policies.

10. Review and Updates

This SOP is reviewed annually, or when significant changes occur in technology, infrastructure, or business processes.

11. References

- Company Data Security Policy
- Disaster Recovery Plan
- Industry Compliance Guidelines