LOGISNEXT AMERICAS INC.

SUPPLIER CODE OF CONDUCT

1. INTRODUCTION

Scope and Purpose

This Supplier Code of Conduct (this "Supplier Code") of Logisnext Americas Inc. ("Logisnext") is a set of standards that articulates Logisnext's expectations for the conduct of its suppliers (its "Suppliers").

Logisnext expects its Suppliers to understand and act consistently with this Supplier Code. Logisnext expects that its Suppliers will flow-down similar expectations throughout their own supply chains.

Logisnext expects its Suppliers will satisfy applicable contractual requirements, comply with all applicable laws and regulations, and act consistently with the principles and values set forth in this Supplier Code.

From time to time, as required under applicable law or as Logisnext determines to be advisable, Logisnext may request Suppliers to provide individual certifications of compliance or other information relating to specific provisions of this Supplier Code and similar matters.

2. HUMAN RIGHTS

Forced Labor

Logisnext opposes the use of forced labor within any portion of its supply chain. Logisnext has developed a Social Compliance Program designed to prevent that goods imported into the United States from its suppliers were mined, produced, or manufactured, wholly or in part, with forced labor, e.g., imprisoned, indentured, or child labor.

Suppliers shall not use forced labor in any of their operations.

Human Trafficking

Suppliers shall not engage, directly or indirectly, in human trafficking.

Conditions of Employment

Suppliers shall comply with all applicable laws regulating work hours, wages, and benefits.

Labor Brokers

If Suppliers use a labor broker, Suppliers shall ensure that their broker employs ethical recruitment practices and complies with all applicable laws.

Discrimination and Workplace Diversity

Suppliers shall follow all relevant laws that prohibit discrimination and harassment in hiring and employment practices and retaliation.

Without limiting the generality of the foregoing, Suppliers and their subcontractors and agents shall, to the extent same are applicable, abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a), which (i) prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, (ii) prohibit discrimination against all individuals based on their race, color, religion, sex, or national origin and (iii) require affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, national origin, protected veteran status or disability. If applicable, Suppliers, their subcontractors and agents shall abide by the requirements of 29 CFR Part 471, Appendix A to Subpart A.

3. DATA PRIVACY AND SECURITY

Protecting Confidentiality and Privacy

Suppliers shall safeguard Logisnext's confidential assets and information from unauthorized access, use, or disclosure. Suppliers shall implement and maintain appropriate processes and measures to ensure the security and integrity of this information.

Suppliers shall comply with all applicable local laws regarding the protection of personal information. Suppliers shall only use, access, and disclose personal information provided by or on behalf of Logisnext only as expressly authorized by Logisnext in writing.

4. WORKPLACE SAFETY

Working in a Safe Environment

Suppliers shall provide clean, healthy, and safe environments for their employees that meet or exceed applicable legal standards.

Continuous Improvement

Suppliers shall continuously review and improve their occupational health and safety procedures and guidelines and give employees the appropriate training and information required to manage risks in their work environment.

5. ENVIRONMENT

Responsible Stewardship

Suppliers shall look to conserve resources and protect the communities and environment that surround them. Suppliers shall develop and use environmentally friendly technologies and to increase the use of renewable energies.

Continuous Improvement

Suppliers shall increase efficiency throughout their companies and take measures to reduce their carbon footprint, energy use, water use, wastes, and other emissions. Suppliers shall continually look for ways to use environmentally friendly processes and materials and to pursue developing environmentally friendly technologies.

Compliance

Suppliers shall comply with applicable national and international regulations as well as standards on environmental protection that affect their operations. Environmental pollution shall be minimized, environmental protection continuously improved and resources used sparingly. Suppliers shall establish and apply an environmental management system in accordance with ISO 14001 or an environmental management system suitable for the relevant industry.

Chemicals of Concern

Suppliers shall comply with applicable statutory ingredient prohibitions, restrictions, and declaration regulations. Supplier shall notify Logisnext of any ingredients contained in the products it supplies to Logisnext identified as Chemicals of Concern by the Environmental Protection Agency or listed in Section 5(b)(4) of the Toxic Substances Control Act or as PFAS ("forever chemicals") and, upon request, provide Logisnext with information on such ingredients, including but not limited to the content, quantities, and origin of any such ingredients.

Hazardous Materials

Suppliers shall not utilize any hazardous materials, including, but not limited to, asbestos or any other toxic or hazardous substances set forth in 29 CFR 1910 Subpart Z—Toxic and Hazardous Substances in the production of any products they supply to Logisnext and shall ensure that any products supplied by them to Logisnext do not contain any such hazardous materials.

