ODYSSEY LOGISTICS

ASSURANCE & TRUST PROGRAM

Consolidated Policy Compendium

The complete set of Odyssey Logistics information-security and IT governance policies, organized against the NIST Cybersecurity Framework 2.0 and cross-referenced to ISO/IEC 27001 and the CIS Controls.

24 POLICIES & PROCEDURES | NIST CSF 2.0 ALIGNED | COMPILED JULY 7, 2026

24 DOCUMENTS

6 CSF 2.0 FUNCTIONS

3 REFERENCE FRAMEWORKS

NIST CSF 2.0

Govern · Identify · Protect · Detect · Respond · Recover — the organizing spine.

ISO/IEC 27001

Information security management system controls and Annex A safeguards.

CIS Controls

Prioritized safeguards mapped to individual control numbers.

Domain Standards

NIST SP 800-series, AI RMF / ISO 42001, ITIL, SOC 2, GDPR/CCPA.

SENSITIVE & RESTRICTED — BUSINESS CONFIDENTIAL

Not for release outside Odyssey Logistics without written authorization. This compendium aggregates assurance-overview one-pagers that demonstrate control coverage without disclosing internal control specifics.

Contents

Policies are ordered by their primary NIST CSF 2.0 function. The page number for each one-pager appears at right and corresponds to its position later in this compendium.

Policy Map to Risk Domains

Every policy is anchored to one of the six NIST Cybersecurity Framework 2.0 functions — the recognized risk-domain model auditors, insurers, and customers use to judge program completeness. Each card lists the policies whose *primary* purpose sits in that function.

5 GOVERN

Establish and monitor the security program, risk decisions, roles, and oversight.

Cybersecurity Policy	POL005
Cybersecurity Program Review	POL011
Risk Management Program	POL020
Cybersecurity Exceptions Policy	POL010-A
Generative AI Policy	POL007

4 IDENTIFY

Understand assets, data, and third-party exposure so risk can be prioritized.

Data Classification Policy	POL006
Asset Management & Purchasing	PRO001
Device Lifecycle Management	PRO
Third-Party Risk Management	POL017

11 PROTECT

Safeguard identities, endpoints, data, and change through preventive controls.

Access Management & Password	POL001
Least Privilege Policy	POL018
Remote Access Software Policy	POL009
Personal Device Use Policy	POL004
Secure Tunnel & Certificate Mgmt	POL019
Onboarding Policy	POL022
Offboarding Policy	POL021
Change Management Policy	POL008
Vulnerability & Patch Management	POL003
Data Retention & Destruction	POL012
Cyber Security Data Access Policy	POL009-A

2 RESPOND

Coordinate, contain, and communicate during active incidents.

Incident Response Plan & Guidelines	PRO003
System Outage Work Process	PRO005

2 RECOVER

Restore data, systems, and operations to resume business.

Backup & Recovery Policy	POL010
Disaster Recovery Program	POL016

Framework Crosswalk

Each policy against the six CSF 2.0 functions and the supporting frameworks it cites. A filled marker is the function the policy chiefly serves; a hollow marker is a supporting role.

#	POLICY	GOV	IDEN	PROT	DET	RESP	REC	ISO 27001	CIS	OTHER
01	**Cybersecurity Policy** POL005 Rev.02	●	○	○				✓	Enterprise safeguards	—
02	**Cybersecurity Program Review** POL011 Rev.01	●	○					✓	—	Maturity Model
03	**Risk Management Program** POL020 Rev.02	●	○					—	—	NIST RMF · Internal Audit
04	**Cybersecurity Exceptions Policy** POL010-A Rev.01	●						✓	—	NIST RMF
05	**Generative AI Policy** POL007 Rev.03	●		○				—	—	NIST AI RMF · ISO 42001
06	**Data Classification Policy** POL006 Rev.02	○	●					✓	—	GDPR · CCPA
07	**Asset Management & Purchasing** PRO001 Rev.001		●					✓	—	ITIL
08	**Device Lifecycle Management** PRO Rev.R03		●	○				✓	CIS 1 & 2	—
09	**Third-Party Risk Management** POL017 Rev.02	○	●	○				✓	CIS v8	SOC 2
10	**Access Management & Password** POL001 Rev.04			●	○			—	CIS 5 & 6	NIST SP 800-63
11	**Least Privilege Policy** POL018 Rev.01			●				✓	CIS Controls	—
12	**Remote Access Software Policy** POL009 Rev.02			●				✓	CIS 6 & 12	—
13	**Personal Device Use Policy** POL004 Rev.02			●				✓	CIS 4	—
14	**Secure Tunnel & Certificate Mgmt** POL019 Rev.01			●				✓	—	NIST SP 800-57/77
15	**Onboarding Policy** POL022 Rev.04			●				✓	CIS Controls	—
16	**Offboarding Policy** POL021 Rev.004			●				✓	CIS Controls	—
17	**Change Management Policy** POL008 Rev.04			●				✓	—	ITIL
18	**Vulnerability & Patch Management** POL003 Rev.03		○	●	○			✓	CIS 7	—
19	**Data Retention & Destruction** POL012 Rev.03		○	●				✓	—	CPRA · CCPA
20	**Cyber Security Data Access Policy** POL009-A Rev.02	○		●				✓	—	Legal/Privacy
21	**Incident Response Plan & Guidelines** PRO003 Rev.02				○	●	○	—	—	NIST SP 800-61 · MITRE ATT&CK
22	**System Outage Work Process** PRO005 Rev.002					●		—	—	ITIL
23	**Backup & Recovery Policy** POL010 Rev.01			○			●	✓	CIS 11	—
24	**Disaster Recovery Program** POL016 Rev.02					○	●	✓	—	Industry DR Std

● **Primary function** ○ **Secondary / supporting** ✓ = ISO/IEC 27001 alignment cited

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Cybersecurity Policy

The governing framework of logical and technical controls Odyssey Logistics uses to manage risk and protect the confidentiality, integrity, and availability of its systems and information.

