**Backup and Recovery Strategy**

**1. Objective**

This document defines the backup and disaster recovery (DR) mechanisms designed to ensure business continuity, data availability, and rapid recovery in the event of system failure, cyber incidents, or data corruption.

**2. Backup Strategy**

A multi-tiered backup architecture is deployed to ensure both short-term and long-term data recovery capabilities across all critical systems.

**2.1. Backup Types and Frequency**

| **Backup Type** | **Description** | **Frequency** |
| --- | --- | --- |
| **Full Backup** | Complete backup of all data and systems | Weekly |
| **Differential Backup** | Changes since the last full backup | Daily |
| **Transaction Log Backup** | Captures database transaction logs | Every 4 hours |
| **Real-Time Replication** | Continuous replication to a secondary data center | Near real-time |

This hybrid approach balances redundancy, recovery speed, and storage efficiency.

**3. Recovery Objectives**

Defined to minimize business disruption and data loss:

* **Recovery Time Objective (RTO):**  
  Maximum allowable downtime after an incident — **2 hours**
* **Recovery Point Objective (RPO):**  
  Maximum acceptable data loss measured in time — **15 minutes**

**4. Backup Storage Locations**

A resilient, geo-distributed backup storage framework is utilized to ensure high availability and fault tolerance.

* **Primary Data Center:**  
  On-premises backup infrastructure for rapid recovery in local incidents.
* **Geographically Dispersed Secondary Data Center:**  
  Acts as a failover site for disaster recovery, with near real-time data replication.
* **Cloud Backup:**  
  Encrypted cloud backups using **military-grade AES-256 encryption** for offsite redundancy and scalability.
* **Offline Tape Backups:**  
  Air-gapped, WORM (Write Once, Read Many) tape archives for critical, long-term retention and ransomware resistance.

**5. Recovery Procedure**

A standardized recovery protocol ensures structured, secure, and auditable restoration of systems.

1. **Immediate System Isolation:**  
   Disconnect affected systems from the network to prevent spread of damage or malware.
2. **Comprehensive Damage Assessment:**  
   Identify affected components, scope of data loss/corruption, and root cause.
3. **Backup Restoration:**  
   Restore systems from the **most recent verified clean backup** based on RPO/RTO targets.
4. **Data Integrity Verification:**  
   Perform checksum comparisons and validation tests to ensure restored data accuracy and completeness.
5. **Gradual System Restoration:**  
   Bring systems online in a phased manner, prioritizing critical services and verifying dependencies.
6. **Post-Incident Analysis:**  
   Conduct forensic investigation, update the incident register, and implement corrective actions to prevent recurrence.

**6. Additional Safeguards**

* **Automated Backup Monitoring:**  
  Real-time alerts and daily health reports on backup status and failures.
* **Version Control:**  
  Maintain multiple versions of critical datasets to mitigate accidental or malicious data changes.
* **Immutable Backups:**  
  Protect against ransomware by enabling immutability for selected backup snapshots.
* **Periodic DR Drills:**  
  Conduct semi-annual disaster recovery simulations to test and refine the recovery plan.