**Backup and Recovery Strategy Document**

1. **Backup Strategy :**

To protect against data loss, we implement multiple backup types with different frequencies, each serving a specific purpose to minimize data downtime and loss.

**1.1 Backup Types**

* Full Backup:
  + **Frequency:** Weekly
  + **Description**: A complete backup of all data, configurations, and system states. This serves as the baseline for other backup types and is critical for full system recovery.
* Differential Backup:
  + **Frequency**: Daily
  + **Description**: A backup of all data that has changed since the last full backup. This provides an efficient way to capture changes without taking up the space or time of a full backup.
* Transaction Log Backup:
  + **Frequency**: Every 4 hours
  + **Description**: A backup of transaction logs that captures all changes made to the database during that period. This ensures that, in the event of a failure, no more than 4 hours of data are lost.

1. **Recovery Objectives :**

The recovery objectives define the acceptable limits for system downtime and data loss, ensuring that the organization can meet its business continuity needs in case of a disaster.

* 1. **Recovery Time Objective (RTO)**
  + **Goal**: 2 hours
  + **Description**: The RTO is the maximum amount of time the system can be down after a failure before it affects business operations. The goal is to restore services within 2 hours of an incident.

2.2 **Recovery Point Objective (RPO)**

* + **Goal**: 15 minutes
  + **Description**: The RPO is the maximum acceptable amount of data loss measured in time. The goal is to ensure that no more than 15 minutes of data is lost during a failure or incident.

1. **Backup Locations :**

To enhance redundancy and ensure data protection, backups are stored in multiple locations.

* 1. **Primary Data Center**

**Description**: The main data center is responsible for the primary storage and backup of data. Regular backups are taken from here to ensure that a local copy of all critical data exists for quick recovery.

* 1. **Geographically Dispersed Secondary Data Center**

**Description**: A secondary data center located in a different geographical location ensures that data is protected from localized disasters (e.g., natural disasters, power outages). This center receives replicated data for disaster recovery scenarios.

* 1. **Cloud Backup with Military-Grade Encryption**

**Description**: Backups are also stored in the cloud with military-grade encryption to provide an additional layer of protection against data loss and ensure easy access to backups in the event of a failure. Cloud storage offers scalability and off-site security.

1. **Recovery Procedure :**

The recovery procedure is a systematic approach to restoring systems and data after a failure or incident. The process is designed to minimize downtime and data loss while ensuring business continuity.

**4.1 Immediate System Isolation**

* **Action**: In the event of a disaster or data breach, the first step is to isolate the affected systems from the network to prevent further damage or data loss. This includes disconnecting servers, databases, and other affected systems from external and internal networks.

**4.2 Comprehensive Damage Assessment**

* **Action**: Once the system is isolated, a detailed assessment will be performed to determine the extent of the damage. This involves identifying lost or corrupted data, compromised systems, and the root cause of the incident.

**4.3 Backup Restoration from the Most Recent Clean Point**

* **Action**: The most recent clean backup (based on the RPO) will be used to restore systems to their last known good state. This may involve restoring full backups, differential backups, or transaction log backups, depending on the recovery requirements.

**4.4 Gradual System Restoration**

* **Action**: Once data integrity is confirmed, the affected systems will be gradually restored. This involves bringing back essential services first, followed by non-essential services, to minimize downtime and impact on business operations.

**4.5 Post-Incident Analysis**

* **Action**: After the system is fully restored and operational, a post-incident analysis will be conducted. This includes reviewing the cause of the failure, evaluating the effectiveness of the backup and recovery process, and identifying areas for improvement. A report will be generated to ensure that lessons learned are incorporated into future disaster recovery planning.

1. **Additional Backup and Recovery Considerations :**

**5.1 Regular Backup Testing**

* Regular testing of backup procedures will be conducted to ensure that all backup data can be successfully restored. This includes testing backup integrity, verifying recovery times, and assessing the overall effectiveness of the backup strategy.

**5.2 Automated Monitoring**

* Backup jobs and systems will be monitored automatically to ensure that backups are completed successfully. Alerts will be generated for any failures or irregularities, allowing IT teams to address issues proactively.

**5.3 Backup Encryption**

* All backups, whether stored in the primary data center, secondary data center, or the cloud, will be encrypted using strong encryption algorithms to protect data from unauthorized access.

**5.4 Data Retention Policy**

* A data retention policy will be implemented to ensure that only the necessary backups are kept, and old backups are securely deleted. This helps manage storage resources and ensures compliance with legal and regulatory requirements.

**Conclusion :**

* + - * The backup and recovery strategy outlined in this document ensures that the organization is well-prepared to handle data loss, system failures, and disasters.
* By implementing a robust and multi-layered backup approach, including diverse backup types, strategic backup locations, and comprehensive recovery procedures, the organization can ensure business continuity and protect against critical data loss.