POLICY POL005 | ENTERPRISE-WIDE SCOPE | UPDATED 12/23/2024

PROGRAM OVERVIEW

Odyssey Logistics maintains a comprehensive enterprise cybersecurity program to safeguard company and customer data. The policy defines governance roles, program goals, and the standards that direct protection of systems and information assets, with oversight from executive and security committees.

01 Govern
Executive and security committees set direction, approve policy, and assign clear roles across the enterprise.

02 Protect
Standards for endpoints, encryption, authentication, and acceptable use safeguard systems and information assets.

03 Manage Risk
The program maintains awareness of threats and manages vulnerabilities to determine risk and business impact.

04 Assure
Compliance is audited and reported to preserve the confidentiality, integrity, and availability of company data.

FRAMEWORK ALIGNMENT

- **NIST CSF** — Govern, Identify & Protect functions — enterprise security program structure.
- **ISO/IEC 27001** — Security management system — controls and governance.
- **CIS Critical Security Controls** — Enterprise safeguards spanning the defined standards domains.

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 Overview & Purpose** — Commitment to protecting information and systems through logical and technical controls.
- **§1.3 Scope** — Applies to all users of systems or data owned or controlled by the company.
- **§1.4 Roles & Authorities** — Governance committees, CISO, and data owner / custodian responsibilities. NIST CSF · Govern
- **§1.5 Goals & Objectives** — Preserving confidentiality, integrity, and availability of company data.
- **§1.6 Standards** — Control domains associated with the security policy, set following systems audit.
- **§1.6.1-1.6.3 Device, Endpoint & Encryption** — BYOD posture, endpoint configuration, and encryption expectations.
- **§1.6.4-1.6.5 Vulnerability & Authentication** — Patching / vulnerability management and authentication requirements. CIS Control 7
- **§1.6.6-1.6.8 Classification, Use & Storage** — Required classification types, acceptable use, and data-storage limitations. ISO/IEC 27001

Supporting note: a separately classified document holds technical implementation and incident-response specifics.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Cybersecurity Program Review

A structured annual review of Odyssey Logistics' cybersecurity program to verify governance, measure maturity, and demonstrate control effectiveness to leadership and stakeholders.

POLICY POL011 | GLOBAL CYBER PROGRAM | UPDATED 8/28/2025

PROGRAM OVERVIEW

Odyssey Logistics conducts a structured annual review of its cybersecurity program. The review assesses governance alignment, audits control effectiveness, measures program maturity against established frameworks, and reports findings and recommended actions to executive leadership and the board.

01 Assess Governance
The review verifies policies, roles, and decision-making structures against governance and strategic goals.

02 Audit Controls
Technical, administrative, and physical controls are tested and validated for effectiveness.

03 Measure Maturity
Program maturity is scored against an established model, and risk posture is evaluated with audit evidence.

04 Report & Improve
Findings, maturity scores, and gaps are reported to leadership and drive the following year's improvements.

FRAMEWORK ALIGNMENT

NIST CSF
Govern function — program alignment and maturity tiers.

ISO/IEC 27001
Management review and internal audit of the security program.

Maturity Model
Defined scoring to assess program progression year over year.

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
Annual review across global cybersecurity functions, processes, and controls.

§2.1 Annual Review Objectives
Governance alignment, maturity measurement, and gap identification.
NIST CSF · Govern

§2.2 Review Components
Governance, control audit, maturity, risk, compliance, and evidence.

§2.3 Roles & Responsibilities
CISO oversight, team participation, and independent validation.

§3 Reporting & Follow-Up
Board reporting with tracked, prioritized action items. ISO/IEC 27001

§3.1 Continuous Improvement
Outcomes inform planning, resourcing, and risk decisions.

Supporting document control: maintained revision history and a referenced documents register.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Risk Management Program

A structured, practical approach to enterprise risk management — identifying, assessing, mitigating, and monitoring risk in alignment with organizational objectives and governance expectations.

POLICY POL020 | ENTERPRISE-WIDE SCOPE | ANNUALLY REVIEWED

PROGRAM OVERVIEW

Odyssey Logistics' risk management program provides a consistent, repeatable framework for identifying and prioritizing risk across cybersecurity, IT operations, logistics, and third-party relationships. The program emphasizes clear ownership, standardized scoring, and continuous improvement through audit feedback.

01 Risk Identification
Risks are documented consistently across the enterprise with description, impact, likelihood, and root cause.

02 Assessment & Scoring
A standardized scoring model evaluates likelihood and impact to produce a quantified risk score.

03 Mitigation & Treatment
Risk owners select avoidance, reduction, transfer, or acceptance strategies with tracked milestones.

04 Governance & Reporting
Key risks are reported quarterly to leadership, with annual program audits and reviews.

FRAMEWORK ALIGNMENT

NIST RMF
Structured lifecycle for categorizing and managing organizational risk.

NIST CSF
Enterprise-wide risk identification and prioritization alignment.

Internal Audit Standards
Independent verification of risk register accuracy and control effectiveness.

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
Enterprise risk strategy applicability across functions, geographies, and third parties.

§2.1 Risk Management Strategy
Guiding principles: simplicity, incident-centric prioritization, and accountability. NIST RMF

§2.2 Risk Identification & Documentation
Required risk entry fields and centralized risk register maintenance.