6. TRADE CONTROLS

Logisnext conducts as part of its business activities a significant volume of U.S. import transactions involving extensive dealings with U.S. Customs and Border Protection ("CBP").

In addition, Logisnext is a member of the CBP Trade Partnership Against Terrorism Program ("CTPAT") that promotes international supply chain security and the prevention of illegal activities in connection with the import of products into the United States.

In view of the foregoing and in order for Logisnext to participate in CTPAT, Logisnext requires its suppliers to comply with:

- the U.S. import procedures summarized in Attachment A – U.S. Import Procedures
- the CBP-mandated security standards set forth in Attachment B - Security Standards for Suppliers, Attachment C – Factory Security Certification Standards and Attachment D – Container Search and Seal Integrity Program

Further, Supplier covenants and agrees to grant Logisnext or a designated representative the right to visit their facilities to conduct CTPAT security training for key Supplier personnel and/or to perform an assessment of their compliance with the CTPAT Security Standards. Logisnext will make such requests in writing and will coordinate the visit so as not to create an unreasonable burden on Supplier. CBP officials may accompany Logisnext on such facility visits. CBP routinely selects Logisnext supplier facilities to visit each year.

Suppliers shall comply with all United States and other applicable trade controls regarding products and services provided to Logisnext. Suppliers shall not engage in direct or indirect commercial activity with sanctioned countries, territories, entities, persons, or sectors and shall conduct appropriate due diligence to comply with sanctions, export controls, and anti-boycott requirements.

7. BUSINESS INTEGRITY

Anti-Corruption and Anti-Bribery

Suppliers shall not tolerate corruption, bribery, embezzlement, or fraud in any form. This includes giving or receiving anything of value, including money, gifts, or unlawful incentives to improperly influence negotiations or any other dealings with governments and government officials, customers, or any other third parties. Suppliers shall not provide facilitation payments.

Conflicts of Interest and Ethical Behavior

Suppliers shall avoid conflicts of interest and operate honestly and ethically throughout their supply chains and in accordance with applicable law, including laws pertaining to: anti-competitive business practices, respect for and protection of intellectual property, company and personal data, export controls, and economic sanctions.

Financial Integrity

Suppliers shall honestly and accurately document and report financial information. Suppliers shall not conceal illicit funds or otherwise facilitate or support money laundering. Suppliers shall not engage in any insider trading.

Reporting and Non-Retaliation

Suppliers shall provide an adequate mechanism for their employees to report integrity concerns, safety issues, and misconduct without fear of retaliation. Suppliers shall appropriately investigate reports and take corrective action, if needed.

Conflict Minerals

Suppliers shall not utilize any tantalum, tin, gold or tungsten originating from any Covered Country in the production of any products they supply to Logisnext and shall ensure that any products supplied by them to Logisnext do not contain any such minerals.

A “Covered Country” includes Democratic Republic of the Congo and any of its adjoining countries, Angola, Burundi, Central African Republic, Congo Republic, Rwanda, South Sudan, Tanzania, Uganda and Zambia.

Reporting Integrity Concerns to Logisnext

Subject to any restriction imposed by applicable law, Suppliers shall promptly inform Logisnext of any concern related to issues governed by this Supplier Code. To report a concern, Suppliers may speak directly to their Logisnext supply chain contact person. In addition, the Logisnext Reporting Line allows Suppliers to report concerns of misconduct occurring at or affecting Logisnext. Individuals can file a report 24 hours a day, 7 days a week online at https://app.convercent.com/en-us/LandingPage/7b5b5478-8185-ea11-a974-000d3ab9f062 or by calling (800) 461-9330. Individuals filing reports on the Logisnext Reporting Line may remain anonymous if they so choose.

Stakeholder Engagement

Suppliers shall develop and implement appropriate internal business processes and policies to ensure compliance with applicable law and this Supplier Code. Suppliers shall demonstrate compliance with this Supplier Code upon Logisnext's request.

Last Updated Date: April 30, 2026.

Attachment A

U.S. Import Procedures

CBP requires that all documents listed below accompany each export to Logisnext. For legal purposes, accurate completion of all documentation is required to avoid the potential delay of a shipment.

Commercial Invoice

The Supplier is required to prepare an accurate commercial invoice that conforms to applicable Foreign Export Requirements and U.S. Importation Requirements for entry into the United States.

19 CFR §141.86 sets forth the general requirements for information to be included on the commercial invoice for imported merchandise. Per U.S. Customs and Border Protection (CBP) requirements, "Proforma" invoices will not be accepted.

Logisnext requires the Supplier to provide a commercial invoice prepared in 'English' and include all the following as specified stated below.

