CONTAINER INSPECTION SOP

1. Principle

Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers has a commitment with respect to C-TPAT, to ensure that shipping containers are secure.

2. Objective

To ensure that all shipping containers have been properly inspected for hidden compartments.

3. Definition

C-TPAT stands for Customs-Trade Partnership Against Terrorism, a supply chain security program sponsored by U.S. Customs & Border Protection (CBP).

Container refers to a shipping container or a shipping trailer.

4. Responsibilities

Senior management at the locations where containers are loaded or unloaded are responsible for ensuring that all containers are inspected per the items noted in this SOP.

5. CONTAINER INSPECTION

5.1 Before a container is loaded (shipping) or after the container is unloaded (receiving) the warehouse staff must conduct a 7- point container inspection using a Container Inspection Checklist. NOTE: If you have received a container inspection checklist (from the loading location) that was completed prior to the container being loaded, please use that checklist to conduct your inspection (make checkmarks, initial, date adjacent to information already on the form for the purpose of verification of the information).

5.2 The inspection is primarily focused on searching for any manipulations, hidden compartments, false walls, floors or ceilings, faulty door hinges and faulty locking mechanisms.

5.3 The inspection should always be performed when the container is empty, because access to the interior is required.

5.4 If any anomalies are discovered during the container inspection your company's senior management must be notified immediately.

5.5 The senior management should ensure that an investigation of the anomaly takes place.

5.6 If the senior management investigation determines that the container integrity has not been violated it should be so noted on the container inspection checklist and the container will be considered normal and ready for continued handling.

5.7 If the senior management investigation determines that the container integrity has been violated or manipulated, the senior management must immediately notify our company as

well as local law enforcement and the appropriate government officials in your area.

5.8 If a container should arrive with a broken seal the warehouse staff must immediately report any such incident to the senior management of your company.

5.9 The inspection checklist must be kept on file for at least 6 months.

5.10 Completed container inspection checklists should be considered a “normal” part of a shipment file and must always be transmitted to our company or to the location in the U.S. where the cargo will be unloaded along with other shipping documents.

6. Procedures

6.1 Container integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At the point of loading, procedures must be in place to properly seal and maintain the integrity of shipping containers. A high security seal must be affixed to all loaded C-TPAT importer containers bound for the United States. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals. The following seven-point inspection process is recommended for all containers:

6.1.1 Check the front wall for integrity or manipulation

6.1.2 Check the left side for integrity or manipulation

6.1.3 Check the right side for integrity or manipulation

6.1.4 Check the floor for integrity or manipulation

6.1.5 Check the ceiling/roof for integrity or manipulation

6.1.6 Check the doors (both inside and outside) for integrity or manipulation

6.1.7 Check the outside undercarriage for integrity or manipulation

7. CONTAINER STORAGE

7.1 All business partners are required to store containers in a secure area to prevent unauthorized access and/or manipulation. Our company requires its international business partners to have written procedures in place for reporting and neutralizing unauthorized entry into containers or container storage areas.

Your company must also notify our company as well as local law enforcement and the appropriate government authorities in the event that a breach of a stored container or a breach of a container storage area has occurred.

SEE CONTAINER INSPECTION CHECKLIST (NEXT PAGE)

8-POINT CONTAINER INSPECTION CHECKLIST

OCEAN CONTAINER ☐ RAIL CONTAINER ☐ OTR CONTAINER ☐ OTHER ☐

CONTAINER IDENTIFICATION NUMBER:_____

HIGH SECURITY SEAL NUMBER: _____

DATE OF INSPECTION:_____CARRIER: _____

IF ANY EVIDENCE OF MANIPULATION, TAMPERING OR INTEGRITY BREACH IS OVERED PLEASE CONTACT U.S. CUSTOMS OR THE PROPER FOREIGN AUTHORITY.

PLEASE CHECK ALL CONTAINERS FOR INTEGRITY AND/OR MANIPULATION AND CHECK THE APPROPRIATE BOX.