§2.3 Risk Assessment & Scoring
Standardized likelihood-and-impact scoring methodology. NIST CSF

§2.4 Risk Register
Structured tracking fields for ownership, treatment decisions, and follow-up dates.

§2.5 Risk Mitigation & Treatment
Defined treatment strategies with milestones and responsible parties.

§3 Auditing, Review & Monitoring
Annual program review and independent audit function.

§4-6 Roles, Reporting & Improvement
Ownership model and quarterly executive reporting cadence.

Document number reassigned from POL016 to POL020 to resolve a numbering conflict with the Disaster Recovery policy.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Cybersecurity Exceptions Policy

The organized process by which requests for exception to Odyssey Logistics security policy are entered, reviewed, approved or denied, and followed up.

POLICY POL010-A | POLICY EXCEPTIONS | UPDATED 6/13/2024

PROGRAM OVERVIEW

Odyssey Logistics governs security-policy exceptions through a documented, case-by-case process. Requests are intake-tracked, paired with compensating controls, approved by cybersecurity management for a defined period, and followed up for closure or re-evaluation.

01 Request
Exceptions to security policy are requested through a defined intake process on a case-by-case basis.

02 Mitigate
The security team and requester agree on compensating controls to reduce the risk of any granted exception.

03 Approve
Exceptions are approved by cybersecurity management for a defined, time-bound period or otherwise rejected.

04 Track & Review
Approved exceptions are tracked in a central register and followed up for closure or re-evaluation.

FRAMEWORK ALIGNMENT

- **NIST CSF** — Govern function — risk acceptance and exception governance.
- **ISO/IEC 27001** — Risk treatment and documented exception handling.
- **NIST RMF** — Risk-based decision-making with compensating controls.

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 Purpose
Organized handling of requests for exception to standard security policy.

§1.2 Scope
Case-by-case, time-bound approvals with defined follow-up.

§1.3 Compensating Controls
Dialogue to identify mitigations for the risk of a granted exception.
NIST CSF · Govern

§1.4 Intake Process
Ticketed request with information gathering by the security team.

§1.5 Approval Process
Review and approval by cybersecurity management, or rejection.
ISO/IEC 27001

§1.6 Reporting
Central tracking of exception requests to support reporting.

§1.7 Policy Review
Changes communicated to affected individuals.

Supporting document control: maintained revision history and referenced exceptions template and tracking register.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Generative AI Policy

Guidelines for the ethical, secure, and responsible use of generative AI tools by Odyssey Logistics employees, contractors, and third parties.

POLICY POL007 | ALL AI TOOL USE | UPDATED 8/12/2025

PROGRAM OVERVIEW

Odyssey Logistics maintains a documented policy for the appropriate use of generative AI. Use is limited to enterprise-approved tools, aligned to the company's data classification standards, and governed by requirements for data protection, ethical use, and human oversight.

01 — Approve Tools
Only enterprise-sanctioned generative AI tools may be used for company business; other tools require leadership approval.

02 — Protect Data
Confidential information, proprietary data, and PII are kept out of generative AI tools unless explicitly approved.

03 — Use Ethically
Outputs are reviewed for accuracy, fairness, and appropriateness, avoiding harmful or biased content.

04 — Oversee & Improve
Human oversight governs critical decisions, and training and review keep practices current as the field evolves.

FRAMEWORK ALIGNMENT

- **NIST AI RMF** — Trustworthy AI — governance, data protection, and human oversight.
- **ISO/IEC 42001** — AI management system — responsible use and continuous improvement.
- **NIST CSF** — Protect function — safeguarding data used with AI tools.

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.

- **§1.1–1.3 Statement, Purpose & Scope** — Responsible-use commitment for employees, contractors, and third parties.
- **§2.1 General Use Requirements** — Approved enterprise toolsets only, aligned to data classification standards. NIST AI RMF
- **§2.2–2.3 Communication & Customer Interaction** — Productivity use for non-sensitive tasks; oversight for sensitive interactions.
- **§2.4 Data Security & Privacy** — Confidential data and PII withheld from tools unless previously approved. NIST CSF · Protect
- **§2.5 Ethical Use** — Fair, professional, and appropriate output free of bias.
- **§2.6 Human Oversight** — Human judgment required for critical decisions and finalized communications.
- **§2.8–2.9 Training & Compliance** — Employee training and defined consequences for non-adherence.
- **§2.10–2.11 Improvement & Contact** — Periodic policy review and a defined point of contact. ISO/IEC 42001

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

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Data Classification Policy

A framework for classifying Odyssey Logistics data by sensitivity, value, and criticality so that appropriate safeguards are applied to each information asset.

POLICY POL006 | ALL COMPANY DATA | UPDATED 12/23/2024

PROGRAM OVERVIEW

Odyssey Logistics classifies all company data by sensitivity and business impact, assigning each asset a classification that determines the required safeguards. The policy defines classification tiers, predefined categories of Confidential data, and the roles responsible for assigning and periodically reassessing labels.

01 Classify
All company data is assigned one of three sensitivity classifications in decreasing order of importance.

02 Define Confidential
Certain data types — authentication verifiers, payment card data, and PII — are predefined as Confidential.

03 Align to Regulation
Data governed by regulations such as GDPR and CCPA is treated as Confidential by default.

04 Review & Reassign
Data owners periodically re-evaluate classifications and align safeguards as sensitivity or obligations change.

FRAMEWORK ALIGNMENT

- **NIST CSF** — Identify function — data and asset management by sensitivity.
- **ISO/IEC 27001 Annex A** — Classification and handling of information.
- **GDPR & CCPA** — Regulatory definitions of personal data mapped to Confidential.