- **Commercial Invoice Number** *(Proforma invoices will not be accepted.)*
- **Purchase Order Number**
- **Shipper Name and Address** must include Contact Name, Full Physical Address (including postal code)
  Phone Number and E-mail Address
- **Buyer/Consignee Full Name and Address** must be listed
- **Customs Broker Name and Address** must include Contact Name, Full Physical Address, Phone Number and E-mail Address
- **Product Number** must be stated
- **Product Description** must include a full description in detail of each product shipped to allow classification of the product under **the United States Harmonized Tariff Schedule of the United States (HTSUS) Code.** For further information, go to: **http://www.usitc.gov/tata/hts/bychapter/index.htm**
- **Country of Origin (COO)** must be listed as 2-letter ISO code per each item shipped. COO refers to the country where a product is produced or substantially transformed, not the country from where the product was last shipped.

  Definition: *The Country of Origin is the country of manufacturer, production or growth of an article or product comes from. If the article is produced, derived from or processed in more than one country, it shall be considered a product of the country where it last underwent a substantial transformation.*
- **Weight and Measure** of each product shipped

- **Quantity** of each product shipped
- List the kind of **currency**
- **Total Value per Product** at the item level
- **Total Value per Shipment** *(Transaction Value – **"Price Paid"** or **"Payable"**)*
- **No Sale of Shipment is** accepted *(Invoice must state **"For Customs Purposes Only"**)*
- **Do Not Use the Wording – "*No Commercial Value"***
- **Shipping Terms** *(INCOTERMS 2020 – in accordance with applicable commercial agreement)*
- **Numbering of Pages** *(i.e., Page 1 of 10; Page 2 of 10....)*
- **Do Not Use Wording** – "***U.S. Goods Returned"***
- **Bearings** must include:
    - **Country of Origin**
    - **Manufacturer Name and Address**
    - **Rolling Element Type** *(including inner and outer diameter)*

Logisnext requires the Supplier to provide a Bearing Worksheet for each bearing product supplied in a given shipment.

Bill of Lading

The Supplier is responsible for completing the Bill of Lading and providing this document to the carrier at the time the shipment is tendered. To reduce the incidence of unauthorized use of the bill of lading, unauthorized access to these critical documents should be prevented by providing a secure, controlled environment with strict access controls. The Bill of Lading (BOL) filed with CBP must show the first foreign location/facility where the carrier takes possession of the cargo destined for the United States.

Logisnext's shipper or its agent must provide BOLs and/or manifests that accurately reflect the information provided to the carrier. Additionally, carriers must exercise due diligence and confirm BOLs are accurate. BOLs and manifests must be filed with CBP in a timely manner by the relevant supply chain security partner.

Packing List

The Supplier will enclose a Packing List with each shipment. The packing list must include a detailed list of the contents of the shipment *(i.e., quantities, items, model numbers, dimensions, net weight, and gross weight).* The packing list must also specify per carton or crate, the number of the type of units of material inside. When more than one package is shipped, the Supplier must identify the specific carton or crate to which the packing list is attached. The carton or crate carrying the packing list is to be placed adjacent to the door of the container to be readily available for receiving personnel.
Each carton or crate exterior must be marked with the Logisnext Purchase Order Number which corresponds with the Purchase Order included within the shipment.

Steel Mill Certificate

A supplier that exports steel products to Logisnext must obtain a Steel Mill Certificate from the steel mill/steel producer that includes all the material specifications and the name and address of the manufacturer and provide it to Logisnext. CBP requires the importer (Logisnext) to submit a Steel Import License for all steel imports.

A Steel Import License is a statement of compliance with the material specifications of the American Society of Mechanical Engineers' Boiler and Pressure Vessel Code, Section II.

For further information, go to: **https://help.cbp.gov/app/answers/detail/a_id/197/~/importing---licenses%2Fpermits**

A Steel Mill Certificate must be provided with all other required import documents to the Logisnext customs broker for accurate and compliant import processing of the product into the U.S.

Manifest

The Supplier, with the assistance of the forwarding agent, must prepare an itemized list of contents of the shipment to the carrier along with sufficient information to enable the carrier to provide a proper manifest to CBP.

Environmental Protection Agency (EPA)

A Supplier that exports engines to Logisnext must submit a **U.S. Environmental Protection Agency (EPA) Engine Declaration Form *(Form 3520-21)*** to CBP for each imported engine to Logisnext. Logisnext must identify the engine manufacturer, engine model, build date and serial number for each engine. To comply with this requirement, the Supplier of the engines must provide Logisnext with the serial number, date of manufacturer *(Month/Year)* and model of each engine.

