SOP Template: Backup and Disaster Recovery Guidelines

This SOP details **backup and disaster recovery guidelines**, encompassing data backup procedures, frequency and storage methods, disaster recovery planning, roles and responsibilities during recovery, system restoration processes, data integrity verification, and regular testing of recovery plans. The objective is to ensure data protection, minimize downtime, and maintain business continuity in the event of data loss, system failure, or other disasters.

1. Purpose

To define the processes and responsibilities required for effective data backup and disaster recovery, ensuring minimal business disruption and secure data restoration.

2. Scope

This procedure applies to all critical business systems and data managed by the IT department and authorized personnel.

3. Responsibilities

Role	Responsibility
IT Manager	Oversee backup and recovery processes; update SOP regularly.
System Administrators	Implement and monitor scheduled backups; execute recovery as needed.
Users	Report data loss incidents; follow best practices for data storage.

4. Data Backup Procedures

1. Identify critical data and systems requiring backup.
2. Configure automated daily incremental and weekly full backups.
3. Secure backup storage in at least two locations: primary onsite and secondary offsite/cloud.
4. Label and document all backup sets.

5. Backup Frequency and Storage Methods

- **Incremental Backup:** Daily, stored locally and in the cloud.
- **Full Backup:** Weekly, retained both onsite and offsite.
- **Retention Policy:** Maintain backups for at least 90 days; older backups archived as necessary.

6. Disaster Recovery Plan

1. Assess the scope and impact of the disaster.
2. Initiate the disaster recovery team and communicate action plan.
3. Prioritize restoration of critical systems and operations.
4. Recover data from the most recent valid backup.
5. Verify system and data integrity before bringing systems online.

7. System Restoration Process

1. Restore affected systems using established recovery images or backup data.
2. Validate the restoration by conducting functional and data integrity tests.
3. Document restoration actions and outcomes.

8. Data Integrity Verification

- Use checksum and validation tools to verify backup data integrity.
- Periodically perform test restorations to ensure recoverability.

9. Testing and Review

1. Conduct disaster recovery drills at least twice yearly.
2. Review and update recovery plans based on drill outcomes and system changes.

10. Review and Maintenance

This SOP should be reviewed biannually or after any major incident, update, or organizational change.

11. References & Related Documents

- Business Continuity Plan
- IT Security Policy
- System Inventory List

12. Approvals

Prepared by: ____________________
Approved by: ____________________
Date: ____________________