	Signs of Tampering	Signs of Integrity Breach	Condition Normal
1. Check the inside of the front wall	☐	☐	☐
2. Check the inside and outside of the left wall	☐	☐	☐
3. Check the inside and outside of the right wall	☐	☐	☐
4. Check the floor	☐	☐	☐
5. Check the ceiling and roof	☐	☐	☐
6. Check both doors inside and outside	☐	☐	☐
7. Check the outside undercarriage	☐	☐	☐
8. Check the inside for cleanliness (dirt, debris, weeds, insects, animal droppings)	☐	☐	☐

COMMENTS:

Please report container tampering or manipulation or to Name & E-Mail

Phytosanitary SOP

1.0 Wood Packaging Materials
Suppliers/shippers must ensure all Wood Packaging Materials (WPM) comply with US and international phytosanitary standards as follows:

1.1 All WPM must be properly marked to indicate it has been either heat treated or treated with methyl bromide,
1.2 All WPM must contain the internationally recognized IPPC mark which certifies treatment.
1.3 All WPM must also be free of timber pests
1.4 All WPM must be very clean, and cannot have any signs of weeds or seeds on them (free from organic plant life).
1.5 Wood Packaging Material (WPM) is defined as wood or wood products (excluding paper products, such as corrugated paper cartons) used in supporting, protecting or carrying a commodity. Wood packaging materials include:
- 1.5.1 Pallets
- 1.5.2 Crates
- 1.5.3 Boxes
- 1.5.4 Packing blocks
- 1.5.5 Drums
- 1.5.6 Cases
- 1.5.7 Skids
- 1.5.8 Pieces of wood used to support or brace cargo

2.0 Identification of Acceptable Recycled Containers.

2.1 Depending on customer requirements Client uses recycled containers, cartons and certified wood pallets.
2.2 All packaging used for export products is inspected prior to use.
2.3 The production staff must clean and verify the condition of all packaging prior to use.
2.4 All wood pallets purchased by Client must be certified. The delivery includes a certificate and corresponding documentation from the supplier.
2.5 All wood pallets purchased by supplier/shipper must comply with the guidelines set forth in this SOP. A certificate and corresponding documentation from the packaging supplier must be kept on file and available for verification by Client (upon request).

3.0 Returnable Containers

3.1 Returnable containers are stored and segregated inside the facility and remain under the supervision of warehouse staff.
3.2 Returnable containers may not re-used until they are cleaned and inspected.

4.0 Shipping Containers

4.1 Shipping containers and wood must be inspected using an 8-point inspection checklist (see checklist on next page). The following points must be inspected and verified.

- Container & pallet cleanliness (dirt, debris, weeds, seeds, insects, animal droppings)

- Underside of Trailer
- Left Wall
- Right Wall
- Front Wall
- Floor
- Ceiling
- Inside and Outside Door / Hinges

CONTAINER SEALING SOP

4. Principle

Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers must be committed to ensuring that shipping containers are properly sealed.

5. Objective

To ensure that all shipping containers have been properly sealed using a single-use high security seal.

6. Definition

C-TPAT stands for Customs-Trade Partnership Against Terrorism, a supply chain security program sponsored by U.S. Customs & Border Protection (CBP).

SEAL refers to a high security seal that is used to secure a shipping container. The high security seals have unique numbers and are tamper-evident. The seals are tested in a laboratory and must meet or exceed PAS ISO 17712:2013 (see U.S. Customs bulletin: https://www.cbp.gov/document/bulletins/c-tpat-bulletin-compliance-isos-17712-standards-standards-high-security-seals

4. Responsibilities

Your company's senior management is responsible for ensuring that all containers used in the transportation of international cargo are in compliance with this procedure.

5. Procedures

5.1 Empty containers arriving at your facility may not be empty, or may have been altered to add hidden compartments. Always perform and document a 7-point container inspection before loading and sealing a container. NOTE: See Container Inspection SOP.

5.2 High security seals must be controlled by management.

5.2.1 The high security seals must be kept in a secure location.
5.2.2 Only designated employees should be given access to the seals.
5.2.3 Only designated, authorized employees should be allowed to distribute and affix container seals for integrity purposes.
5.2.4 Cut seals must not be discarded into the general company trash because criminals or terrorists may try to reuse the cut seals for nefarious purposes.
5.2.5 Cut seals must be stored securely, in a secure location, until such time as they can be disposed of in a secure manner.