Each engine must be covered by a valid U.S. Certificate of Conformity and bear a U.S. Emission Control label in English.

Shipments of forklift engines that do not comply with EPA requirements and are destined to the U.S. must meet additional labeling requirements.

The Supplier must include the following verbiage on the label that is affixed to the non-EPA compliant engine.

> "***This engine is never to be offered for sale in the US or Canada. This engine is solely for export from the U.S. and is therefore exempt under 40 CFR § 1068.230 from U.S. emission standards and related requirements."***

The Label must remain on the product for the entire life of the engine. Logisnext will seek reimbursement for fines or penalties if the Supplier fails to properly mark label of goods.

Importer Security Filing (ISF)

To facilitate compliance with the CBP **Importer Security Filing Program (ISF)**, each Supplier is required to provide a copy of the commercial invoice to the customs broker within a **72-hour period** prior to the goods being laden on the vessel in the foreign port for **ocean shipments only.**

Failure to provide complete, accurate and timely filing may result in liquidated damages ranging from $5,000 up to $10,000 maximum fine per violation by CBP.

Labeling and Marking of Product with Country of Origin

The product, related packaging, labeling and other relevant documentation including all related advertisements furnished by or authorized by the Supplier must clearly and properly indicate the correct Country of Origin of the product in accordance with CBP laws and regulations.

Generally, the Country of Origin of a product is the country in which the product exported to Logisnext was manufactured. An exception may apply where further work or materials must be added to an article in another country resulting in a new article signified by a different product name, character and/or use.

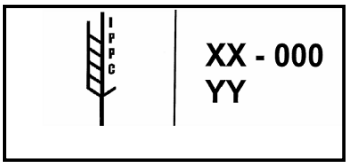
For further guidance as to the marking of Country of Origin on U.S. Imports, go to:
https://www.cbp.gov/document/publications/informed-compliance-publication-marking-country-origin-us-imports

Agricultural Requirements and Wood Packaging Materials Regulations

The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service (APHIS) has revised its import regulations for **Wood Packaging Materials (WPM)**. The regulation restricts the importation of any non-exempt WPM for international trade used to treat or kill harmful insects that may be present. The required WPM markings serve to provide notice that the WPM has received approved treatments.

Logisnext requires the Supplier to comply with International Standards for Phytosanitary Measures No. 15 (ISPM) in the transportation of all products shipped to Logisnext in the U.S.

Sample of acceptable WPM marking



The following wording must accompany the WPM marking and provided for legibility purposes:

- **XX** represents the ISO Country Code
- **000** represents the unique number assigned by the National Plant Protection Organization
- **YY** represents HT for heat treatment or MB for methyl bromide fumigation

For further information on Wood Packaging Material Regulations, go to: **http://www.palletcentral.com** or
http://www.aphis.usda.gov/import_export/plants/plant_imports/wood_packaging materials.shtml
Imports into the U.S. utilizing wooden packaging must be free of bark and pests as well as in accordance with the USDA regulations.

Procedures must be in place to prevent pest infestation on exported products and associated Instruments of International Traffic. The supplier must follow international agricultural pest and contamination requirements. It is critical for the supplier to confirm the absence of pest infestation for a shipment prior to the departure of the goods from the foreign port.

Any shipments containing WPM in violation of applicable laws and regulations may be immediately exported from the U.S. supervision of CBP. In addition, CBP or APHIS may allow removal of the imported merchandise from the non-compliant WPM.

If separation is possible, the importer or party in interest must pre-pay all estimated expenses to be incurred for the services of the CBP and APHIS personnel involved in the separation and re-inspection of the cargo.

If it is determined that it is not feasible to separate the imported merchandise from the violated WPM, the WPM and associated merchandise shall be exported**.**

Logisnext requires written confirmation from the Supplier verifying that Logisnext will be reimbursed for the costs associated with the separation prior to authorizing the action, and the Supplier shall cover any actual and ancillary expenses related thereto.

For most current regulations, go to: http://www.aphis.usda.gov/ppq/swp/

Incoterms

All Logisnext shipments shall be governed pursuant to **INCOTERMS 2020** unless otherwise indicated in the applicable contract. The applicable terms of sale shall be indicated on the commercial invoice.

Customs Brokers

The Supplier must provide the Logisnext designated customs broker with all required documentation *(i.e., Commercial Invoice, etc.)* and any additional information necessary to identify and comply with applicable CBP import laws and regulations. To ensure a smooth transition through CBP and avoid shipment delays, all required documents must be E-mailed to the designated customs broker.

