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.*