ISCPO
International Supply Chain Protection Organization

CARRIER CERTIFICATION & SELF-ASSESSMENT

This Carrier self-assessment will be used to help determine ISCPO Certification acceptance.

The Carrier will evaluate whether their internal programs and policies at the organizational level meet the ISCPO standards within this document. This is not intended to assess whether individual Carrier locations currently pass all standards.

The Carrier must assign a grade of fully meets, partially meets or does not meet to each ISCPO Security Requirement within this document. Requirements that either partially meet or do not meet will require a detailed explanation of each deficiency on the lines below each section.

It is permissible to mark a requirement as fully meeting expectations even if some locations may fail as long as the Carrier expects those deficient locations to be brought up to ISCPO standards within 30 days of recognizing them. It is NOT permissible to mark fully meets if the Carrier knows that they cannot or will not bring a specific location(s) up to ISCPO standards.

I. Introduction

II. ISCPO Verification

CARRIER SELF-ASSESSMENT

- Onboarding Employees/Contractors
- Systems and Access Control
- Security of Deliverables & Returns
- Loss Notifications/Investigations
- Policies and Awareness
- Operations & Scanning

I. Introduction

This document reflects a collection of best loss prevention and theft detection practices within the Security/Loss Prevention industry. The standards set forth in this document by a consortium of Security/Loss Prevention practitioners from various companies agree that Regional Carriers a.k.a. Final-mile Carriers are an instrumental component our own supply chains and should be embraced as valuable business partners.

This consortium known as the **ISCPO Carrier Audit Committee** intends to stay current with changing laws or regulations and provide updates to this document as needed while being mindful not to unnecessarily impede business with impracticality or cost prohibited requirements.

It is our hope and desire that these ISCPO Carrier Security Requirements will be adopted by a majority of Final-mile or Regional Carriers as well as the organizations that contract with them. By embracing these standards, the benefits to both parties are numerous but most importantly the Carriers can stand behind one set of requirements without having to manage various customer programs differently within the same space. It sets the Carrier up for success by reducing wasteful time and expense from the operation.

For the purpose of this document, the carrier's management, employees, agency workers, contractors, subcontractors and independent contractors that handle or access Carriers client's deliverables or account information will be referred to as "The Carrier" unless otherwise written to address a particular role.

II. ISCPO Verification

ISCPO Members reserve the right to conduct unannounced remote or onsite audits at any time in order to measure and report on Carrier security/Loss Prevention compliance. This may be in congruence with any operational work that the member is doing on behalf of their employer if that employer is currently in a work relationship with the Carrier. The Carrier shall assist the audit by providing all requested documents and information required to complete a comprehensive review of Security/Loss Prevention compliance. The ISCPO will recognize any propriety audit form that its members might use for its normal course of business with the Carrier.

The ISCPO Carrier Audit Committee and/or Board of Directors will review all audits submitted by its members. If the ISCPO deems the carrier is not in compliance or not following the standards they disclaimed in there self-assessment, the ISCPO may ask the carrier to produce an action plan addressing the discrepancies found. The ISCPO does reserve the right to revoke the Carrier's Certification at any time if it deems the Carrier is not in compliance.

CARRIER SELF-ASSESSMENT

Onboarding Employees/Contractors

Background Screening: **A**ll Carrier workers including but not limited to employees, agency labor, drivers, subcontractors and independent contractors who handle or supervise deliverables or account information have undergone an extensive background check to include:

(a) A comprehensive criminal background check conducted in accordance with the applicable laws for the relevant state. It is recommended that no person convicted of a felony in the last 7 years to include but not limited to Drug, Theft, Violent Crimes or other convictions that pose a foreseeable liability to either party will be allowed to handle, access, or supervise the Carriers client's freight.

(b) Proof of United States of America citizenship or valid visa, green card, or other documentation issued by the government authorizing such person to work in the United States of America.

Drug Screening: **A**ll Carrier personnel including but not limited to employees, agency labor, drivers, subcontractors and independent contractors who handle or supervise the Carrier's client's deliverables or account information have undergone a certifiable drug screening test to identify illegal substances.

(a) A passing record must be on file with the Carrier before the person is allowed to handle, access, or supervise the Carrier's client's deliverables or account information.

Full ☐ Partial ☐ No Compliance ☐

Systems and Access Control

Intrusion Alarm System: Carrier facilities that close or are void of personnel for any amount of time, require an alarm system that can detect unauthorized access to Carriers client's deliverables or account information. The basic requirements for an intrusion alarm system are:

- Armed during unoccupied times

- 24/7 alarm monitoring company
- Current notification and user list on file with the monitoring company
- Tested at least quarterly
- Unused perimeter doors (i.e. emergency exits) are on siren 24/7
- Personal Identification Numbers (PINs) are unique to each user and are not shared.

