ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Vulnerability & Patch Management Program

A risk-based approach to identifying, prioritizing, and remediating vulnerabilities across Odyssey Logistics' technology environment — reviewed and continuously improved as part of our security governance program.

POLICY POL003 | ENTERPRISE-WIDE SCOPE | ANNUALLY REVIEWED

PROGRAM OVERVIEW

Odyssey Logistics maintains a formal, documented program governing how vulnerabilities and required patches are identified, evaluated, and remediated across company systems, services, and network infrastructure. The program is risk-based — remediation is prioritized by severity and potential business impact — and is subject to ongoing oversight by Security and Technology leadership.

01 Identify & Assess

Systems and vendor sources are continuously monitored to identify available patches and emerging vulnerabilities.

02 Risk-Based Prioritization

Findings are prioritized using industry-standard severity scoring, weighed against data sensitivity and service criticality.

03 Controlled Remediation

Patches are tested and deployed on a defined, recurring cadence, with formal, time-bound exception handling where needed.

04 Verify & Govern

Completion is logged, reviewed by the Security team, and reassessed regularly to confirm the program is operating as designed.

FRAMEWORK ALIGNMENT

NIST CSF
Identify & Protect functions — asset and vulnerability management practices.

CIS Critical Security Controls
Control 7 — Continuous Vulnerability Management.

ISO/IEC 27001 Annex A
Technical vulnerability management & change control 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
Program intent and enterprise-wide applicability across systems, services, and infrastructure.

§1.3 Policy Statement
Custodian responsibilities and the governance basis for keeping systems current. NIST CSF · Govern

§1.4.1 Identification & Testing
Vendor monitoring and controlled validation of available patches.
CIS Control 7

§1.4.2 Evaluation & Deployment
Risk-based, time-bound remediation on a consistent cadence.
NIST CSF · Protect

§1.4.3 Documented Procedures
Repeatable, auditable operating process aligned to change control.

§1.4.4 Exception Handling
Formal risk-acceptance with defined review and re-evaluation.
ISO/IEC 27001

§1.4.5 Controls & Management
Logging, monitoring, and independent verification for audit evidence.
CIS Control 7

§1.4.6 Enforcement
Accountability and compliance obligations for responsible teams.

Supporting document control: maintained revision history and referenced Change Advisory Board procedures.