Instruments of International Traffic

Lift vans, cargo vans, shipping tanks, re-usable pallets and certain articles used to ship goods internally are designated by CBP as instruments of international traffic. With certain exceptions, instruments of international traffic may be released without entry or duty payment. Containers fitted to contain a specific product and suitable for long term use and entered with the product for which they were intended are classifiable with the accompanying products.

Customs Trade Partnership Against Terrorism (CTPAT)

Logisnext is a participant in the **Customs Trade Partnership Against Terrorism (CTPAT)** and CTPAT Trade Compliance (formerly known as Importer Self-Assessment) programs**.**

CTPAT is a voluntary government-business initiative to build cooperative relationships that strengthen and improve overall international supply chain and U.S. border security. Through this initiative, CBP is asking businesses to confirm the integrity of their security practices and communicate the security guidelines of their business partners within the supply chain. Under the CTPAT Program, participants receive less scrutiny and inspections of their incoming cargo resulting in fewer cargo delays and detentions.

CTPAT Trade Compliance is a CBP program open to CTPAT participants that allows importers to assess their own compliance with CBP laws and regulations. Under the CTPAT Trade Compliance Program, participants are given the opportunity to assess their own compliance with CBP laws and regulations, rather than undergoing comprehensive CBP audits.

As a CTPAT member, Logisnext must maintain good standing in the CTPAT and CTPAT Trade Compliance Programs, and, thus, it is incumbent upon Suppliers to Logisnext to have adequate security processes and procedures in place to assure the integrity of all cargo shipped to Logisnext.

The following are key security elements that must be observed by Logisnext Suppliers and available for verification by Logisnext:

- Container and Trailer Security Controls
- Physical Security & Access Controls
- Personnel and Visitor Controls
- Physical & Procedural Security *(related to shipping)*
- Information Technology Security
- Financial Soundness
- Capability of meeting Contractual Security Requirements
- Ability to identify and correct Security deficiencies, as needed

Attachment B

CTPAT Security Standards for Suppliers

A. Written Procedures

All suppliers shall maintain written recordkeeping procedures for tracking all products exported to Logisnext from point of origin to point of delivery in the United States. Upon written request by Logisnext, the supplier must produce this written recordkeeping procedure along with any other relevant documentation.

B. Security Procedures

All suppliers shall maintain written security procedures at their manufacturing and/or distribution facilities including:

Physical Security

- Alarm System
- Building Structure
- Fencing
- Gate and Gate Houses Limited Access
- Information Technology Security
- Locking Devices and Key Controls Lighting
- Parking
- Video Surveillance Cameras

Personnel Security

- Personnel Background Checks
- Personnel Termination Procedures
- Pre-Employment Verification

Procedural Security

- Container Security
- Container Inspection
- Container Seals
- Container Storage
- Physical Access Controls
- Employee Identification System
- Visitor Identification
- Procedures for Challenging and Removing Unauthorized Persons
- Documentation Processing
- Manifesting Procedures
- Shipping and Receiving
- Cargo Discrepancies
- Security Training and Threat Awareness

C. Facility Visits

All suppliers will be requested to grant Logisnext or a designated representative the right to visit their facilities to perform an assessment of their compliance with CTPAT standards. Logisnext will make such requests in writing and will coordinate the visit so as not to create an unreasonable burden on the supplier.

CBP officials may accompany Logisnext on such facility visits. CBP routinely selects Logisnext non-U.S. supplier facilities to visit each year.

D. Corrective Action

Logisnext will advise relevant suppliers in writing of any corrective action required to assure compliance with the CTPAT program. Logisnext reserves the right to terminate its business relationship with any company which fails to comply with the CTPAT standards.

Attachment C

Factory Security Certification Standards

General Standards

1. Maintain a written security policy.
2. Distribute written security policy to all personnel.
3. Conduct security awareness training for all personnel.
4. Provide ongoing security awareness training for all personnel.

Physical Security for Facilities Containing Export Products

1. Construct and maintain facilities in a way that will resist unlawful entry. Examples of such measures are: solid walls/ceilings, perimeter fences, operational locks and/or alarms on external and internal doors, windows, gates and fences.
2. Monitor and secure all loading dock and cargo areas.
3. Maintain operational locking devices for all external and internal doors, windows, gates and fences.
4. Maintain operational lighting inside and outside the facility; including parking areas.
5. Maintain a parking area for private vehicles separate from the shipping/loading dock and cargo areas.
6. Designate an employee devoted to security compliance.
7. Establish an internal/external communications system at product facilities for internal security personnel and/or local law enforcement.
8. Conduct a complete background check for all security personnel.
9. Conduct periodic training for all security personnel.
10. If the facilities depend on a visible electronic security system (for example; working security CCTV cameras, electronic motion detectors or automatic alarms) confirm the system covers all critical areas. For example: entry/exit doors as well as loading, receiving and storage areas.
11. If the facilities operate a visible electronic security system, the supplier should maintain documented records of service work performed and periodic quality control testing of the system.
12. If facilities operate security cameras, recorded video media shall be maintained in a secure area with limited access, for at least 30 days.
13. Provide for segregation and marking of international, domestic, high-value, and dangerous goods categories of cargo within the facility by means of a restricted-access safe, cage or otherwise fenced-in area.
14. Provide for the proper storage of empty and loaded containers, trailers, railcars or other implements of international shipping to prevent unauthorized access.

