Disaster Recovery Protocol for Databases

1. Objective

To outline the procedures and responsibilities for responding to database disasters to ensure data integrity, availability, and minimal downtime.

2. Scope

This protocol applies to all production databases managed by the organization, including on-premises and cloud-hosted environments.

3. Disaster Scenarios

- Hardware Failure
- Software Corruption
- Data Deletion or Loss
- Natural Disasters
- Security Breaches

4. Roles and Responsibilities

Role	Responsibility
Database Administrator (DBA)	Leads disaster response, initiates recovery procedures
IT Manager	Approves recovery steps, communicates status
Support Team	Assists with technical tasks and documentation

5. Recovery Steps

1. **Incident Detection**
   - Monitor alerts and user reports
   - Confirm disaster scenario
2. **Assessment**
   - Determine extent of data loss or corruption
   - Identify affected systems
3. **Notification**
   - Notify IT Manager and Support Team
   - Document incident details
4. **Recovery**
   - Restore database from latest valid backup
   - Apply transaction logs if applicable
   - Validate integrity and consistency
5. **Validation**
   - Test restored database with critical queries
   - Confirm with stakeholders

6. **Resumption**
    - Reconnect applications
    - Resume normal operations

7. **Post-Incident Review**
    - Document root cause and recovery performance
    - Update protocol as needed

6. Backup Policy

- Full backup: Daily at 2:00 AM
- Incremental backup: Hourly
- Offsite backup replication: Every 24 hours
- Retention period: 30 days

7. Contact Information

Team	Email	Phone
Database Support	db-support@example.com	+1 234 567 8901
IT Manager	it-manager@example.com	+1 234 567 8902

8. Revision History

Date	Version	Description
2024-06-01	1.0	Initial release