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
Framework to classify data by sensitivity across staff, agents, and affiliates.

§1.3 Goals
Classification supports confidentiality, integrity, and availability of data.

§1.4 Roles & Authorities
Data owners classify assets; Technology & Security Operations governs the policy. NIST CSF · Govern

§1.5 Data Classification
Confidential, Sensitive, and Public tiers with default-Sensitive handling. ISO/IEC 27001

§1.6 Predefined Confidential Data
Authentication verifiers, payment card information, and PII.

§1.7 GDPR
EU personal data treated as Confidential. Regulatory

§1.8 CCPA
California personal information treated as Confidential. Regulatory

§1.9 1.10 Assigning & Reassigning Labels
Most-restrictive labeling and periodic re-evaluation of classifications.

Supporting document control: maintained revision history and referenced Cybersecurity Policy.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Asset Management & Purchasing Process

Governance over how IT equipment is purchased and managed across Odyssey Logistics, standardizing vendor relationships, configurations, and financial oversight.

PROCESS PR0001 | ENTERPRISE-WIDE SCOPE | REVIEWED AS NEEDED

PROGRAM OVERVIEW

Odyssey Logistics consolidates IT purchasing through a defined set of preferred vendors, standardized equipment packages, and documented supplier management practices, retaining accountability for service delivery regardless of which vendor is involved.

01 Vendor Governance
Accountability for service delivery is retained internally, with documented supplier requirements.

02 Standard Equipment Packages
Defined in-office and at-home equipment sets apply based on work arrangement.

03 Preferred Vendor Selection
Purchasing is consolidated through a short list of approved manufacturers.

04 Budget Oversight
Costs are budgeted in detail and monitored against forecast for financial control.

FRAMEWORK ALIGNMENT

ITIL Supplier Management
Structured evaluation, contracting, and performance monitoring of vendors.

ISO/IEC 27001
Asset management and supplier relationship safeguards.

Internal Financial Controls
Budget forecasting and cost-versus-actual monitoring practices.

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 Purpose
Governance objectives for IT equipment purchasing and asset lifecycle.

§1.2 Scope
Vendor management goals, including cost efficiency and strategic alignment. ITIL

§1.3 Roles & Authorities
Vendor and supplier role definitions and accountabilities.

§1.4 Supplier Management
Contract requirements, performance monitoring, and dispute handling. ISO/IEC 27001

§1.4.2 Standard Equipment Packages
Defined in-office and remote equipment sets by employment arrangement.

§1.4.3 Computer Selection Process
Approved vendor list and standard configuration options.

§1.5 Budgeting & Accounting
Cost forecasting, budget control, and financial reporting practices.

Supporting document control: maintained revision history and referenced PC Life Cycle Procedure and Material Equipment Listing Matrix.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Device Lifecycle Management

Best practices for managing the lifecycle of Odyssey Logistics end-user IT equipment — from procurement and maintenance through secure disposal.

PROCEDURE | END-USER IT EQUIPMENT | UPDATED 1/20/2026

PROGRAM OVERVIEW

Odyssey Logistics manages the lifecycle of end-user IT equipment to reduce downtime, prevent security failures from outdated systems, and improve planning and productivity. The procedure defines maintenance, upgrade, replacement, and secure disposal practices across the equipment lifecycle.

01 Plan & Inventory
Existing IT assets are reported and budgeted to meet current and future business requirements.

02 Maintain
Equipment is monitored and maintained through established device-management systems.

03 Upgrade & Replace
Hardware is reviewed on a set cadence and refreshed on a defined depreciation schedule.

04 Dispose Securely
End-of-life equipment is recycled, donated, or retained only after verified secure data destruction.

FRAMEWORK ALIGNMENT

NIST CSF
Identify function — asset management across the lifecycle.

CIS Critical Security Controls
Controls 1 & 2 — inventory of enterprise assets and software.

ISO/IEC 27001 Annex A
Asset lifecycle and secure disposal of equipment.

WHAT THIS POLICY COVERS

The procedure 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
Lifecycle management of end-user IT equipment and its objectives.

§1.3 Roles & Authorities
End users who operate company equipment.

§1.4 Schedule
Asset reporting and budgeting to meet business requirements.
CIS Control 1

§1.4.1 1.4.2 Maintenance & Upgrades
MDM-managed maintenance and cadence-based hardware review.

§1.4.3 Replacement
Depreciation-based refresh cadence for desktops and laptops.

§1.4.4 Disposal
Certified recycling and standards-based data destruction at end of life.
NIST CSF · Protect

Supporting document control: maintained revision history and referenced asset-management, equipment-listing, and retention documents.

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.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Access Management & Password Policy

A defined, formally managed approach to how user credentials are constructed, protected, and assured across Odyssey Logistics information systems and third-party-hosted services.

POLICY POL001 | ALL CREDENTIALED USERS | UPDATED 5/30/2025

PROGRAM OVERVIEW

Odyssey Logistics maintains a documented access management and password policy governing how login credentials are provisioned, constructed, used, and protected across company information systems. The policy applies risk-based requirements scaled to account privilege and is subject to ongoing oversight by Security and Technology leadership.

01 Establish Identity
Unique credentials and formal provisioning substantiate each user's claimed identity before access is granted.

02 Enforce Strength
Password construction, complexity, and reuse controls are scaled to account privilege level and enforced by system.

03 Authenticate & Protect
Multi-factor authentication, secure login, and protected credential handling guard sessions against unauthorized access.

04 Log & Assure
Authentication events are logged and services are aligned to defined authenticator assurance levels for ongoing confidence.

