SOP Template: Backup, Restore, and Data Recovery Procedures

This SOP details **backup, restore, and data recovery procedures** to ensure the integrity and availability of critical data. It covers scheduled backup routines, storage protocols for backup media, data restoration processes in case of data loss or corruption, verification and testing of backup data, roles and responsibilities for data recovery, and documentation of recovery activities. The aim is to minimize downtime and data loss, maintaining business continuity and protecting organizational information assets.

1. Purpose

To establish standardized procedures for backing up, restoring, and recovering data to mitigate risks associated with data loss and ensure prompt recovery and continuity of business operations.

2. Scope

This SOP applies to all personnel, systems, and data assets within the organization requiring backup and recovery provisions.

3. Definitions

- **Backup:** The process of creating copies of data to protect against data loss.
- **Restore:** The process of returning data from a backup to an operational state.
- **Data Recovery:** The process of retrieving data that has been lost, corrupted, or made inaccessible.

4. Roles and Responsibilities

Role	Responsibility
IT Manager	Approving backup strategies; oversight of backup, restore, and data recovery.
System Administrators	Executing backup/restore tasks; monitoring backup jobs; testing recovery processes.
Data Owners	Identifying critical data; requesting and validating restoration as needed.
Compliance Officer	Ensuring adherence to regulatory and organizational policies regarding data backup and retention.

5. Backup Procedures

1. **Backup Schedule:**
    - Perform daily incremental backups and weekly full backups for critical systems.
    - Backup non-critical systems weekly or as specified in the data retention policy.
2. **Backup Media & Storage:**
    - Use secure, encrypted storage media (onsite and offsite/cloud).
    - Label and store physical backup media in a secure, access-controlled environment.
3. **Backup Monitoring & Logging:**
    - Monitor backup jobs and review logs daily for errors or failures.

6. Data Restoration Procedures

1. Initiate a restoration request through the Service Desk or IT ticket system.
2. Verify existence and integrity of backup data for requested date/version.
3. Restore data to the specified location, ensuring minimal disruption to business operations.
4. Notify the Data Owner and verify data integrity post-restoration.

7. Data Recovery Procedures

1. Assess the nature, scope, and impact of data loss or corruption.
2. Determine the latest valid backup and begin the recovery process as per restoration procedure.
3. Document root cause and corrective actions taken during recovery.
4. Communicate status and resolution to stakeholders.

8. Verification and Testing

- Conduct scheduled tests of backup restores (at least quarterly).
- Verify backup data integrity and accessibility after each backup session.
- Document testing outcomes and address deficiencies promptly.

9. Documentation and Record-Keeping

- Maintain detailed logs of backup and restore activities.
- Document incidents of data loss, recovery actions, and outcomes.
- Archive records according to the data retention policy.

10. Review and Revision

- Review this SOP annually or when significant changes to systems or procedures occur.

11. References

- Data Retention Policy
- Information Security Policy
- Regulatory Compliance Requirements

12. Approval

SOP Owner	_____
Approval Date	_____
Next Review Date	_____