Control of Access to Facilities

1. Implement a written procedure for limited access to production, shipping, loading dock and cargo areas.
2. Require photo identification of all employees, visitors, and service providers.
3. Provide employees with photo identification badges or other visible means of identification.
4. Establish a written policy requiring employees to show a photo identification / badge before being admitted to the facilities.
5. Restrict employees from taking personal items into the production area.
6. Require all visitors to sign a log upon entry/exit of the facilities.
7. Require all visitors to be issued temporary visitor badges or other visible means of identification.
8. Establish written procedures for challenging or confronting unauthorized or unidentified persons.
9. Require all visitors desiring access to secured areas be accompanied by a company representative at all times.
10. Maintain key or entry code access to the facilities.
11. Replace keys or change access codes periodically.
12. Post signs indicating the mandatory requirements for access to certain areas.
13. If the facilities have a card access system, maintain records of daily transactions in a secure area with limited access by authorized personnel.
14. If facilities have a card access system, maintain a documented procedure to service and test the system; limited access to such records is required.

Procedural Security

1. Maintain a written Security Policy (a system, procedure, or manual) covering procedural security; either a distinct document or part of a quality or procedures manual.

2. Designate a manager or group responsible for security.
3. Designate a security officer manager to supervise the introduction and removal of cargo.
4. Implement written procedures for monitoring and documenting the timely movement of incoming and outgoing goods.
5. Implement written procedures for properly marking, weighing, counting and documenting products.
6. Implement written procedures for detecting and reporting shortages or overages.
7. Restrict access to the loading area during loading; access should be restricted to authorized employees only.
8. Subject outgoing trucks, trailers and containers to random inspection for content verification.
9. Subject incoming trucks, trailers and containers to random inspection to verify contents prior to granting access to restricted areas.
10. Maintain a log for outbound shipments specifically designed to record outbound shipment information at the time of loading. Information captured should include carrier, driver name, container/trailer number, seal number (if applicable), destination, purchase order, item number, manifest quantity, date loaded, time loaded and security guard name.
11. Retain copies of the completed log for outbound shipments at the facilities. Such records must be made available upon request and should be accessed by authorized personnel only.
12. Lock and secure empty and loaded containers. Each container should be checked daily for tampering.
13. Inspect all inbound and outbound containers for tampering prior to receipt or unloading.
14. Establish written procedures to protect seal integrity of outbound containers between the factory and the in-gate at the ocean terminal or approved container yard.
15. Verify seals on inbound and outbound containers match the corresponding shipping documents prior to receipt or unloading.
16. Where applicable, the facility should have written procedures for affixing, replacing, recording, tracking and verifying seals on containers, trailers and railcars.
17. Establish written procedures for the distribution of container seals to authorized employees only.
18. Conduct random, documented internal security assessments which should be maintained for review.
19. Maintain an updated file of “corrective action” procedures for security issues detected during the security assessment.
20. Establish a written procedure for security personnel or other Supplier employees to report any suspicious activity.
21. Establish written procedures for notifying local law enforcement and other authorities (e.g. customs authorities) in cases where anomalies or illegal activities are detected, or suspected (including compromised seals where applicable).
22. Institute a supplier certification program/process of some type to screen raw materials suppliers.
23. Properly supervise authorized subcontractors to ensure compliance with security protocols.

Personnel

1. Document security and the formal education level, qualifications, and experience of staff responsible for the supplier.
2. Conduct comprehensive employment interviews and background screening of prospective employees and follow-up with periodic background checks post-employment.
3. Establish documented procedures for terminating employees to ensure the return of security instruments such as access cards, identification cards, and keys.
4. Implement a procedure for the reporting of potential security issues observed by employees.
5. Where applicable, the company should assure that only designated employees are approved to distribute container seals.
6. The company’s management and appropriate personnel should be aware of and maintain compliance with the U.S. Bureau of Customs and Border Protection (“CBP”) 24-hour rule. The rule requires a complete cargo manifest be presented to CBP at least 24 hours prior to cargo loading if that vessel is calling a US port direct.

