ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Secure Tunnel & Certificate Management

Requirements for the secure creation, management, and operation of network tunnels across Odyssey Logistics' infrastructure, protecting data in transit through strong cryptography and automated lifecycle controls.

POLICY POL019 | ENTERPRISE-WIDE SCOPE | ANNUALLY REVIEWED

PROGRAM OVERVIEW

All network tunnels connecting Odyssey Logistics infrastructure — internally, externally, or across hybrid cloud environments — must be established using certificate-based authentication, automated key rotation, and secure certificate management practices overseen by Cybersecurity and Network Operations.

01 Certificate-Based Authentication

Tunnels are authenticated using industry-standard cryptographic algorithms.

02 Automated Lifecycle Management

Tunnel creation, certificate deployment, and key rotation are automated to reduce error.

03 Secure Key Storage

Cryptographic keys are stored using approved hardware security modules with logged, role-based access.

04 Trusted CA Governance

A hardened, regularly audited Certificate Authority issues and manages all tunnel certificates.

FRAMEWORK ALIGNMENT

NIST SP 800-57
Cryptographic key management recommendations.

NIST SP 800-77
Guide to IPsec VPN implementation and security.

ISO/IEC 27001
Cryptographic controls and information security management.

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
Tunnel security requirements across infrastructure, cloud, and third-party connections.

§1.3.1 Certificate-Based Authentication
Approved cryptographic standards required for tunnel authentication. NIST SP 800-57

§1.3.2 Automated Tunnel & Key Management
Automation requirements for tunnel creation and key rotation.

§1.3.3 Secure Key Management
Storage, encryption, and access-control requirements for cryptographic keys. NIST SP 800-77

§1.3.4 Trusted CA Management
Certificate authority hardening, auditing, and issuance standards.

§1.4 Roles & Responsibilities
Accountabilities across CISO, Network Operations, and Cybersecurity teams. ISO/IEC 27001

§1.5 Compliance & Enforcement
Quarterly compliance audits and handling of non-compliant tunnels.

§1.6-1.8 References & Review Cycle
Standards alignment and annual policy review requirements.

Supporting document control: maintained revision history and referenced Internal Data Classification Policy.

Sensitive & Restricted for Distribution — Business Confidential. Not for release outside Odyssey Logistics without written authorization.