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.