Security Education and Training

1. Maintain a documented security education and awareness program.
2. Designate a management representative to be responsible for the education and training awareness program.
3. Conduct periodic verbal and written security awareness training of employees.
4. Verify security awareness training educates employees in acceptable and unacceptable behavior including related disciplinary consequences.
5. Provide a security program for employees communicating a clear explanation of how different security procedures apply. For example, explain the correct channels or means to report suspicious behavior and procedures for gaining entrance to secure areas.
6. Employee training should include discussions on:

a. the importance of security measures
b. the prevention of unauthorized access to secure areas
c. how to prevent and recognize product tampering
d. recognizing and reporting illegal conduct and activities by other employees

7. Encourage and promote employee reporting of any potential security issues they may observe.
8. Conduct periodic employee meetings where security issues are discussed.
9. Develop a method to inform employees on a timely basis of potential security problems (e.g. bulletin postings or announcements).

Threat Awareness

1. Maintain a documented threat awareness program to be maintained by security personnel.

2. Ensure the threat awareness program includes routine briefings/postings about smuggling trends, seizures and information on terrorist threats relevant to the facility's individual supply chain and location.

Information Technology Security

1. Document the Supplier's internal controls for securing information technology, such as firewalls, virus protection, passwords, and levels of restricted access.
2. Provide for periodic password changes.

Attachment D

Container Search and Seal Integrity Program

Container Search Program Procedures

The following steps are to be taken to ensure the integrity of the shipment and shipping container prior to the transportation document being signed by Logisnext receiving personnel.

1. Container Tracking: Container arrivals should be scheduled with Logisnext prior to their arrival at the Logisnext facility.

2. Inspection of all Vehicles: All vehicles attempting to gain access to shipping and receiving areas must be inspected.

3. Container Inspection: All containers destined for delivery to Logisnext arriving at the supplier facility must be inspected at earliest practicable point outside the facility.

4. Seal Inspection: Seal inspection/verification must be completed prior to giving a container access to the facility.

5. All containers arriving at the facility must have:
   a. Documentation verified
   b. Seven Point Container Inspection
   c. Seal Number Integrity verified

Seal Integrity Program

Seals must be verified at the factory, port of origin, port of arrival, distribution center entrance, and Receiving Dock. Seal used must be a high security seal on all containers, ISO17712:2010 standard or higher.

The VVTT seal verification and inspection process should be used before seals are put in place and closed:

V---View seal and container locking mechanism.
V---Verify seal number for accuracy. Compare with shipping documents and look for alterations.
Confirm the type of seal used is normal for the shipping line.
T---Tug on seal to make sure it is affixed properly.
T---Twist and Turn seal to make sure it does not unscrew.

After the container and seal(s) have passed inspection, the container may be opened. Seals should be kept for investigative purposes.

After the container is opened, a visual inspection of the inside of the container should be conducted. If contraband is discovered, immediately close the container doors and contact a Factory Supervisor and Freight Forwarder.

Container Inspection Checklist

The Container Inspection Checklist (CIC) included as Annex 1 of this document should be employed for all empty containers entering the premises. The supplier may adopt an equivalent document, but all information contained on the CIC must be included on any adopted document. Prior to the loading of product leaving the origin facility destined for Logisnext, the checklist shall be signed by a representative of the supplier and maintained with the shipping file for at least one year. The checklist is subject to review by Logisnext or designated representatives as well as by CBP officials.

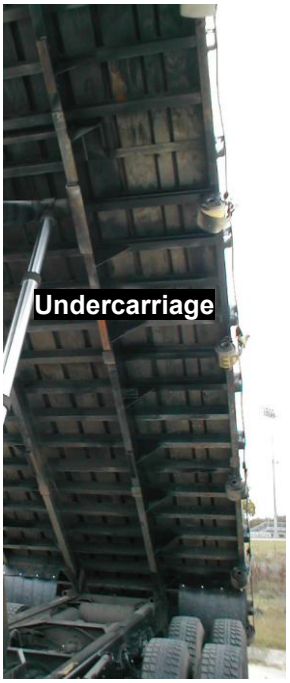
Container Inspection Incident Response

A Container Inspection Incident Response (CIIR) form included as Annex 2 of this document should be used to report any incidents. Please note that all areas listed on the incident report should be provided on any alternate form used in place of the CIIR. An incident report must be completed: (i) when an unacceptable condition or unmanifested material is found during a container inspection and the container is not approved for stuffing, and/or (ii) upon receipt of a loaded container, to verify the integrity of the seals, to confirm record of any changes in the structure of the container or to record whether any unmanifested materials are discovered with the shipment. Upon completion of an incident report, the written report should be signed by a designated representative of the company and maintained with the shipping file for at least one year. Incident reports are also subject to review by Logisnext or its designated representatives as well as by CBP officials.

