

Backup & Recovery Policy

A framework for the protection, preservation, and restoration of critical Odyssey Logistics data and systems to support business continuity.

PROCEDURE POL010

CRITICAL DATA & SYSTEMS

UPDATED 7/31/2025

PROGRAM OVERVIEW

Odyssey Logistics maintains a documented backup and recovery program to safeguard critical data and systems. The program covers inventory and risk assessment, tiered backup and recovery procedures, secure retention and destruction, and recurring testing to confirm data can be restored when needed.

01

Inventory & Assess
IT assets are inventoried and evaluated through recurring risk assessment and business impact analysis.

02

Back Up & Protect
Critical data is backed up on tiered schedules with access control, encryption, and immutable copies.

03

Test & Verify
Backup integrity and recovery are verified through recurring testing against required timeframes.

04

Report & Improve
Backup activity is monitored and reported, and results drive documentation and procedure updates.

FRAMEWORK ALIGNMENT

NIST CSF
Recover & Protect functions — data security and resilience.

CIS Critical Security Controls
Control 11 — Data Recovery.

ISO/IEC 27001 Annex A
Backup and business continuity safeguards.

WHAT THIS POLICY COVERS

The policy is structured across the sections below. Each is mapped to the corresponding area of recognized security practice — demonstrating coverage without disclosing internal control specifics.

§1.1
1.2

Purpose & Scope
Protection, preservation, and restoration of critical data and systems.

§1.4

Inventory & Assessment
Asset inventory, recurring risk assessment, and business impact analysis.

§1.6
1.7

Log Retention & Destruction
Protected activity logs and certified secure data destruction.

§1.10
1.11

Security & Documentation
Encryption, access controls, and maintained procedure documentation.

§1.3

Policy
Access control, immutable backups, encryption, and regular audits.
CIS Control 11

§1.5

Backup & Recovery Procedures
Tiered backup schedules across primary and replicated sites.
NIST CSF - Recover

§1.8
1.9

Reporting & Testing
Monitoring, failure alerting, and recurring recovery testing.

§1.12

Communication & Roles
Defined roles, communication plan, and contact information.

Supporting document control: maintained revision history and referenced inventory, risk, impact, and communication artifacts.