

# Disaster Recovery Data Backup Policy Guidelines

Document Version: 1.0

Last Reviewed: [Date]

---

## 1. Purpose

The purpose of this policy is to define the requirements for data backup and recovery to ensure the preservation, protection, and restoration of critical information in the event of a disaster or data loss incident.

## 2. Scope

This policy applies to all employees, contractors, and third-party providers responsible for managing, storing, or processing organizational data.

## 3. Policy Guidelines

### 3.1 Backup Frequency

- Full backups must be performed at least once per week.
- Incremental or differential backups should be performed daily, or as defined by system criticality.

### 3.2 Data to be Backed Up

- All mission-critical systems and data repositories.
- Databases, files, configurations, and any other essential digital assets.
- Backup scope should be reviewed and updated regularly.

### 3.3 Backup Storage and Retention

- Backups must be stored in secure, access-controlled locations.
- At least one backup copy must be kept offsite or in geographically separate locations.
- Retention periods should comply with legal, regulatory, and business requirements.

### 3.4 Backup Protection

- Backup data must be encrypted both in transit and at rest.
- Access to backup files must be restricted and monitored.

### 3.5 Testing and Verification

- Backup and restoration procedures must be tested at least annually.
- Testing should verify data integrity and completeness.
- Issues identified during tests must be documented and addressed promptly.

### 3.6 Roles and Responsibilities

- IT staff are responsible for performing backups and restorations.
- Department managers ensure critical data is identified for backup.

- Employees must report data loss incidents promptly.

## 4. Compliance and Review

Compliance with this policy will be reviewed periodically. Any violations may result in disciplinary action. This policy will be reviewed and updated as necessary to reflect changes in technology or business requirements.

## 5. References

- [Insert relevant laws, standards, and regulatory requirements]
- 

### Approval:

Name: \_\_\_\_\_ Date: \_\_\_\_\_