ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Third-Party Risk Management Program

A structured approach to assessing, managing, and monitoring cybersecurity risk across vendors, contractors, cloud providers, and partners throughout the full engagement lifecycle.

POLICY POL017 | ENTERPRISE-WIDE SCOPE | ANNUALLY REVIEWED

PROGRAM OVERVIEW

Odyssey Logistics maintains a formal, documented program governing how third-party cybersecurity risk is evaluated and managed, from initial vendor selection through offboarding. The program is coordinated across Procurement, Legal, Technology, and Cybersecurity, and is subject to ongoing oversight by Security leadership.

01 Classify & Assess

Third parties are risk-tiered by data sensitivity and system criticality, with due diligence assessments required before engagement.

02 Contractual Safeguards

Agreements incorporate confidentiality, audit rights, breach notification, and data protection obligations.

03 Continuous Oversight

High-risk vendors are monitored on an ongoing basis, with periodic reassessment based on risk tier.

04 Offboarding & Closure

Data return or destruction, access revocation, and closure documentation are required at termination.

FRAMEWORK ALIGNMENT

NIST CSF
Identify & Protect functions — third-party and supply chain risk management.

ISO/IEC 27001 Annex A
Supplier relationship and information security safeguards.

CIS Controls v8 / SOC 2
Third-party security control alignment and audit guidance.

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 applicability across the vendor lifecycle and cross-functional teams.

§2.1 Risk Classification & Due Diligence
Tiered risk classification and pre-engagement cybersecurity assessment requirements. NIST CSF

§2.2 Roles & Responsibilities
Accountabilities across Procurement, Legal, Technology, and Cybersecurity.

§2.3-2.4 Contractual & NDA Requirements
Mandatory security, audit, and confidentiality clauses in vendor agreements. ISO/IEC 27001

§2.5 Monitoring & Oversight
Continuous monitoring and periodic reassessment of high- and medium-risk vendors. SOC 2

§2.6-2.7 Incident Response & Offboarding
Breach notification obligations and termination data-handling requirements.

§3-4 Risk Register & Exceptions
Centralized risk documentation, scoring, and CISO-approved exception handling. CIS Controls

§5-6 References & Review
Standards alignment and annual policy review cadence.

Supporting document control: maintained revision history and referenced Data Classification and Information Security policies.