Annex 1

Container Inspection Checklist

1. Undercarriage
   - Inspect prior to entering facility
   - Check support beams – all should be visible
2. Outside/Inside Doors
   - Check all locking mechanisms
   - Color of container should be uniform
   - Plates or repairs to the container must look professional & same color as container
3. Right Side
   - Repairs to the walls or wall beams on the inside of the container must be visible on the outside
   - Use tool to tap side walls – Listen for hollow sound
4. Left Side
   - Repairs to the walls or wall beams on the inside of the container must be visible on the outside
   - Use a tool to tap side walls – Listen for hollow sound
5. Front Wall
   - Blocks and vents must be visible
   - Repairs to the walls or wall beams on the inside of the container must be visible on the outside
   - Use a tool to tap front wall – Listen for hollow sound
   - Range finder/measuring tape can be utilized to confirm container length (If there is a false wall, dimensions of the container will be shorter)
6. Ceiling/Roof
   - Certain height from floor to ceiling.
   - Blocks and vents must be visible
   - Repairs to ceiling on inside of container should be visible from the outside
   - Use a tool to tap ceiling – Listen for hollow sound
7. Floor
   - Should be certain height from ceiling
   - Look for unusual repairs
   - Use a tool to tap for false floor



Left Side

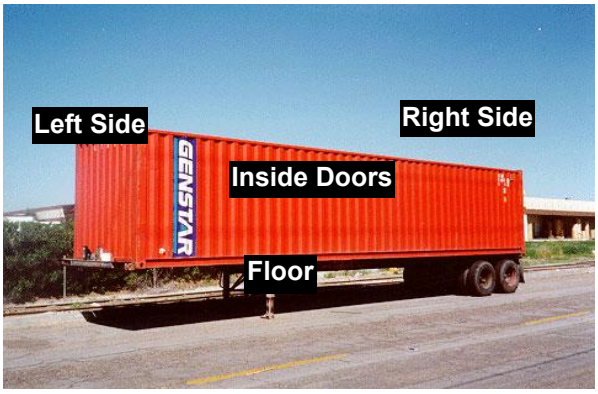
Front Wall Undercarriage

Ceiling/Roof

Left Side Right Side

Front Wall

Floor



Annex 2

Container Inspection Incident Response

Logisnext Americas Inc. Container Inspection Incident Response

To be completed and filed locally in the event that an unacceptable condition or unmanifested material is found during a container inspection and the container is not approved for stuffing. This form is to be utilized upon receipt of a loaded container to verify the integrity of the seals and to confirm and record any changes in the structure of the container or to record if any unmanifested materials are discovered with the shipment.

DATE:	**CONTAINER NUMBER:**
SHIPPING MANIFEST NUMBER:	**CARRIER SEAL NUMBER:**
CABLE SEAL NUMBER:	**OTHER SEAL NUMBER:**
INSPECTOR NAME:	**INSPECTOR SIGNATURE:**

TYPE OF INCIDENT AND RESPONSE

Type of Incident and Recommended Response	Actual Response and Resolution
Evidence of Container Tampering (e.g., New Paint or Recent Weld Repair) **Recommended Response:** A more detailed inspection of the container looking for false wall including measuring the container to verify there is no false compartment prior to loading.	
Unmanifested Material (e.g., People, Personnel, Weapons of Mass Destruction, Drugs or Contraband discovered) **Recommended Response: I**f there appears to be a weapon of mass destruction, other unsafe material or contraband in the container, call local law enforcement or a hazardous material response team, notify senior company management and senior management will notify the local authorities and Customs and await further instructions. If there is an apparent immediate threat, evacuate the immediate area.	
Not Watertight / Unsafe Structure **Recommended Response:** If the container appears unsafe or not watertight, the container should not be used, but tagged for repair.	
Locking Mechanisms Broken **Recommended Response:** If the container cannot be properly sealed and secured, the container should not be used. Tag the container for repair.	
Seal Numbers Not Matched **Recommended Response:** If the seal attached to the container does not match the shipper's documents or the ASN, an investigation and report to the U.S. Customs and Border Protection ("CBP") may be warranted. Documents should be reviewed to ascertain if the new seals are the result of a CBP inspection or other custodians may have added/changed the seals. If there is no resolution for the new seals, further investigation and reports may be warranted. This information will be reviewed by the Logisnext Trade Compliance Manager and a determination will be made as to whether an investigation and report to CBP are warranted.	