Standard Operating Procedure (SOP): Regular Document Backup Protocols

This SOP details **regular document backup protocols**, including the scheduling of automatic backups, storage best practices, data verification processes, and recovery procedures. The goal is to protect critical documents from data loss due to hardware failures, accidental deletions, malware attacks, or other unforeseen events by ensuring consistent and secure backup operations.

1. Scope

This SOP applies to all employees and departments responsible for managing and storing organizational documents, both digital and physical (where digital backup is applicable).

2. Responsibilities

- **IT Department:** Implements, monitors, and maintains the backup system.
- **Department Heads:** Ensure compliance with backup protocols within their teams.
- **All Staff:** Follow protocols for document storage and report any anomalies or issues.

3. Backup Scheduling

- Automatic full backups shall be scheduled **daily at 2:00 AM** for all critical document directories.
- Incremental backups will occur every **4 hours** during business hours (8:00 AM â€“ 8:00 PM).
- Backup schedules should be reviewed and adjusted quarterly or as necessary.

4. Storage Best Practices

- Backup data must be stored in at least **two separate locations** (e.g., on-premises server and secure cloud storage).
- Backup media (external drives, tapes) should be kept in locked, fireproof storage when not in use.
- All backup storage must be encrypted and access restricted to authorized personnel only.
- Retain daily backups for 7 days, weekly backups for 6 months, and monthly backups for 1 year.

5. Data Verification Process

- Automatic backup jobs must generate and log a report of completion and any errors.
- The IT department must verify backup integrity weekly using checksum comparison or test file restores.
- Any failed backup or verification process must be escalated to the IT manager within 24 hours.

6. Recovery Procedures

- Requests for document restoration should be submitted via the helpdesk system.
- Restoration requests must be fulfilled within 24 hours for critical documents and within 3 business days for non-critical documents.
- All restoration processes must be logged, and users should verify recovered data for completeness and accuracy.

7. Review and Improvement

- This SOP will be reviewed **annually** or after any significant data loss incident.
- Feedback or suggested improvements should be submitted to the IT department for assessment.

8. References

- Company IT Security Policy
- Data Protection and Retention Policy

9. Approval

Prepared by: _____
Approved by: _____
Date: _____