SOP: Periodic System Backup and Data Recovery Procedures

This SOP defines the **periodic system backup and data recovery procedures**, covering scheduled data backups, secure storage of backup files, verification of backup integrity, restoration process in case of data loss, roles and responsibilities, and preventive measures to minimize data loss. The goal is to ensure data availability, integrity, and quick recovery to maintain business continuity and minimize downtime during system failures or data corruption incidents.

1. Purpose

To establish consistent processes for system backup, storage, recovery, and verification to safeguard organizational data and ensure business continuity.

2. Scope

This SOP applies to all information systems, applications, and relevant data assets managed within the organization.

3. Definitions

- **Backup:** A copy of data taken to restore the original after data loss.
- **Restore:** The process of copying backup data to its original or alternative location after a data loss event.
- **Integrity Verification:** Process of ensuring backup data is complete and uncorrupted.

4. Roles and Responsibilities

Role	Responsibility
IT Manager	Approve backup schedules and procedures; oversee recovery processes.
System Administrators	Perform backups, verify integrity, and manage secure storage of backup files.
Disaster Recovery Team	Lead data restoration in case of incidents and coordinate with stakeholders.
End Users	Report any suspected data loss promptly.

5. Backup Procedures

1. **Backup Schedule:**
    - Full backups: Weekly (Every Sunday 2 AM)
    - Differential/incremental backups: Daily (2 AM Mondayâ€“Saturday)
    - Offsite/cloud backups: Weekly (Every Sunday after full backup)
2. **Backup Media:**
    - Use certified external drives, network storage, or encrypted cloud services.
3. **Secure Storage:**
    - Store backup files in physically secure and access-controlled locations.
    - Maintain multiple backup copies (onsite, offsite, cloud).
4. **Labeling and Retention:**
    - Label backups by date and type.
    - Retain full backups for a minimum of 3 months; incremental for 1 month.

6. Backup Integrity Verification

1. Verify backup job logs daily.
2. Perform monthly test restores to confirm data integrity and recoverability.
3. Document and address any backup failures immediately.

7. Data Recovery Procedure

1. Identify affected systems and the extent of data loss.
2. Notify IT manager and Disaster Recovery Team.
3. Select the most recent valid backup for restoration.
4. Restore data to designated location and verify completeness.
5. Document incident, actions taken, and lessons learned.

8. Preventive Measures

- Regular system updates and patch management.
- Access controls and authentication for backup files.
- Periodic staff training on data loss prevention.
- Review and update backup and recovery SOP annually.

9. Documentation and Reporting

- Maintain comprehensive logs of all backup and restoration activities.
- Report backup failures and recovery incidents to management.
- File regular compliance reports as required by regulations.

10. Review and Revision

This SOP shall be reviewed annually and updated as necessary to reflect changes in technology, business processes, or compliance requirements.

Approval Date: ____________ *Next Review Date:* ____________