FRAMEWORK ALIGNMENT

NIST CSF
Protect function — identity management, authentication, and access control.

CIS Critical Security Controls
Controls 5 & 6 — Account and Access Control Management.

NIST SP 800-63
Digital identity guidelines — authenticator assurance levels (AAL1–AAL3).

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 to all users issued credentials to company or third-party systems.

§1.3 Policy Statement
Formal, controlled management process for the allocation of password information. NIST CSF · Govern

§1.3.1 Password Protection Guidelines
Construction and reuse rules scaled to privilege level and screened against banned values. CIS Control 5

§1.3.2 Secure Login Procedures
MFA/SSO, minimal disclosure, and brute-force protections at login. NIST CSF · Protect

§1.3.3 Password Management System
Enforced complexity, history, and separated, protected credential storage.

§1.3.4 Password Use & Protection
Confidential handling, approved secure sharing, and offboarding controls.

§1.3.5 Audit Controls – Event Logging
Logging of authentication events in support of the audit function. CIS Control 8

§1.4 Authenticator Assurance Levels
Alignment of services to defined identity and authentication assurance levels. NIST SP 800-63

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

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Least Privilege Policy

Procedures governing the granting, review, and revocation of administrative privileges, ensuring access remains aligned with job responsibilities at all times.

POLICY POL018 | ENTERPRISE-WIDE SCOPE | ANNUALLY REVIEWED

PROGRAM OVERVIEW

Odyssey Logistics grants administrative privileges only when justified by job function, through a documented approval process, with access reviewed on a regular cadence and revoked promptly when no longer required.

01 Justified Access
Administrative privileges are granted only when clearly justified by job function.

02 Documented Approval
Requests move through a formal, multi-party approval and validation workflow.

03 Role-Based Blueprints
Predefined access packages align privilege levels with specific job roles.

04 Periodic Review & Revocation
Scheduled reviews and prompt revocation follow role changes or departures.

FRAMEWORK ALIGNMENT

NIST CSF
Protect function — identity management and access control.

CIS Controls
Access control management and administrative privilege governance.

ISO/IEC 27001
Access control and least-privilege 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 Introduction
Purpose, scope, and key definitions for administrative access.

§2 Policy Statement
Core principles governing how administrative access is granted and maintained. NIST CSF

§3 Roles & Responsibilities
Accountabilities across IT Security, Managers, System Owners, and HR.

§4 Granting Admin Privileges
Request, approval, and documentation workflow for new access.

§5 Revoking Admin Privileges
Trigger events and revocation timeline requirements. CIS Controls

§6 Role-Based Access Blueprints
Predefined access packages by functional role.

§7 Periodic Access Reviews
Review cadence and verification steps for existing access. ISO/IEC 27001

§8-10 Exceptions, Enforcement & Review
Exception approval, enforcement consequences, and annual policy review.

Supporting document control: maintained revision history and role-based access blueprints for key technical functions.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Remote Access Software Policy

The approved tools and secure-configuration requirements governing how Odyssey Logistics personnel connect remotely to company workstations and servers.

POLICY POL009 | ALL REMOTE ACCESS | UPDATED 12/23/2024

PROGRAM OVERVIEW

Odyssey Logistics permits remote access only through a defined set of approved tools, authorized by role. The policy sets secure-connection requirements — including multi-factor authentication and strong encryption — and defines how compliance is measured and enforced.

01 Approve Tools
Only a defined set of approved remote access tools may be used to connect to company systems.

02 Authorize by Role
Tool use is authorized by role, limiting who may connect to workstations, servers, and virtual machines.

03 Secure the Channel
Remote sessions require multi-factor authentication, mutual authentication, and strong end-to-end encryption.

04 Verify Compliance
Compliance is measured through reporting and audits, with a formal exception path and defined consequences.

FRAMEWORK ALIGNMENT

NIST CSF
Protect function — identity, authentication, and secure remote access.

CIS Critical Security Controls
Controls 6 & 12 — access control and network infrastructure management.

ISO/IEC 27001 Annex A
Remote access and secure communications 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 Overview
Approved-tools-only model to reduce remote access security risk.

§2.1 Scope
Applies to employees, contractors, and temporary staff.

§3.1 Policy
Role-based authorization of remote access tools and their use.

§3.1.1 Approved Remote Access Tools
Defined, mandatory-configuration toolset with exception handling.

§3.1.2 Remote Access Requirements
MFA/SSO, mutual authentication, and strong end-to-end encryption.
NIST CSF · Protect

§4.1 Policy Compliance
Compliance measurement, exceptions, and non-compliance consequences. CIS Control 12

Supporting document control: maintained revision history and referenced Exceptions and Exclusion form.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Personal Device Use Policy

Guidelines and minimum safeguards for the limited, as-needed use of personally owned devices to access Odyssey Logistics systems and services.

POLICY POL004 | PERSONAL DEVICES | UPDATED 12/23/2024

PROGRAM OVERVIEW

Odyssey Logistics maintains a documented policy governing employee use of personally owned devices for work-related purposes. Personal devices are permitted only on an as-needed basis, must meet minimum security and data-handling requirements, and are validated before being granted access to company resources.

01 — Qualify the Device
Personal devices are permitted only as needed and must meet minimum data-handling and security requirements.

02 — Harden & Protect
Devices are secured through screen lock, encryption, endpoint protection, and maintained operating systems.

03 — Assign Responsibility
Users accept defined responsibilities for company data, prompt loss reporting, and device upkeep.

04 — Validate Access
Every device is untrusted by default and validated before it is granted access to company systems and data.