5.3 Unauthorized employees should never have access to or be allowed to handle, distribute or affix container seals.

5.4 Only high security seals that meet or exceed exceed the current PAS/ ISO 17712:2013 standards for high security seals are acceptable for use on containers bound for the US.

5.5 Seals must be affixed to the right door of the container on the hasp that has the welded rivet. This practice raises the level of security of the shipment.

5.6 After the seal is affixed to the container, an authorized employee must make sure that the seal is secure by pulling down on it.

6. Seal Verification and Inspection

6.1 View the seal & container locking mechanisms. Excessive damage to the seal or locking mechanisms must be reported to a supervisor before opening the container.
6.2 Watch for and report different brands of seals attached together.
6.3 Watch for and report loose bolts and hasps.
6.4 Verify the seal number for accuracy. Compare the seal number with the seal number indicated on the shipping documents. Look for alterations to the seal numbers.
6.5 Watch for and report incorrectly manifested seal numbers.
6.6 Watch and report a seal brand that is not normally used by your company.
6.7 Watch for and report original seal numbers that have been sanded or filed off.
6.8 Tug on the seal to make sure it is affixed properly. Seals that come apart must be reported to a supervisor. Human error might cause this to happen, or the container might have contraband inside.
6.9 Watch for and report bent seal stems.
6.10 Watch for and report seals that do not lock properly.
6.11 Watch for and report glue inside the locking mechanism that causes the seal to not lock properly.
6.12 Twist & turn the seal to make sure it does not come off. Altered seals that have been threaded so that they can be unscrewed are not acceptable. These altered seals are reusable throughout the supply chain, allowing persons to unseal and reseal the container after adding contraband or removing merchandise
6.13 Twist counter-clockwise to see if the seal can unscrew. Report seals that are able to be unscrewed.

CONVEYANCE SECURITY SOP

1. Principle

Your company must have a commitment to ensure that conveyances are secure.

2. Objective

The purpose of this SOP is to ensure that all conveyances (tractor/trailer/container) that are involved in the international supply chain have been properly inspected and that appropriate measures are in place to ensure secure storage, tracking and monitoring.

3. Definition

C-TPAT stands for Customs-Trade Partnership Against Terrorism, a supply chain security program sponsored by U.S. Customs & Border Protection (CBP).

Conveyance refers to a truck or tractor joined together with a shipping container or a shipping trailer.

4. Responsibilities

Company management is responsible for ensuring that all trucking companies have appropriate conveyance inspection, tracking and monitoring procedures in place.

5.0 Procedures

5.1 Trucking company management and drivers are responsible for ensuring conveyance (tractor & trailer/container) integrity. The conveyance operators and owners must have adequate security measures in place to protect against the introduction of unauthorized material and/or persons.
5.2 Drivers or warehouse staff are required to conduct conveyance inspections that are systematic. These inspections must be completed upon entering and departing from the truck yard and at the last point of loading prior to reaching the port of departure.
5.3 Using a checklist, drivers must inspect their conveyances for natural or hidden compartments.
5.4 The following systematic practices should be considered when conducting training on conveyances. Highway carriers must visually inspect all empty trailers/containers, to include the interior of the trailer/container, at the truck yard and at the point of loading, if possible.

The following 18- point inspection process is recommended for all tractors and trailers/containers:

Tractors:
- Bumper/tires/rims
- Doors/tool compartments
- Battery box
- Air breather
- Fuel tanks
- Interior cab, compartments/sleeper
- Faring/roof

Trailers:
- Fifth wheel area - check natural compartment/skid plate
- Exterior - front/sides
- Rear - bumper/doors
- Front wall
- Left side
- Right side
- Floor
- Ceiling/Roof
- Inside/outside doors
- Outside/Undercarriage
- Security Seals
- Cleanliness

5.5 To counter internal conspiracies, trucking company supervisory personnel or a security manager, held accountable to senior management for security, should search the conveyance after the driver has conducted a search. These searches should be random documented and based on risk.
5.6 Conveyance providers are required to pay special attention to inspections for those shipments that are deemed to be high risk. The factors that make a shipment potentially high risk are things like a) unknown shipper, b) new shipper, c) country of origin, d) volume, etc.

