Backup & Recovery Procedures: The PureIoT Data Protection Guide

Introduction

Data is your most valuable asset. A robust backup and recovery procedure is the only insurance against data loss from hardware failure, human error, or cyberattack. This guide outlines the essential steps for scheduling, testing, and maintaining reliable server backups.

1. The 3-2-1 Backup Strategy

The industry-standard **3-2-1 rule** is the foundation of any reliable backup strategy:

- **3 Copies of Data:** Maintain at least three copies of your data (the primary data and two backups).
- **2 Different Media Types:** Store the copies on two different types of storage media (e.g., internal disk and cloud storage).
- **1 Copy Offsite:** Keep at least one copy of the backup data in a secure, geographically separate location.

2. Defining Backup Types and Schedules

The type and frequency of your backups depend on your Recovery Point Objective (RPO).

Backup Type	Description	RPO Impact	Best Use Case
Full Backup	Copies all selected data. Slowest to perform, fastest to restore.	Lowest RPO	Initial backup, monthly archive.
Differential Backup	Copies all data that has changed since the *last full backup*. Faster than full, slower than incremental.	Medium RPO	Weekly backup.

Backup Type	Description	RPO Impact	Best Use Case
Incremental Backup	Copies all data that has changed since the *last backup* (full or incremental). Fastest to perform, slowest to restore.	Highest RPO	Daily or hourly backups.
Image-Level Backup	Captures the entire server, including OS, applications, and data.	Lowest RPO	Disaster Recovery (bare-metal restore).

3. The Recovery Procedure: Testing is Key

A backup is worthless if it cannot be restored. **Testing is the most neglected step in backup procedures.**

- **Regular Restore Drills:** Schedule and perform full restore drills at least **quarterly**. This involves restoring a server image to a test environment to verify data integrity and recovery time.
- **Verification:** After every backup job, the backup software must perform a verification check to ensure the data is readable and not corrupted.
- **Documentation:** Maintain clear, step-by-step documentation of the recovery procedure, including contact information for the DR team and location of offsite media.

4. Backup Security and Maintenance

Backups are a prime target for ransomware and must be secured.

- **Immutability:** Use storage that supports **immutable backups**, meaning the data cannot be deleted or modified for a set period, even by an administrator. This protects against ransomware.
- **Air-Gapping:** Ensure at least one copy of your backup is **air-gapped** (physically or logically isolated) from the production network.
- **Monitoring:** Monitor backup jobs daily. Failure alerts must be treated as a critical security incident.

Backup & Recovery Checklist

Item	Status	Notes
3-2-1 Rule Implemented	[ ]	
Quarterly Restore Drills Performed	[ ]	
Backup Data is Immutable/Air-Gapped	[ ]	
Backup Jobs Monitored Daily	[ ]	
Recovery Documentation is Current	[ ]	

Conclusion

A proactive, tested backup and recovery plan is the cornerstone of business continuity. PureIoT provides fully managed backup solutions that meet the 3-2-1 standard and include regular, verified restore testing.