FRAMEWORK ALIGNMENT

- **NIST CSF** — Protect function — endpoint protection and access control for non-corporate devices.
- **CIS Critical Security Controls** — Control 4 — Secure Configuration of Enterprise Assets and Software.
- **ISO/IEC 27001 Annex A** — Mobile device and teleworking 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
Intent and guidelines for using a personal device for company business.

§1.3 Acceptable Use Guidelines
Device hardening, encryption, endpoint protection, and software currency requirements. CIS Control 4

§1.4 Risks & Liabilities
User accountability for local data, loss reporting, and device maintenance.

§1.5 Compliance & Enforcement
Default-untrusted validation before access, with reserved right to expand controls. NIST CSF · Protect

Supporting document control: maintained revision history and referenced Data Classification and Access Management & Password policies.

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.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Onboarding Policy

A formalized onboarding process spanning pre-hire IT setup, equipment provisioning, and Day 1 readiness, ensuring new hires are equipped and integrated in a timely, compliant manner.

POLICY POL022 | ENTERPRISE-WIDE SCOPE | ANNUALLY REVIEWED

PROGRAM OVERVIEW

Odyssey Logistics standardizes onboarding timelines, communications, and ticketing processes across HR, IT, and hiring managers, applying the same structured workflow to full-time employees, contractors, and temporary staff.

01 — Advance Notice
Required lead time ensures equipment and accounts are ready before the start date.

02 — Standardized Provisioning
Defined ordering, imaging, and setup steps follow a consistent timeline.

03 — Access Governance
Account creation is tied directly to a formal, validated new-hire submission.

04 — Consistent Equipment Standards
Standard imaging and peripheral packages apply based on work arrangement.

FRAMEWORK ALIGNMENT

- **NIST CSF** — Protect function — identity and asset provisioning at hire.
- **CIS Controls** — Account and asset management for new user onboarding.
- **ISO/IEC 27001** — Onboarding and access provisioning 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 **Executive Summary** — Objective to ensure timely, compliant new-hire readiness.
- §1.2 **Scope** — Lifecycle coverage from pre-hire setup through Day 1 readiness.
- §1.3 **Objective** — Standardization and cross-functional collaboration goals. NIST CSF
- §1.4 **New Hire Request** — Ticket timing, required data fields, and procurement sequencing.
- §2 **IT Account Creation** — Account and application access request process tied to formal submission. CIS Controls
- §3 **Equipment Setup** — Standard imaging and peripheral provisioning by work arrangement. ISO/IEC 27001

Supporting document control: maintained revision history and referenced Device and Asset Management Process.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Offboarding Policy

A formalized offboarding process ensuring account deactivation, access revocation, and equipment retrieval are completed in a timely, consistent manner to protect organizational security.

POLICY POL021 | ENTERPRISE-WIDE SCOPE | ANNUALLY REVIEWED

PROGRAM OVERVIEW

Odyssey Logistics standardizes offboarding timelines, communications, and ticketing processes across HR, IT, and hiring managers for full-time employees, contractors, and temporary staff, ensuring terminations are handled securely and without delay.

01 Termination Notification
Defined trigger events and Help Desk notification timelines by termination type.

02 Account Deactivation
Access is disabled promptly based on the nature and urgency of the termination.

03 Equipment Retrieval
Structured retrieval steps apply to both on-site and remote employees.

04 Post-Employment Contact
All former-employee communications are coordinated centrally through HR.

FRAMEWORK ALIGNMENT

NIST CSF
Protect function — identity and asset management at separation.

CIS Controls
Access revocation and asset recovery upon termination.

ISO/IEC 27001
Termination and change of employment 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 Executive Summary
Objective to ensure timely, secure offboarding across the organization.

§1.2 Scope
Lifecycle coverage from termination notice through equipment return.

§1.3 Objective
Standardization goals spanning HR, IT, and business units. NIST CSF

§2 Terminations
Voluntary and involuntary trigger events and Help Desk notification timelines.

§2.b Account Termination Schedule
Access deactivation timing tied to termination type. CIS Controls

§2.c Equipment Retrieval
Structured retrieval steps for on-site and remote employees.

§2.d Post-Employment Contact
Centralized HR coordination for former-employee communications.
ISO/IEC 27001

Supporting document control: maintained revision history and referenced Employee Asset Retention Policy.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Change Management Policy

A systematic, risk-based approach to planning, reviewing, and implementing changes to Odyssey Logistics production infrastructure and dependent services.

POLICY POL008 | PRODUCTION INFRASTRUCTURE | UPDATED 1/26/2026

PROGRAM OVERVIEW

Odyssey Logistics manages changes to production infrastructure through a structured Change Advisory Board process. The policy classifies change types, sets requirements for review and approval, and requires complete planning, testing, and rollback information to mitigate risk and reduce disruption.

01 Submit
Changes to production infrastructure are classified and submitted with complete, structured request information.

02 Review
A Change Advisory Board evaluates requests on a defined cadence, weighing risk, impact, and business value.

03 Approve
Changes proceed only with required approval; emergency and pre-approved paths are governed with documentation.

04 Execute & Recover
Testing strategies, rollback plans, and communication requirements protect operations through implementation.

FRAMEWORK ALIGNMENT

ITIL
Change Enablement — structured evaluation and authorization of changes.

NIST CSF
Protect function — configuration and change management.

ISO/IEC 27001 Annex A
Change control safeguards for operational systems.

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 Purpose
Systematic mitigation of risk in changes to production infrastructure.

§2 Scope
Standard, emergency, and recurring (pre-approved) change types.

§3 Process Requirements
Defined CAB cadence, submission deadlines, and approval requirements. ITIL

§4 Participating Stakeholders
CAB roles, functional proxies, and communication representatives.