6.0 Storage

6.1 For all trailers/containers, integrity must be maintained, to protect against the introduction of unauthorized material and/or persons.
6.2 Trailers & Containers must be stored in a secure area to prevent unauthorized access and/or manipulation. Immediately report unauthorized entry into trailers/containers, tractors or storage areas to U.S. customs or the appropriate foreign authority and take appropriate measures to neutralize the situation.
6.3 Trailers must be kept locked during storage and reinspected before beginning post-storage use.

7.0 Tracking and Monitoring

7.1 Trucking companies must ensure that conveyance and trailer integrity is maintained while the conveyance is in route transporting cargo to or from the U.S. border by requiring their business

partners to utilize a tracking and monitoring activity log, GPS and telephone communications.
7.2 When driver logs are utilized, they are required to reflect that trailer integrity was verified.
7.3 Predetermined routes should be identified, and random route checks along with documenting and verifying the length of time between the loading point/trailer pickup and the delivery destinations.
7.4 Drivers are required to notify the dispatcher of any route delays due to weather, traffic and/or rerouting.
7.5 During government or other physical inspections on the conveyance as required by law, drivers must report and document any anomalies or unusual structural modifications found on the conveyance.

8.0 Container/Trailer Seals

8.1 A high security seal must be affixed to all loaded containers & trailers bound for the U.S.
8.2 All seals must meet or exceed the current ISO PAS 17712:2013 standards for high security seals.
8.3 All suppliers are required to keep high security seal lab certificates on file for a minimum of 6 months.
8.4 Business Partners must have control the storage & distribution of high security seals. Only certain employees should be allowed access to high security seals and the distribution should be documented and controlled by company management.
8.5 Based on risk, a high security barrier bolt seal may be applied to the door handle and/or a cable seal must be applied to the two vertical bars on the trailer/container doors.
8.6 Please see Security Seals SOP section of this document.
8.7 Business partners must ensure that drivers are briefed on the high security seal procedures and must also insure (through testing, or other means) that the drivers understand the procedures. Business partners should keep driver training and testing documentation on file for at least 1 year.

9.0 Less-Than-Truck-Load LTL - Padlocks

9.1 LTL carriers must use a high security padlock or similarly appropriate locking device when picking up local freight in an international LTL environment.
LTL carriers must ensure strict controls to limit the access to keys or combinations that can open these padlocks.

SEE CONTAINER INSPECTION CHECKLIST (NEXT PAGE)

CONVEYANCE/TRACTOR SECURITY CHECKLIST

TRACTOR/CONVEYANCE IDENTIFICATION NUMBER: _____

TRACTOR/CONVEYANCE CHECKED BY: _____

DATE OF INSPECTION: _____CARRIER: _____

PLEASE CHECK ALL CONTAINERS FOR INTEGRITY AND/OR MANIPULATION AND CHECK THE APPROPRIATE BOX.

	Condition Normal	Signs of Manipulation or Tampering	Signs of Integrity Breach
1. Check Bumpers/Tires/Rims	☐	☐	☐
2. Check Doors/Tool Compartments	☐	☐	☐
3. Check Battery Box	☐	☐	☐
4. Check Air Breather	☐	☐	☐
5. Check Fuel Tanks	☐	☐	☐
6. Check Interior Cab, Compartments/Sleeper	☐	☐	☐
7. Check Faring/Roof	☐	☐	☐
8. Check 5th Wheel Area – Natural Compartment/Skid Plate	☐	☐	☐
9. Trailer - Check Exterior – Front/Sides	☐	☐	☐
10. Trailer – Check rear – Bumpers/Doors	☐	☐	☐
11. Trailer – Check front wall	☐	☐	☐
12. Trailer – Check left side	☐	☐	☐
13. Trailer – Check right side	☐	☐	☐
14. Trailer – Check floor	☐	☐	☐
15. Trailer – Check Ceiling/Roof	☐	☐	☐
16. Trailer – Check inside/outside doors	☐	☐	☐
17. Trailer – Check outside / undercarriage	☐	☐	☐
18. Trailer – Security seal intact	☐	☐	☐
19. Check the inside for cleanliness (dirt, debris, insects, animal droppings)	☐	☐	☐

