Standard Operating Procedure (SOP)

Disaster Recovery and Data Backup Procedures

This SOP details the **disaster recovery and data backup procedures** designed to protect critical information and ensure business continuity. It includes guidelines for regular data backups, secure storage of backup copies, recovery point objectives, recovery time objectives, roles and responsibilities during a disaster, testing and validation of recovery plans, and steps to restore systems and data after incidents such as hardware failures, data corruption, natural disasters, or cyber-attacks. The aim is to minimize data loss and downtime by implementing efficient recovery strategies and maintaining up-to-date backups.

1. Purpose

To define processes and responsibilities for backing up data, securely storing backup copies, and efficiently restoring systems and information in the event of disaster, minimizing data loss and downtime.

2. Scope

This procedure applies to all organizational data, systems, applications, and IT infrastructure deemed critical for business operations.

3. Definitions

- **Recovery Point Objective (RPO):** The maximum tolerable period in which data might be lost.
- **Recovery Time Objective (RTO):** The maximum tolerable amount of time taken to restore systems back to normal.
- **Backup:** A copy of data stored separately for restoration in case of data loss.
- **Disaster:** Any unplanned event disrupting business operations, such as hardware failure, cyber-attack, or natural disaster.

4. Roles and Responsibilities

Role	Responsibilities
IT Manager	Oversee backup and disaster recovery planning and execution; coordinate recovery efforts.
System Administrators	Perform backups, monitor backup status, and initiate restoration procedures as needed.
Data Owners	Identify critical data and ensure regular updates regarding data importance and location.
All Staff	Report incidents, follow procedures, and support recovery efforts as directed.

5. Procedures

5.1 Regular Data Backups

1. Identify all critical systems and data that require backups.
2. Establish backup schedules (e.g., daily, weekly, monthly) in line with RPO requirements.
3. Use automated backup solutions wherever possible to minimize manual errors.

5.2 Secure Storage of Backup Copies

1. Store backup copies in location(s) physically separate from the primary data center (offsite/cloud).
2. Encrypt backup data both in transit and at rest.
3. Restrict access to backup storage to authorized personnel only.

5.3 Recovery Objectives

- Define and document RPO and RTO for each critical system and dataset.
- Review and update objectives periodically, or as business needs change.

5.4 Disaster Recovery Plan Activation

1. In the event of disaster, assess the scope of impact and activate the Disaster Recovery Plan.
2. Notify all relevant stakeholders and disaster recovery team members.
3. Begin restoration according to pre-defined priorities (based on RTO/RPO).

5.5 System and Data Restoration Steps

1. Retrieve most recent unaffected backup copy for restoration.
2. Follow documented restoration protocols for systems and applications.
3. Validate the integrity of restored data and perform system testing.
4. Communicate recovery status to stakeholders.

5.6 Testing and Validation

1. Perform regular (at least annual) DR and backup restoration tests.
2. Document outcomes, remediate issues, and update procedures as necessary.

6. Review and Maintenance

1. Review this SOP annually or whenever significant system changes occur.
2. Update procedures to reflect new risks, technologies, or business requirements.