**Backup and Recovery Mechanisms**

**1. Introduction**

Data loss can severely impact business continuity, making a well-defined **backup and recovery** strategy essential. This document outlines a comprehensive backup plan, recovery objectives, and the step-by-step process to restore data efficiently.

**2. Backup Strategy**

A robust backup strategy ensures that data can be recovered with minimal downtime. The following backup mechanisms will be implemented:

**Backup Types and Frequency**

| **Backup Type** | **Description** | **Frequency** |
| --- | --- | --- |
| **Full Backup** | Complete copy of all data and system configurations. | Weekly (Sunday) |
| **Differential Backup** | Backs up data changed since the last full backup. | Daily (Every Night) |
| **Transaction Log Backup** | Captures all database transactions since the last backup, ensuring minimal data loss. | Every 4 hours |
| **Real-time Replication** | Continuous mirroring of critical systems to a secondary site. | Continuous |

**3. Recovery Objectives**

To minimize the impact of data loss, the following recovery objectives are defined:

| **Objective** | **Definition** | **Target** |
| --- | --- | --- |
| **Recovery Time Objective (RTO)** | Maximum acceptable downtime after a failure. | **2 hours** |
| **Recovery Point Objective (RPO)** | Maximum acceptable data loss from the last backup. | **15 minutes** |

**4. Backup Locations**

Multiple storage locations are used to ensure data is always accessible, even in the event of disasters.

1. **Primary Data Center:** On-site storage for quick recovery.
2. **Geographically Dispersed Secondary Data Center:** Ensures redundancy in case of primary site failure.
3. **Cloud Backup:** Encrypted cloud storage for additional security and accessibility.
4. **Offline Tape Backups:** Securely stored tapes in a physically separate location for long-term archival and disaster recovery.

**5. Recovery Procedure**

In case of data loss, the following recovery procedure is followed:

**Step-by-Step Recovery Plan**

1. **Immediate System Isolation**
   * Disconnect the affected system from the network to prevent further damage (e.g., ransomware attacks, data corruption).
2. **Comprehensive Damage Assessment**
   * Identify the extent of the failure.
   * Determine whether data loss is due to hardware failure, cyber-attack, or accidental deletion.
3. **Backup Restoration from Most Recent Clean Point**
   * Retrieve the most recent **full backup** and apply the latest **differential** and **transaction log backups**.
   * For real-time replicated data, initiate failover to the secondary data center.
4. **Data Integrity Verification**
   * Check database consistency using checksum validation.
   * Verify application functionality and logs to ensure no corruption.
5. **Gradual System Restoration**
   * Restore services in stages to avoid overload and detect issues early.
   * Prioritize critical services like authentication systems, databases, and web applications.
6. **Post-Incident Analysis**
   * Conduct a root cause analysis to prevent recurrence.
   * Improve backup and recovery processes based on findings.
   * Update security policies and conduct a post-mortem report.

**6. Monitoring and Testing**

To ensure effectiveness, backups are regularly tested:

1. **Daily Backup Verification:** Automated integrity checks.
2. **Monthly Recovery Drills:** Simulated disaster recovery scenarios.
3. **Annual Full Disaster Recovery Simulation:** Complete restoration test to ensure readiness.

**7. Security and Compliance**

* **Encryption:** All backups use **AES-256 encryption** for data at rest and **TLS 1.3** for data in transit.
* **Access Controls:** Role-Based Access Control (RBAC) limits access to backup systems.
* **Regulatory Compliance:** Aligns with **GDPR, HIPAA, ISO 27001** requirements.

**8. Conclusion**

This backup and recovery strategy ensures that **data remains protected, downtime is minimized, and business operations can quickly resume** in case of disruptions. Regular testing and updates will keep the plan effective and aligned with evolving risks.