Security Cameras: Each Carrier facility must have a functional security camera system with:

- Recording retention of at least 30 days
- Recording device is kept secured. Only accessible to authorized Carrier personnel
- Camera coverage for all area(s) of the interior of the terminal.
- Cameras on all Carrier client's areas must provide sufficient clarity to positively identify people and handling/movement of Carrier client's deliverables.
- Lighting must be sufficient to support video clarity

Access Control: Carrier must be able to appropriately restrict and deny access into the facility. Controlling access may be accomplished in many different ways including utilization of personnel, guards or locking mechanisms.

- **Restrict Access**: This means that a person such as an employee, agency labor, driver, subcontractor, independent contractor or visitor must have received explicit permission to enter by the Carrier. Entry is granted only when the Carrier opens the door for this person or the Carrier has provided the person with an appropriate "key" (key, card, code, etc…) to disengage the locking mechanism.

- **Deny Access**: This means that any person that the Carrier has not authorized to enter is physically prohibited from entry or denied further entry by personnel/guard or locking mechanism.

- **Key Control**: "Keys" (key, card, code, etc…) must never be left unattended in an unsecured manner. A "key" log must be kept updated indicating who is in possession of "keys". All "keys" must be returned or deactivated at the end of the person's employment or contract. Procedures must be in place to secure the area/facility if keys are not returned.

Identification Badge: All Carrier personnel including but not limited to employees, agency labor, drivers, subcontractors and independent contractors who handle, access or supervise Carrier client's deliverables or account information must have a Carrier issued ID badge visibly displayed on their person while at the Carrier's place of business or any Carrier client's receiving or shipping destinations. All ID badges are to be controlled by the Carrier and collected upon the termination or resignation of the person. ID Badges must include the following identifiers:

- Carrier's name/logo
- Person's name
- Photo (recommended)

Visitor Sign-In: All visitors to the Carrier's facility must sign in on a visitor's log which at a minimum documents the visitor's name, company, person visited, visitor badge number and time/date of arrival and departure. Sign-in must also include verification of the visitor's identity by checking government issued identification such as a driver's license. Visitors must be escorted at all times.

Visitor's Badge: All visitors to the Carrier's facility must be issued a visitor's badge or alternative method of identification, prior to accessing the facility. Visitor badges or alternative must be visibly displayed on the person at all times and returned at the conclusion of the visit. The Carrier must demonstrate that badge inventory and accountability is being maintained.

Full	Partial	No Compliance
☐	☐	☐

Security of Deliverables & Returns

Deliverables: The Carrier must continuously "monitor" all deliverables between receiving and driver launch. Monitoring means proving a chain-of-custody is present to document movement and safeguard of the deliverables. Monitoring can be accomplished by utilizing security cages, locked rooms, security cameras or personnel guarding the deliverables without any gaps in the chain-of-custody. All deliverables must be monitored at all times, regardless of the disposition (i.e. bad/missing label, damaged, returned, etc…).

Returns: Carrier must treat all Carrier client's returns with the same level of security as deliverables. Returns must be monitored at all times within the Carrier facility. Returns must be separated and held in a staging area by Customer. Staged returns must be segregated from all deliverables. The returns area must be clearly identified with signage. Returns must be transported in a secured cargo area with proper seal control.

Vehicle Security: Delivery vehicles must be secured whether in transit or parked. Cargo doors to the vehicle must be locked immediately after loading/unloading and while in transit. The vehicle must be completely secured when it is unattended outside the Carrier's facility or at stops. Secured means that the vehicle is turned off (exceptions for fob controlled ignitions), keys removed from the ignition switch, windows rolled up and all doors are locked. Deliverables/Returns must be kept in the cargo area, never in the driver's cab. The cargo area must be secured at all times, whether internal locking mechanism or padlock.

Seal Control: Carrier must demonstrate proper seal control. Seals must be kept secured when unattended. A seal log must be kept to historically document all seal assignments. Seal logs must include at least the

date/time of application, seal serial number, destination, truck or BOL identifier and person applying the seal. The removal process is documented by the Carrier, circling and initialing the seal's serial number on all copies of the BOL after verifying that there is a match between the actual seal and paperwork. Carrier must never permit drivers to apply, break or handle seals.

