SOP: Database Backup and Recovery Processes

This SOP details the comprehensive **database backup and recovery processes**, covering regular backup schedules, types of backups, storage and encryption methods, verification and testing of backup integrity, recovery procedures for different failure scenarios, and roles and responsibilities for database administrators. The goal is to ensure data availability, integrity, and quick restoration in case of data loss or corruption.

1. Purpose

To define procedures for the backup and recovery of all organization-managed databases, ensuring business continuity and data protection.

2. Scope

This SOP applies to all production, development, and test databases managed by the IT Department.

3. Responsibilities

Role	Responsibility
Database Administrator (DBA)	Perform backups, test restores, maintain backup logs, initiate recovery as needed.
IT Manager	Review and approve backup schedules and strategies. Escalate issues.
Infrastructure/Storage Team	Manage backup storage solutions and ensure integrity of backup hardware.

4. Backup Schedule

- **Full Backups:** Performed weekly every Sunday at 2:00 AM.
- **Incremental Backups:** Performed daily at 2:00 AM (except Sunday).
- **Transaction Log Backups:** Performed hourly for critical databases.

5. Types of Backups

- Full Backup: Complete copy of the database including all data and metadata.
- Differential Backup: Contains changes since the last full backup.
- Incremental Backup: Contains changes since the last backup of any type.
- Transaction Log Backup: Backup of database transaction logs for point-in-time recovery.

6. Storage and Encryption

- **Primary Storage:** Backups stored on secure, redundant on-premises storage.
- **Secondary Storage:** Copies sent to offsite/cloud storage for disaster recovery.
- **Encryption:** All backup files must use AES-256 encryption for data at rest and in transit.

7. Verification and Integrity Checks

1. Post-backup, use checksum/hash verification to ensure file integrity.
2. Perform quarterly restoration tests on random backup sets.
3. Maintain logs of all verification and test results.

8. Recovery Procedures

1. **Identify Failure Type:** Classify event as accidental deletion, corruption, or catastrophic disk failure.
2. **Select Appropriate Backup:** Use the latest valid backup appropriate to the situation.
3. **Restore Process:**
    - Restore full backup, then apply incremental/differential and transaction log backups as needed.
    - For point-in-time recovery, apply transaction logs up to the desired time.
4. **Validation:** Perform post-recovery testing and validation to ensure data consistency.
5. **Notification:** Communicate status and post-mortem to stakeholders.

9. Documentation and Logs

- Maintain detailed logs of all backup and restore operations.
- Archive logs securely for one year.
- Document all incidents, procedures followed, and outcomes.

10. Review and Update

This SOP shall be reviewed and updated annually, or after any significant change in IT infrastructure.

11. References

- Company Data Protection Policy
- Disaster Recovery Plan
- Vendor Backup & Recovery documentation