# Data Privacy and Cybersecurity Policy

Protecting client, partner and employee information

| DOCUMENT REFERENCE | REVISION | ISSUE DATE |
|---|---|---|
| FLG-POL-006 | 1 | 04 February 2026 |
| **POLICY OWNER** | **APPROVED BY** | **NEXT REVIEW** |
| Information Technology Lead | Jorge O. Freig Carrillo, Chief Executive Officer | February 2027 |

## 1. Purpose

Freig Logistics Group holds commercially sensitive shipment data, customs declarations, client pricing and personal data belonging to employees, drivers and client contacts. This policy sets how that information is protected, who may access it, and what happens when something goes wrong.

## 2. Scope

This policy applies to every entity, facility, employee, officer, temporary worker and contracted third party operating under the Freig Logistics Group name, including Nogales Transportation Services, LLC and every affiliated transportation, customs brokerage and warehousing company within the group. It applies at all owned and leased facilities in the Arizona and Sonora corridor and on every lane managed on behalf of a client, on both sides of the United States and Mexico border.

It covers all information in any form, including data held in the transportation management system, customs filing platforms, telematics and IoT systems, email, cloud storage, mobile devices and physical records.

## 3. Legal Framework

- Mexican Ley Federal de Proteccion de Datos Personales en Posesion de los Particulares and its implementing regulations.
- California Consumer Privacy Act as amended by the California Privacy Rights Act, and other United States state privacy laws where applicable.
- EU General Data Protection Regulation, where personal data of individuals in the European Union is processed.
- Data handling obligations attaching to customs filings with U.S. Customs and Border Protection and with SAT through VUCEM in Mexico.
- Client contractual data protection and data residency requirements.

## 4. Data Protection Commitments

1. Collect only the data required for a defined and lawful purpose, and use it only for that purpose. Client shipment data is never used for any secondary commercial purpose and is never sold.
2. Hold client data in logically segregated environments, apply the data residency required by contract, and retain it only for the defined retention period before secure destruction.
3. Grant access on the principle of least privilege through role based access control, reviewed on a scheduled basis and revoked on the day a person leaves or changes role.
4. Encrypt data in transit and at rest using current industry standard algorithms.

5. Require multi factor authentication for all remote and administrative access, and single sign on integration where the client environment supports it.
6. Maintain endpoint protection, network segmentation, centralized logging, vulnerability scanning and a defined patching cadence with prioritized remediation of critical vulnerabilities.
7. Back up critical systems on a defined schedule and test restoration at least annually against documented recovery time and recovery point objectives.
8. Honor data subject rights, including access, correction, deletion and objection, within the timeframes set by the applicable law.

## 5. Third Party and Platform Assurance

Core platforms are assessed before adoption and monitored thereafter. Where a platform processes client or personal data we require current independent assurance, such as a SOC 2 Type II report or ISO/IEC 27001 certification, together with contractual security, confidentiality, breach notification and audit terms. Subcontracted carriers and agents receive only the minimum data required to perform the movement.

## 6. Personnel

All personnel sign a confidentiality undertaking, complete security awareness training on appointment and annually thereafter, and are subject to background verification where this is lawful and proportionate to the role. Access is removed on the day employment ends.

## 7. Incident Response and Breach Notification

A documented incident response plan defines detection, containment, eradication, recovery and post incident review, with named roles and an escalation path. Any suspected breach must be reported internally immediately. Affected clients are notified without undue delay, and regulators and data subjects are notified where and within the timeframe the applicable law requires. The plan is exercised at least annually.

## 8. Business Continuity

Recovery time and recovery point objectives are defined for each critical system. Manual fallback procedures exist for dispatch, customs filing and client communication so that freight continues to move during a system outage. Continuity arrangements are tested at least annually.

## 9. Responsibilities and Review

- The Chief Executive Officer is accountable for information security and privacy across the group.
- The Information Technology Lead maintains the controls, the incident response plan and the vendor assurance register, and reports to management.
- Managers are responsible for the access held by their teams and for requesting timely revocation.
- Every user is responsible for protecting credentials, using approved systems only, and reporting suspected phishing or compromise immediately.

This policy is reviewed at least annually and following any material incident, system change or change in applicable law.

**Approved and issued by**

**Jorge O. Freig Carrillo**
Chief Executive Officer
Freig Logistics Group

**Signature and date**