Cross Docking: Cross Docking refers to when the Carrier transports deliverables from their origin facility to a destination facility, where further handling and delivery will be performed. The transport of these deliverables requires the same level of security as with Delivery Vehicles, including a secured cargo area. Cross docking vehicles must have a cargo area that is completely segregated from the driver's area and secured with a trailer seal and lock. Carrier must never permit drivers to apply, break or handle seals. The seal's serial number must be communicated to the subsequent Carrier location so validation can be conducted upon receiving.

Dropped Trailers: Carriers must properly monitor dropped trailers containing Carriers client's deliverables. The Carrier must have a layered security approach for any load that is not live. Trailer locks in addition to secured yards and/or camera coverage are mandatory. Additional layers of security may be required by various clients based on risk factors (i.e. type of load, frequency of drops and hours of operation).

- Trailer Locks (5th wheel locks, dock locks, etc…)
- Secured Yard (i.e. Fence w/ locked gates or Guard Coverage)
- Yard Camera Coverage
- Adequate Yard Lighting

Full ☐ Partial ☐ No Compliance ☐

Loss Notification/Investigations

Theft: When the carrier discovers a theft or loss situation is occurring they must have plan of action in place to notify customers affected. In coordination with clients Loss Prevention or Operations departments, a joint investigation will be conducted to determine the root cause of the losses, individuals involved and exposures identified that attributed to the loss. Under no circumstances should the carrier withhold information from its clients as it pertains to losses.

Policies and Awareness

Parking: Personal vehicles are not allowed to park at or near Carrier dock doors. All personal vehicles must park only in designated parking spaces.

Document Security: Carrier must ensure that all paper and electronic documents pertaining to Carrier client's account(s) are secured when unattended. Locks and/or password protection is used to deny access to persons who are not authorized.

Information Security: User Ids and passwords must never be shared. Each user must have unique sign-on credentials for scanners and computer systems. Carrier must be able to definitively identify who created a specific scan transaction using a scanner or computer terminal, being either an actual scan of a bar code or keyed entry.

Ethics Reporting Program: Carrier must provide a method for employees, agency workers, contractors, subcontractors and independent contractors to report unethical or criminal behavior, anonymously if desired.

Loitering: Carrier must not allow employees, agency workers, contractors, subcontractors or independent contractors to loiter in spaces with access to Carrier client's deliverables or account information, after their shift or assignment has been completed.

Full ☐ Partial ☐ No Compliance ☐

Operations & Scanning

Freight Receiving: When Carrier client's deliverables arrive, the Carrier must first verify that the cargo was transported in a locked and sealed trailer. Carrier will follow proper seal and load verification procedures which include reviewing the Bill of Lading (BOL) to verify the seal number and quantity of tendered units match what is physically present. Carrier will document the verification process by circling and initialing the BOL's seal number and tendered units. Any discrepancy must be noted on all copies of the BOL and reported to the respective client. BOLs must be kept on file for a minimum of 90 days.

Created: 11-2015
Revised: 4-2016

Scan Receiving & Sort: All deliverables must be monitored during the scan receiving & sortation process, without gaps in the chain-of-custody. All deliverables must be scan received as soon as they are off-loaded from the trailer either by the driver or warehouse personnel.

Loading: Carrier must monitor the loading process to ensure accuracy, prevent losses and ensure all Carrier client's deliverables are accounted for on each route. First, the Carrier must visually inspect all delivery vehicles' cargo and cab areas prior to loading to ensure no undelivered freight from prior day(s) business is present. Second, mis-sorted or problematic deliverables identified by drivers during the loading process must be corrected by Carrier personnel, not the driver. All deliverables must be scanned to the driver's route during the physical loading process.

Delivery: Drivers must scan all deliverables at the exact location that the End Receiver takes physical possession. Delivery scans must never be conducted at or inside the delivery vehicle. Drivers must capture a receiver's signature on the scanner or paper manifest. Drivers must never complete the POD signature field themselves. Drivers must never leave deliverables without a signature. An "unattended delivery" model is the exception to the "POD capture" rule and will be documented for the Carrier separately by those respective clients. Drivers must report all delivery concerns to the Carrier.

Reconciliation: Carrier must reconcile each route, every day. Reconciliation means verification that all deliverables received will total the amount of deliverables loaded and delivered. The reconciliation process must include a comparison of delivery scans and PODs (both electronic and paper manifests) against load and receiving scans.

Exceptions: The Carrier must report any concerns or deviation of these security/loss prevention requirements to their respective clients. This includes any operational issues with the ASN, OS&D, scanning, labels, return logs, etc…

Full ☐ Partial ☐ No Compliance ☐

CARRIER: _____

EMPLOYEE NAME: _____

TITLE: _____

SIGNATURE: _____

DATE: _____

ISCP
International Supply Chain Protection Organization