COMMENTS:

PERSONNEL SECURITY SOP

1. Principle

Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers must have a commitment to properly screen potential employees and to ensure that employees are trained in these supply chain security procedures.

2. Objective

To ensure that Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers have proper employee screening and hiring practices in place as well as post-employment procedures and termination procedures.

3. Definition

C-TPAT stands for Customs-Trade Partnership Against Terrorism, a supply chain security program sponsored by U.S. Customs & Border Protection (CBP).

4.0 Responsibilities

Your company's senior management is responsible for ensuring that all C-TPAT employee screening, hiring and termination procedures are implemented and followed.

5.0 Procedures

5.1 All new employees must be introduced to the overall principals and objectives of C-TPAT during the hiring process.

5.2 Business partners must communicate to its employees the importance of supply chain security and maintaining chain of custody.

5.3 All staff must be made aware of the C-TPAT supply chain security measures and are instructed to notify senior management immediately upon discovery of any illegal or suspicious activities related to security.

5.4 Business partner's employees are required to attend security training that focuses on threat awareness, recognizing internal conspiracies and how to identify and report suspicious behaviors and activities.

5.5 Employee training must be documented. Training records must be retained for a minimum of 5 years.

5.6 Business partners must maintain a list of all employees (domestic & foreign), which includes their name, social security number (U.S. citizens only) or national ID number, date of birth and position held. This list must be made available to U.S. Customs upon written request, to the extent permitted by law.

6.0 PERSONNEL SECURITY / PRE-EMPLOYMENT VERIFICATON

6.1 Consistent with local laws & regulations, background checks and investigations are conducted for prospective employees. Once employed, periodic checks and reinvestigations are performed based on cause, and/or the sensitivity of the employee's position.

6.2 Your company's senior management is responsible for screening all applicants for permanent positions and must conduct the following required verifications:

6.2.1 Verification of all employment hiring documents for completeness and accuracy.

6.2.2 Employment history verification - reference checks.

6.2.3 Background check including 7-year criminal history (or the best available alternative if local laws prevent criminal history background checks).

6.3 Your employees are responsible for following the policies and procedures set forth in this security procedure and must be subject to disciplinary action, up to and including termination for failure to do so.

6.4 Business partners must maintain individual employee files, with a cover sheet (i.e. checklist) of the data contained within (notes, copy of photo ID, training received, testing, etc.).

6.5 Business partners must maintain a list of company property that has been issued to employees. When an employee's employment is terminated the list must be used to ensure that all company property has been returned.

7.0 PERSONNEL SECURITY / POST-EMPLOYMENT VERIFICATON

7.1 Post-employment investigations must be conducted when necessary by business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers or their assigned agent.

7.2 Business partners must reserve the right to conduct post-employment investigations based on cause.

7.3 Should your company's management be informed of or suspect that an employee has provided false information during the hiring process a new investigation must be conducted to verify the information and take the appropriate action as necessary.

8.0 PERSONNEL SECURITY / EMPLOYEE TERMINATION

8.1 Upon termination of an employee, an issued company property checklist must be used to ensure that the individual has returned all company property, building access codes, key cards and keys.

8.2 All automated system passwords and access codes for the terminated employee must be disabled and removed from the system.

8.3 All systems passwords and data access for the terminated employee must be terminated.

FACILITIES & PHYSICAL ACCESS SOP

1.Principle

Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers must have a commitment to ensure proper security measures are in place in each of its facilities.

2.Objective

To ensure that business partner's facilities are secure environments for staff members and to ensure that the premises and the employees are protected from threats.