§5 Change Request Requirements
Planning, impact, severity, testing strategy, and rollback plan.
NIST CSF · Protect

Supporting document control: maintained revision history and a referenced documents register.

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.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Data Retention & Destruction Policy

A framework governing how Odyssey Logistics retains, secures, and disposes of records — electronic and non-digital — in line with business needs and legal obligations.

POLICY POL012 | ALL RECORDS | UPDATED 6/9/2025

PROGRAM OVERVIEW

Odyssey Logistics maintains a documented data retention and destruction policy covering electronic and non-digital records. The policy defines retention responsibilities, regulated-record handling, secure destruction methods, and litigation holds, with periodic review by Human Resources, Legal, and Finance.

01 Retain
Records are retained for defined periods to meet business needs and legal and regulatory obligations.

02 Classify & Secure
Digital and non-digital media are classified, securely handled, and stored according to sensitivity.

03 Destroy Securely
Records no longer needed are disposed of using secure, verifiable destruction methods.

04 Hold & Review
Legal holds preserve records under litigation, and retention periods are reviewed periodically.

FRAMEWORK ALIGNMENT

NIST CSF
Identify & Protect functions — data lifecycle and secure disposal.

ISO/IEC 27001 Annex A
Records management and disposal safeguards.

CPRA / CCPA
Regulatory retention obligations for defined record types.

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**
Retention and disposal objectives across records and data files.

§1.3.1 **Regulated Records Retention**
Handling of CPRA-governed record types. Regulatory

§1.4 **Individual & Corporate Duties**
User adherence and IT-enforced automated retention tooling.

§1.6 **Litigation**
Indefinite preservation under legal hold with periodic re-evaluation.

§1.3 **Roles & Authorities**
Data owner responsibilities for preservation and disposal.

§1.3.4 **Termination & Disposal**
Offboarding-based marking, holding, and transfer of records.

§1.5 **Non-Digital Media**
Classification, secure handling, and certified destruction of physical media. NIST CSF · Protect

§1.7 1.8 **Enforcement & Review**
Exception handling and periodic review; schedules in Appendices A & B.

Supporting document control: maintained revision history and included CPRA and internal data retention schedules.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Cyber Security Data Access Policy

The procedures governing requests for access to current and departed employee email and file data from Odyssey Logistics IT systems.

POLICY POL009-A | EMAIL & FILE ACCESS | UPDATED 12/23/2024

PROGRAM OVERVIEW

Odyssey Logistics governs requests for employee email and file data through a defined, default-deny procedure that safeguards privacy while supporting business continuity. Legitimate needs are routed to appropriate alternatives, and departed-employee access follows established offboarding controls with escalation to Legal where warranted.

01 — Default Deny
Access to a current employee's mailbox, forwarding, and personal folders is denied by default.

02 — Route Alternatives
Requesters are guided to distribution groups and shared folders to meet legitimate visibility needs.

03 — Govern Offboarding
Access for departed employees follows defined offboarding steps, with escalation to Legal for critical needs.

04 — Document & Review
All access grants and revocations are logged, and access rights are reviewed periodically for compliance.

FRAMEWORK ALIGNMENT

- **NIST CSF** — Govern & Protect functions — access control and data governance.
- **ISO/IEC 27001 Annex A** — Access control and privacy of personal information.
- **Legal & Compliance** — Data privacy alignment with applicable laws and regulations.

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 & Objective** — Safeguarding assets and continuity when handling email data access.
- **§1.3 Procedure** — Defined framework for handling data-access and retrieval requests.
- **§1.4–1.6 Current Employee Access** — Default-deny for mailbox, forwarding, and personal-folder requests.
- **§1.7 1.8 Departed Employee Access** — Offboarding-driven handling with Legal escalation for critical needs.
- **§1.9 Documentation & Audit Trail** — Detailed records of access grants and revocations for auditing. NIST CSF · Protect
- **§1.10 Security Protocol Updates** — Regular updates to keep procedures effective against evolving threats.
- **§1.11 Legal & Compliance** — Alignment with data privacy and protection requirements. Regulatory
- **§1.12 Follow-Up** — Periodic review of access controls and audit logs.

Supporting document control: maintained revision history and a referenced documents register.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Incident Response Plan & Guidelines

A structured, role-based process for detecting, coordinating, containing, and recovering from security incidents across Odyssey Logistics — built for consistent execution under pressure and continuous improvement afterward.

PROCEDURE PRO003 | ENTERPRISE-WIDE SCOPE | REVIEWED AFTER EACH INCIDENT

PROGRAM OVERVIEW

Odyssey Logistics maintains a formal, documented incident response process governing how security events are assessed, escalated, investigated, contained, communicated, and recovered from. A designated Incident Commander coordinates a structured response across dedicated investigation, remediation, and communication functions — prioritizing containment of active threats, preservation of evidence, and accurate stakeholder communication.

01 Assess & Triage
Events are evaluated for functional, environmental, and information impact to confirm an incident and initiate a proportionate response.

02 Coordinate Response
An Incident Commander activates the response team over secure channels, assigns roles, and drives a disciplined cadence of updates.

03 Investigate & Remediate
Evidence is collected with chain of custody, indicators developed, and threats contained and eradicated on a deliberate timing strategy.

04 Communicate & Recover
Stakeholders are kept informed with accurate, timely updates, and a formal after-action review captures lessons learned.

FRAMEWORK ALIGNMENT

NIST CSF
Detect, Respond & Recover functions — incident handling and recovery practices.

NIST SP 800-61
Computer security incident handling lifecycle and coordination.

