**Backup and Recovery Strategy Document**

**1. Backup Strategy**

**Backup Types**

To ensure comprehensive data protection, the following backup types will be implemented:

1. **Full Backup**
   * **Frequency**: Weekly (every Sunday at 2:00 AM)
   * **Scope**: Complete backup of all critical data and systems.
2. **Differential Backup**
   * **Frequency**: Daily (at 11:00 PM)
   * **Scope**: Captures all changes since the last full backup.
3. **Transaction Log Backup** (For databases)
   * **Frequency**: Every 4 hours
   * **Scope**: Ensures point-in-time recovery for databases.
4. **Real-time Replication** (For mission-critical systems)
   * **Scope**: Continuous synchronization to a secondary site for high availability.

**2. Recovery Objectives**

* **Recovery Time Objective (RTO)**: **2 hours** (Maximum acceptable downtime).
* **Recovery Point Objective (RPO)**: **15 minutes** (Maximum acceptable data loss).

**3. Backup Storage Locations**

To mitigate risks of data loss due to disasters, backups will be stored in multiple locations:

* **Primary Data Center**: On-site backups for quick recovery.
* **Secondary Data Center**: Geographically distant (at least 500 miles away) for disaster recovery.
* **Cloud Backup**: Encrypted with **AES-256** military-grade encryption.
* **Offline Tape Backups**: Stored in a secure, fireproof vault for critical long-term retention.

**4. Recovery Procedure**

In case of data loss or system failure, the following steps will be executed:

1. **Immediate System Isolation**
   * Identify and contain the affected systems to prevent further corruption.
2. **Comprehensive Damage Assessment**
   * Determine the cause (cyberattack, hardware failure, human error).
   * Identify the most recent uncorrupted backup.
3. **Backup Restoration**
   * Restore from the latest **full backup** followed by the most recent **differential/log backups**.
   * For databases, apply transaction logs to reach the nearest recovery point.
4. **Data Integrity Verification**
   * Validate restored data using checksums and automated integrity checks.
5. **Gradual System Restoration**
   * Bring non-critical systems online first, followed by core services.
6. **Post-Incident Analysis**
   * Document the root cause, lessons learned, and improvements for future resilience.

**5. Testing & Maintenance**

* **Quarterly Disaster Recovery Drills**: Simulate failures to validate recovery procedures.
* **Automated Backup Health Checks**: Daily verification of backup integrity.
* **Retention Policy**:
  + Full backups retained for **30 days**.
  + Critical data archived for **7 years** (compliance requirements).