3.Definition

C-TPAT stands for Customs-Trade Partnership Against Terrorism, a supply chain security program sponsored by U.S. Customs & Border Protection (CBP).

4.0 Responsibilities

Your company's senior management is responsible for ensuring that all facilities are secure and that the security items noted in this SOP are implemented and maintained.

5.0 Procedures

5.1 Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers must control access to its offices to prevent unauthorized access to the facility and to protect company property and employees.

5.2 Employees must not be provided office keys unless approved by management.

6.0 VISITOR CONTROLS

6.1 Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers must control visitor access to its offices to prevent unauthorized access.

6.2 All visitors must a visitor's log.

6.3 Unknown visitors must present government-issued photo identification.

6.4 Visitors must be issued a visitor badge, which the visitor must wear at all times while on the premises.

6.5 The visitor badge must be numbered. The badge number must be noted adjacent to the visitor's name and signature on the visitor log. This will help to determine who has possession of a missing visitor badge so that its return can be brought about.

6.6 If disposable visitor badges are used, the issued badge must have the current date written on it to prevent reuse on another day.

6.7 Visitors must be escorted by a staff member at all times.

6.8 Visitor must return their badges upon departure.

7.0 DELIVERIES AND CONTROL OF SUSPICIOUS MAIL AND PACKAGES

7.1 Assigned staff should use the following guidelines. Staff shall check for the following:

- 7.1.1 Mailed from a foreign country
- 7.1.2 Fictitious or no return address
- 7.1.3 Strange odor
- 7.1.4 Protruding wires
- 7.1.5 Excessive postage
- 7.1.6 Misspelled words
- 7.1.7 Addressed to a business title only (i.e. President)
- 7.1.8 Rigid or bulky
- 7.1.9 Badly typed or written
- 7.1.10 Special endorsements
- 7.1.11 Lopsided or uneven
- 7.1.12 Oily stains, discoloration or crystal on wrapping
- 7.1.13 Emitting noise
- 7.1.14 Is leaking

7.2 The contents of a letter or package may cause concern if:

- 7.2.1 There is a powder or liquid
- 7.2.2 It contains a threatening note
- 7.2.3 It contains an object that you did not expect to receive or cannot identify

7.3 If after reviewing received letters and packages, staff is concerned that the package is suspicious, they should follow the procedures listed below: Do not open the letter or package

7.3.1 Leave the letter or package where it is
7.3.2 Remove clothing that may have gotten powder or liquid on it and seal it in a plastic bag
7.3.3 Wash your hands or shower with soap and water
7.3.4 Get everyone out of the room and close the door
7.3.5 Call 911 or the local emergency number
7.3.6 If applicable, alert the Supervisor.
7.3.7 Wait in a safe place until the authorities arrive
7.3.8

8.0 CHALLENGING AND REMOVING UNAUTHORIZED PERSONS

8.1 If a visitor to your facility is suspected of being unauthorized, employees should be instructed not to approach or confront the person and to immediately notify a supervisor or manager.
8.2 Your company's supervisors or managers are responsible for approaching the unauthorized person and asking him to leave.
8.3 If the unauthorized person will not leave when requested, your company's supervisors, managers, security, or upper management must call the local police department.
8.4 If an unauthorized person acts in a threatening manner any employee should immediately call the designated emergency response telephone number.

9.0 CONTROL OF COMPANY PROPERTY

9.1 The senior management of Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers must approve the issuance of all company property, including keys, credit cards, cell phones & laptops.
9.2 Your company must maintain a list of all keys that have been issued.
9.3 A list of company-owned property that has been issued to employees must be kept on file.
9.4 Your employees are required to return all company-issued property upon termination of their employment, whether termination was initiated by the company or by the employee.
9.5 Upon the termination of an employee who has been in possession of a key to the premises, your company's senior management must assess the risk exposure and take appropriate action, up to and including having the locks changed.
9.6 Employees are required to notify your company's senior management immediately upon discovery of lost or missing company-owned property.
9.7 Your company's senior management or upper management will conduct an investigation of lost or missing company property to determine the risk exposure resulting from the missing property and must take appropriate action.
9.8 In the case of a lost key to the premises, your company's senior management must have the appropriate locks changed.

