SOP: Backup and Archiving Procedures

Purpose:

This SOP establishes **backup and archiving procedures** to ensure the secure and systematic preservation of data. It covers the regular scheduling of data backups, secure storage methods for both primary and archived data, data integrity verification processes, retention policies, and restoration protocols. The objective is to minimize data loss, facilitate quick recovery in case of data corruption or hardware failure, and comply with regulatory requirements for data retention and security.

1. Scope

This procedure applies to all digital data maintained by [Organization Name], including operational files, databases, and critical business documents.

2. Responsibilities

- **IT Department:** Responsible for implementing, monitoring, and maintaining backups and archives.
- **Data Owners:** Ensure their data is included in the backup scope and report any discrepancies.
- **All Employees:** Follow guidelines regarding temporary storage and data retention.

3. Procedure

3.1 Backup Scheduling

- **Full Backups:** Performed weekly, capturing all designated data sets.
- **Incremental/Differential Backups:** Performed daily to capture changes since the last backup.
- **Backup Schedule Review:** Conducted quarterly to adjust for organizational or data set changes.

3.2 Storage Methods

- **Primary Backups:** Stored on secure, encrypted on-premises or certified cloud storage solutions.
- **Secondary Backups:** At least one copy stored offsite to mitigate risk of local disasters.
- **Archiving:** Data that is no longer actively used but must be retained, moved to archival storage with reduced access.

3.3 Data Integrity Verification

- Automated checksum or hash verification after each backup operation.
- Manual test restorations conducted quarterly to ensure data recoverability.

3.4 Retention Policy

- **Operational Backups:** Retained for a minimum of 30 days.
- **Archived Data:** Retained per legal or regulatory requirements, typically 3-7 years.
- Document and securely dispose of data once retention period elapses, following data destruction protocols.

3.5 Restoration Process

1. Restoration requests submitted to IT via [support ticket/email process].

2. IT confirms requester authorization and identifies relevant backup/archive.
3. Data restored to agreed location; integrity validated post-restoration.
4. Incident logged for auditing and review.

4. Compliance and Review

- Regular audits conducted to ensure adherence with policy and regulatory requirements.
- This SOP reviewed annually and upon significant system or regulatory changes.

5. References

- [Applicable regulatory requirements â€“ e.g., GDPR, HIPAA, etc.]
- Organizational IT Security Policy
- Data Retention Policy

Revision History

Date	Version	Description	Author
[YYYY-MM-DD]	1.0	Initial draft	[Name]