The Product Realization Company

NOTE: After review of this document please return signed copy to PLXS-CORP.CTPAT@plexus.com

Plexus Corp.
Import Vendor Compliance Manual

Plexus Corp. ("PLEXUS") requires its foreign shippers to provide all documentation required for entry into the U.S. to their foreign freight consolidator, carrier, or directly to PLEXUS prior to exportation, as specified under other associated agreements, such as a approved purchase order. Because of the requirements and regulations for various U.S. government agencies, documentation types may vary and may include additional declarations or statements that are not contained in the following list. The foreign shipper is to contact the PLEXUS' Corporate Logistics Group if there are any questions regarding the type of documentation required for entry into the U.S. In general, the following documentation is required:

1. Commercial Invoice
2. Packing List
3. Bill of Lading
4. Other U.S. government agency documentation and declarations, such as the Federal Communications Commission, Food and Drug Administration, Department of Transportation, Environmental Protection Agency, and Textile Manufacturer's name and address, when applicable.

With the enactment of the U.S. Treasury Directive 02-62 on December 2, 2002, it is a requirement for shippers to provide complete and accurate product descriptions and/or HTS Numbers (to the six-digit level) to the companies providing the cargo manifest to U.S. Customs & Border Protection (CBP) 24 hours prior to the cargo being laden on board. If accurate descriptions are not provided, the cargo can be denied loading on board the vessel. This regulation applies to all ocean cargo destined for the U.S., whether the cargo is to remain in the U.S. or be transported in-bond to another country. These regulations have been implemented as well for air and truck cargo as of December 2003. In addition, under Title 19 of the Code of Federal Regulations (19 CFR §141.86), commercial invoices are required to provide the following information in English:

1. Invoice number
2. Invoice date
3. Terms of sale (i.e. "Net 30, Draft/At Sight, etc.")
4. Trade terms (i.e. INCOTERMS (EXW, FOB, CIF, etc.)
5. Net and gross weight for merchandise
6. Detailed, accurate description of merchandise, including a part or model number/style, marks and numbers
7. Quantity of merchandise
8. Shipping unit of measurements
9. Unit price in the currency of the purchase
10. Type of currency
12. Country of origin of the merchandise
12. Name and address of the foreign party responsible for invoicing, and the actual manufacturer's complete name and address (if the party varies from the foreign invoicing party)

***Note**: PLEXUS has issued formal Importer Security Filing Requirements and Commercial Invoice requirements to its suppliers through its purchase order terms and conditions and at the following website: https://www17.plexus.com/extranet/file_storage/logistics.cfm. Plexus partners are required to following these guidelines.*

PLEXUS expects that its foreign Shippers will immediately work towards implementing the U.S. Customs-Trade Partnership Against Terrorism (C-TPAT) “Required Procedures”, and strive towards implementing the “Recommendations”, consistent with C-TPAT Supply Chain Security Criteria listed below:

1. Container Security

Required Procedures

Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At point of stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers. A high security seal must be affixed to all loaded containers bound for the U.S. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

a. Container Inspection
Procedures must be in place to verify the physical integrity of the container structure prior to stuffing, which includes the reliability of the container door locking mechanisms.

b. Container Seals
Written procedures must stipulate how seals are to be controlled and affixed to loaded containers, which includes procedures for recognizing and reporting compromised seals and/or containers to U.S. Customs & Border Protection or the appropriate foreign authority.

c. Container Storage
Containers must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers or container storage areas.

Recommendations

d. Container Inspection
A seven-point inspection process is recommended for all containers:
- Front wall
- Left side
- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors
- Outside/Undercarriage

Container Seals
Only designated employees should distribute container seals for integrity purposes.

2. Physical Access Controls

Required Procedures

Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

a) Employees

An employee identification system must be in place for positive identification and access control purposes. Company management or security personnel must adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (e.g. keys, key cards, etc.) must be documented.

b) Visitors

Visitors must present photo identification for documentation purposes upon arrival.

c) Deliveries (including mail)

Proper vendor ID and/or photo identification must be presented for documentation purposes upon arrival by all vendors.

d) Challenging and Removing Unauthorized Persons

Procedures must be in place to identify, challenge and address unauthorized/unidentified persons.

Recommendations

e) Packages

Arriving packages and mail should be periodically screened before being disseminated.

f) Visitors

All visitors should be escorted and visibly display temporary identification.

g) Secure Access

Employees should only be given access to those secure areas needed for the performance of their duties.

3. Personnel Security

Required Procedures

Processes must be in place to screen prospective employees and to periodically check current employees.

a) Pre-Employment Verification

Application information, such as employment history and references must be verified prior to employment.

b) Personnel Termination Procedures

Companies must have procedures in place to remove identification, facility, and system access for terminated employees.

Recommendations

c) Background checks / investigations:

Consistent with foreign, federal, state, and local regulations, background checks and investigations should be conducted for prospective employees. Once employed, periodic checks and reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.

4. Procedural Security

Required Procedures

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

a) Documentation Processing
Procedures must be in place to ensure that all information used in the clearing of merchandise/cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information. Documentation control must include safeguarding computer access and information.

b) Manifesting Procedures
To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and timely.

c) Shipping & Receiving
Drivers delivering or receiving cargo must be positively identified before cargo is received or released.

d) Cargo Discrepancies
All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. Customs and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected, as appropriate.

Recommendations

e) Cargo Discrepancies
Arriving cargo should be reconciled against information on the cargo manifest. The cargo should be accurately described, and the weights, labels, marks, and piece count indicated and verified. Departing cargo should be verified against purchase or delivery orders.

5. Security Training and Threat Awareness

Required Procedures

Employees must be made aware of the procedures the company has in place to address security and threat situations, and how to report them.

Recommendations

a) Threat Awareness
A security training and threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorism at each point in the supply chain

b) Training
Additional training should be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail. Additionally, specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation.

6. Physical Security

Required Procedures

Cargo handling and storage facilities in domestic and foreign locations must have physical barriers and deterrents that guard against unauthorized access.

a) Fencing
All fencing must be regularly inspected for integrity and damage.

b) Gates and Gate Houses
Gates, through which vehicles and/or personnel enter or exit, must be manned and/or monitored.

c) Building Structure
Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by periodic inspection and repair.

d) Locking Devices and Key Controls
All external and internal windows, gates and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

e) Lighting
Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.

Recommendations

f) Alarms Systems & Video Surveillance Cameras
Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.

g) Parking
Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas.

h) Fencing
The number of gates should be kept to the minimum necessary for proper access and safety. Fencing: Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo.

7. Information Technology Security

Required Procedures

a) Password Protection
Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards must be in place and provided to employees in the form of training.

b) Accountability
A system must be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators must be subject to appropriate disciplinary actions.

We have read and agree to work towards implementing all U.S. Customs-Trade Partnership Against Terrorism (C-TPAT) Required Procedures in the PLEXUS Shipper C-TPAT Instructions, in a timely manner. Furthermore, we will strive towards implementing the Recommendations, were deemed appropriate. Upon any updates or improvements to our Supply Chain Security Procedures we will immediately notify PLEXUS' Corporate Logistics Group.

Shipper Name:

_____

Shipper Contact Person:

_____

Shipper Signature:

_____

Agreement Date:

_____