MITRE ATT&CK
Adversary tactics referenced to guide investigation & remediation.

WHAT THIS PROCEDURE COVERS

The procedure is structured across the steps below. Each is mapped to the corresponding area of recognized incident-response practice — demonstrating coverage without disclosing internal response specifics.

§1.1 1.2 Purpose & Process Summary
Program intent and the end-to-end incident lifecycle, from detection through post-incident activity.

§2.1 Assess Impact
Functional, environmental, and information-impact triage to confirm and scope an incident. NIST 800-61

§2.2 Initiate Response
Incident Commander activation, secure communication channels, and timely escalation. NIST CSF · Respond

§2.3 Investigate
Evidence handling with chain of custody, hypothesis-driven analysis, and indicator development. MITRE ATT&CK

§2.4 Remediate
Protect, detect, contain, and eradicate actions applied on a risk-based timing strategy. NIST CSF · Respond

§2.5 Communication
Coordinated internal, executive, customer, and regulatory notification grounded in verified facts.

§2.6 Recover
Business continuity integration and a structured after-action review of each incident. NIST CSF · Recover

§2.7 A-B Governance & References
Document review and approval, response-team structure, and an attacker-tactics reference matrix.

Supporting materials: maintained response-team roster, 24/7 escalation contacts, and an attacker-tactics-to-key-questions reference matrix.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

System Outage Work Process

Guidelines for communicating during Priority 1 IT outages, ensuring timely, accurate communication among stakeholders and swift resolution with minimal impact on operations.

PROCESS PRO005 | ENTERPRISE-WIDE SCOPE | ANNUALLY REVIEWED

PROGRAM OVERVIEW

Odyssey Logistics follows a formalized incident communication process for outages affecting client shipment management, defining escalation paths, update cadence, and root cause analysis requirements to support swift, coordinated resolution.

01 — Incident Notification
P1 incidents are reported and severity-assessed immediately upon identification.

02 — Escalation & Response
Defined internal escalation paths route issues to the appropriate response team.

03 — Structured Communication
Stakeholders and clients receive updates on a consistent cadence until resolution.

04 — Root Cause Analysis
A formal RCA process documents findings and drives continuous improvement.

FRAMEWORK ALIGNMENT

- **NIST CSF** — Respond function — coordinated incident communication and resolution.
- **ITIL Incident Management** — Structured incident lifecycle from detection through closure.
- **Internal Escalation Standards** — Defined regional and divisional escalation framework.

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 Purpose** — Guidelines for P1 outage communication and coordinated resolution.
- **§1.2 Process Objectives** — Notification, escalation, communication cadence, and RCA goals. NIST CSF
- **§1.3-1.4 Process Flow** — Step-by-step sequence from issue identification through remediation. ITIL
- **§1.4.4 Communications** — Client and stakeholder update cadence and messaging standards.
- **§1.4.5-1.4.6 Resolution & RCA** — Closure confirmation and root cause documentation timeline.
- **§1.5 Division Escalations** — Structured regional escalation framework across business divisions.

Supporting document control: maintained revision history. Escalation contact details are maintained separately and excluded from this summary.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

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.

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

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

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

§1.6 1.7 Log Retention & Destruction
Protected activity logs and certified secure data destruction.

§1.8 1.9 Reporting & Testing
Monitoring, failure alerting, and recurring recovery testing.

§1.10 1.11 Security & Documentation
Encryption, access controls, and maintained procedure documentation.

§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.

ODYSSEY LOGISTICS
ASSURANCE & TRUST PROGRAM

Disaster Recovery Program

A structured approach to responding to and recovering from disruptive incidents impacting critical IT systems, designed to minimize downtime, protect data integrity, and maintain operational continuity.

POLICY POL016 | ENTERPRISE-WIDE SCOPE | ANNUALLY REVIEWED

PROGRAM OVERVIEW

Odyssey Logistics maintains a documented disaster recovery plan addressing natural disasters, cyberattacks, and hardware failures. The plan defines recovery objectives, escalation procedures, and testing requirements to support rapid restoration of essential logistics services.

01 — Risk & Impact Assessment
IT facility risks and redundancies are catalogued, with recovery priorities set through business impact analysis.

02 — Backup & Recovery Strategy
Scheduled backups, diversified storage locations, and defined RTO/RPO targets by system tier.

03 — Incident Escalation
A structured notification tree carries incidents from first response through executive oversight.

04 — Testing & Improvement
Recurring drills and post-incident reviews feed lessons learned back into the plan.

FRAMEWORK ALIGNMENT

- **NIST CSF** — Respond & Recover functions — incident handling and service restoration.
- **ISO/IEC 27001** — Business continuity and disaster recovery safeguards.
- **Industry DR Standards** — Tiered data center resilience and recovery objective benchmarking.

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 Introduction** — Plan objectives and executive commitment to business continuity.
- **§1.2 Risk & Business Impact Assessment** — Facility risk inventory and RTO/RPO framework by system priority. NIST CSF
- **§1.3 Incident Response Procedures** — Escalation tree and notification cadence during active events.
- **§1.4 Documentation & Record Keeping** — Version control and knowledge-retention practices for recovery procedures. ISO/IEC 27001
- **§1.5 Plan Activation & Execution** — Activation criteria and sequenced recovery execution steps.
- **§Post-Inc. Post-Incident Review** — Structured debrief and after-action reporting process.
- **§App. A-C Risk & Facility Detail** — Disaster scenario library and facility redundancy documentation.
- **§App. D-F Recovery Reference Material** — Priority system recovery objectives and restoration procedures.

Supporting document control: maintained revision history and referenced Incident Response and System Outage Work Process documentation.