Disaster Recovery Plan for Cloud Data

1. Purpose

This document outlines the disaster recovery plan for ensuring the availability, integrity, and confidentiality of critical cloud-hosted data in the event of disruptive incidents.

2. Scope

This plan applies to all cloud data services, storage, and relevant infrastructure used by the organization.

3. Objectives

- Minimize downtime and data loss.
- Define recovery time (RTO) and recovery point objectives (RPO).
- Outline roles, responsibilities, and procedures during a disaster.

4. Roles & Responsibilities

Role	Responsibility
DR Manager	Plan activation, coordination, communication
IT Team	Technical recovery, cloud infrastructure restoration
Data Owners	Data validation and integrity checks

5. Risk Assessment Summary

- Cloud provider outage
- Data corruption or loss
- Cyber-attacks (e.g., ransomware)
- Human error

6. Preventive Measures

- Daily automated cloud backups
- Multi-region data replication
- Access controls and MFA
- Regular vulnerability scans

7. Disaster Recovery Procedures

1. Assess incident severity and impact.
2. Notify DR Team and key stakeholders.
3. Activate DR site/resources as appropriate.
4. Restore data from latest clean backups.
5. Test functionality and user access.
6. Communicate recovery status.

8. Recovery Objectives

- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 1 hour

9. Testing & Maintenance

- Conduct semi-annual recovery drills.
- Review backup logs weekly.
- Update this plan annually or after significant changes.

10. Contact Information

Name/Role	Email	Phone
DR Manager	dr.manager@example.com	+123 456 7890
Cloud Support Lead	cloud.lead@example.com	+123 555 7890