SOP Template: Backup and Recovery of Electronic Documents

This SOP details the **backup and recovery of electronic documents**, covering procedures for regular data backups, secure storage of backup copies, verification of data integrity, disaster recovery planning, and step-by-step recovery methods to restore lost or corrupted files. The goal is to ensure the protection and availability of critical electronic documents to minimize data loss and maintain business continuity.

1. Purpose

To establish standardized procedures for the backup and recovery of all electronic documents to prevent data loss, ensure data integrity, and support business continuity in the event of accidental deletion, corruption, or disaster.

2. Scope

This SOP applies to all employees and contractors who handle electronic documents within the organization, regardless of document format or storage medium.

3. Responsibilities

Role	Responsibility
IT Manager	Oversees backup infrastructure, schedules, and ensures compliance.
System Administrators	Executes backups, verifies data integrity, and conducts recovery tests.
Department Heads	Ensure departmental data is included in scheduled backups.
End Users	Store critical documents on approved storage systems and report data loss incidents.

4. Definitions

- **Backup:** A copy of electronic data stored separately for restoration purposes.
- **Recovery:** The process of restoring data from a backup to its original location or a new location.
- **Data Integrity:** The accuracy and consistency of stored data.
- **Disaster Recovery:** Procedures and policies for restoring critical IT infrastructure and data after a major incident.

5. Procedures

5.1 Regular Data Backups

- Schedule full system backups at least weekly; incremental/differential backups daily.
- Use automated backup software approved by IT.
- Confirm backup completion via system logs and email notifications.

5.2 Secure Storage of Backup Copies

- Store backup copies in a physically secure, access-controlled location.
- Maintain at least one offsite or cloud-based backup for disaster recovery.
- Encrypt all backup data in transit and at rest.

5.3 Verification of Data Integrity

- Perform monthly test restores of sampled backup files to verify usability.
- Implement backup checksums or hash verifications for data integrity.

5.4 Disaster Recovery Planning

- Maintain a current, documented disaster recovery plan accessible to all staff.
- Define critical data and systems and prioritize their recovery sequence.
- Conduct annual disaster recovery drills and update plans as needed.

5.5 Step-by-Step Recovery Methods

1. **Identify** the missing, lost, or corrupted files and their last known backup time.
2. **Notify** the IT team or designated authority of the incident.
3. **Access** backup software or storage to locate the correct backup copy.
4. **Restore** files to their original directory or a protected staging location.
5. **Verify** that restored files are accurate, complete, and functional.
6. **Document** the incident and recovery steps taken.

6. Documentation and Records

- Maintain backup logs and reports for a minimum of 12 months.
- Document all incidents of data loss and recovery actions in the designated logbook or system.

7. Review and Revision

- SOP to be reviewed annually or following significant changes to IT infrastructure or processes.
- All revisions to be documented with version history and approval signatures.

8. References

- Company IT Security Policy
- Disaster Recovery Plan
- Data Protection & Privacy Policy

Version History

Version	Date	Description
1.0	2024-06	Initial draft