**Backup and Recovery Mechanisms**

**1. Backup Strategy**

A well-defined backup strategy ensures business continuity in the face of data loss, corruption, or disaster.

**Backup Types and Schedule**

| **Backup Type** | **Frequency** | **Description** |
| --- | --- | --- |
| **Full Backup** | Weekly (e.g., Sunday 2 AM) | Captures entire system or database; used as a baseline for all other backups. |
| **Differential Backup** | Daily (e.g., Mon–Sat 2 AM) | Captures changes since the last full backup. Faster than full but larger than incremental. |
| **Transaction Log Backup** | Every 4 hours | Backs up DB transaction logs to minimize data loss in high-change systems. |
| **Real-time Replication** | Continuous | Mirrors production systems in near real-time for mission-critical services. |

**2. Recovery Objectives**

Clearly defined recovery goals help set expectations and drive infrastructure design.

* **Recovery Time Objective (RTO)**  
  ⏱️ Maximum allowable **downtime**: **2 hours**
* **Recovery Point Objective (RPO)**  
  📉 Maximum allowable **data loss**: **15 minutes**

These objectives ensure rapid service restoration and minimal operational impact.

**3. Backup Locations**

Data backups must be resilient to localized failures and disasters.

**Redundant, Geographically Dispersed Storage Strategy**

| **Location** | **Purpose** |
| --- | --- |
| **Primary Data Center** | On-site access to recent backups; fast recovery for minor incidents. |
| **Secondary Data Center** *(Geo-Redundant)* | Disaster recovery site; ensures business continuity in case of regional outages. |
| **Cloud Backup** *(Encrypted)* | Long-term archival; encrypted with **AES-256**, access via RBAC. |
| **Offline Tape Backup** | Air-gapped storage for highly critical or regulated data; prevents ransomware attacks. |

**4. Recovery Procedure**

A step-by-step plan to contain damage and restore operations.

**Standard Recovery Workflow:**

1. **Immediate System Isolation**
   * Disconnect affected systems to prevent further data corruption or malware spread.
2. **Comprehensive Damage Assessment**
   * Security and IT teams identify root cause and scope of damage.
3. **Restore from Clean Backup**
   * Use the most recent verified backup (based on RPO) from cloud, tape, or replication.
4. **Data Integrity Verification**
   * Validate data accuracy and completeness using checksum/hash comparison or application-level validation.
5. **Gradual System Restoration**
   * Restore services in prioritized order (e.g., databases → applications → front-end systems).
6. **Post-Incident Analysis**
   * Conduct RCA (Root Cause Analysis), document lessons learned, and update policies/procedures.