Disaster Recovery Plan (DRP)

Plan ID: 1

Purpose & Scope: This Disaster Recovery Plan (DRP) provides comprehensive procedures for recovering

Regulatory References: ISO 27001:2013, RBI IT Framework, NIST Cybersecurity Framework, SOX Compl

Critical Systems: Core Banking API, Payment Gateway, Database Servers, Web Application Servers, Loac

Critical Applications: Core Banking System, Payment Processing Engine, Customer Portal, Mobile Banking

RTO Targets:

Core Banking API: 2 hours

Payment Gateway: 1 hour

Database Servers: 4 hours

Web Application Servers: 6 hours

Load Balancers: 30 minutes

Firewall Systems: 1 hour

RPO Targets:

Core Banking API: 5 minutes

Payment Gateway: 1 minute

Database Servers: 15 minutes

Web Application Servers: 30 minutes

Load Balancers: 0 minutes

Firewall Systems: 5 minutes

Disaster Declaration Process:

Disaster declaration requires approval from CTO and COO. Assessment criteria include: system unavailability > 4 hours, data corruption detected, security breach confirmed, or physical damage to infrastructure.

Data Backup Strategy:

Multi-tier backup strategy: Real-time replication to DR site, hourly incremental backups, daily full backups, weekly archival backups. Offsite storage with 30-day retention. Encrypted backups with separate key management. Regular backup validation and restoration testing.

Recovery Site Details:

Primary DR site located in Mumbai with 99.9% uptime SLA. Secondary DR site in Delhi for geo-redundancy. Hot standby systems with automatic failover capability. Network connectivity via multiple ISPs with automatic routing. Power backup with 72-hour capacity.

Failover Procedures:

1. Detect failure via monitoring systems
2. Verify disaster declaration criteria
3. Activate DR site systems
4. Redirect network traffic
5. Validate data integrity
6. Restore application services
7. Notify stakeholders
8. Monitor system performance

Testing & Validation Schedule:

Monthly backup restoration tests, Quarterly DR drills, Annual full-scale DR testing, Continuous monitoring validation, Post-change testing for all system updates, Regular security testing and validation.

Maintenance & Review Cycle:

DRP reviewed quarterly with updates to contact lists and procedures. Annual comprehensive review including technology updates and regulatory changes. Post-incident review within 48 hours of any DR activation. Continuous improvement based on testing results.