SOP: Backup and Disaster Recovery Instructions

This SOP details **backup and disaster recovery instructions**, including data backup schedules, storage methods, recovery point objectives, disaster recovery plan activation, system restoration procedures, data integrity verification, communication protocols, and regular testing of recovery processes. The goal is to ensure business continuity by protecting critical data and enabling swift recovery from data loss or system failures.

1. Purpose

To outline standardized procedures for backing up organizational data and recovering systems in the event of a disaster, thereby minimizing downtime and data loss.

2. Scope

This SOP applies to all critical IT systems and data managed by the organization.

3. Definitions

- **Backup:** A copy of data stored at a location separate from the original.
- **Disaster Recovery (DR):** The process of restoring systems and data after a disruptive event.
- **Recovery Point Objective (RPO):** Maximum acceptable amount of data loss measured in time.
- **Recovery Time Objective (RTO):** Maximum acceptable time to restore service after a disaster.

4. Responsibilities

- **IT Manager:** Oversee backup and DR processes.
- **System Administrators:** Execute backups, restorations, and tests.
- **All Staff:** Report incidents promptly.

5. Procedures

5.1 Data Backup Schedule

Data Type	Backup Frequency	Backup Type	Retention Period
Critical Databases	Daily (incremental), Weekly (full)	Full/Incremental	30 days
User Files	Nightly	Differential	14 days
System Configuration	Weekly	Full	60 days

5.2 Storage Methods

- Primary backups stored on secure network-attached storage (NAS).
- Secondary copies replicated off-site (cloud storage or remote data center).
- Periodic offline backups (external drives, tapes) as needed.
- Backups encrypted at rest and in transit.

5.3 Recovery Point Objectives (RPOs)

- Critical business data: RPO ≤ 24 hours
- System files: RPO ≤ 72 hours

5.4 Disaster Recovery Plan Activation

1. Identify incident and assess scope (data loss, system failure, etc.).
2. Notify DR Team and management as per communication protocol.
3. Declare disaster and activate DR plan if downtime/data loss exceeds RPO/RTO.

5.5 System Restoration Procedures

1. Isolate affected systems to prevent further damage.
2. Verify backup integrity before restoration.

3. Restore data/software from most recent, verified backup.
4. Validate system functionality post-restoration.
5. Document all actions taken.

5.6 Data Integrity Verification

- Perform checksum/hash validation on restored files.
- Conduct spot checks on randomly selected data.

5.7 Communication Protocols

- Immediate notification of key stakeholders in event of disaster.
- Regular updates to management and affected users throughout the recovery process.
- Post-event debrief for continuous improvement.

5.8 Regular Testing of Recovery Processes

- Quarterly backup restoration drills.
- Annual full DR simulation tests.
- Document test results and address deficiencies.

6. Documentation and Records

- Maintain logs of all backups, restorations, and DR tests.
- Retain incident reports for at least 12 months.

7. Review and Update

This SOP should be reviewed annually or after any significant incident involving data loss or disaster recovery.

8. References

- Organizational IT Security Policy
- Vendor Backup Solution Manuals