IT / COMPUTER SECURITY SOP

1 Principle

Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers must have a commitment, to ensure that information Technology (IT) systems are secure.

2 Objective

To ensure that Business partner's computer systems, networks and internet connections are secure and protected from internal & external threats.

3 Definition

C-TPAT stands for Customs-Trade Partnership Against Terrorism, a supply chain security program sponsored by U.S. Customs & Border Protection (CBP).

Information Technology refers to computer systems, hardware, software, internet connections and other things associated with processing computer data.

4. Responsibilities

Your company's senior management is responsible for ensuring that all computer systems are secure and that the security items noted in this SOP are implemented and maintained.

5. IT Security

5.1 Network password protection - Automated systems must use individually assigned accounts with unique access codes and passwords. Employees must select their own password (passwords should not be assigned by a manager or computer systems administrator).

5.2 Network passwords must be changed at least every 90 days.

5.3 Network password changes must be "forced". This means that each user should receive an automated e-mail notification instructing them that their password must be changed by a certain date. Failure to change the password by the indicated date must result in the user's loss of access to the network until such time that the password has been changed and access has been reestablished by an administrator.

5.4 All computers must be programmed so that 3 failed login attempts will result in the user being locked out of the system.

5.5 All computers must be programmed so that after 15 minutes of inactivity the user will be locked out and will be required to log back in.

5.6 Network Passwords and access codes must be deleted from the system upon the last day of employment for all employees.

6. IT Policies

6.1 IT security policies, procedures and standards must be in place and provided to employees in the form of training.

6.2 Employee access to systems and databases must be limited by levels of authority, assigned by management as per the employee job description.

6.3 The Business partner's computer system must include tools for tracking and recording a user's activities and allow for authorized management to monitor the user.

6.4 Abuse of IT systems, including improper access, tampering or the altering of business data must be prohibited. All system violators must be subject to

appropriate disciplinary actions for abuse, up to and including termination.

BUSINESS PARTNER SCREENING SOP

1.Principle

Business partners, including vendors, service providers, factories, cargo freight stations, 3rd party warehouses, transportation providers, foreign agents and customs brokers must have a commitment to properly screen business partners who are involved in the international supply chain.

2.Objective

To ensure that Business partners have proper business partner screening practices in place.

3.Definition

C-TPAT stands for Customs-Trade Partnership Against Terrorism, a supply chain security program sponsored by U.S. Customs & Border Protection (CBP).

Supply Chain refers to every company or transportation step involved in transporting products from the factory/supplier to the destination where the container is unloaded.

Business Partner refers to any company that is involved in our international supply chain, including freight forwarders, trucking companies, rail companies, airlines, sea carriers, terminals, customs brokers, CFS (Cargo Freight Stations), trans-loading warehouses and final destinations.

4.0 **Responsibilities**

Your company's senior management is responsible for ensuring that all business partner screening is conducted initially and periodically (annually).

5.0 Procedures

Your company must require their international business partners to comply with C-TPAT supply chain security practices. You must screen potential business partners to ensure compliance. Your company must give additional scrutiny to potential business partners that are of a higher risk due to one or more factors such as being located in a high-risk country, directly involved with loading and/or storing of containers, volume (amount of business you do with them), unknown companies or companies with a history of security violations.

5.1 Your company must divide its business partners into two major categories:

5.1.1 Category 1 – Those business partners who are C-TPAT certified or who are certified in a U.S. Customs-approved supply chain security program such as AEO (Taiwan, Japan, EU, Mexico, Korea, Singapore, Mexico), Secure Export Scheme Program (New Zealand), Partners in Protection (Canada) or the Golden List Program (Jordan).

5.1.2 Category 2 - Those business partners who are not a member of a government-sponsored supply chain security program.

5.2 For Category 1 business partners you must require proof of their certification, such as their government-issued supply chain security certificate, other government-issued documentation or a screen-shot of the companies c-TPAT portal account showing their status as "certified".

NOTE: Status Verification Interface (SVI) numbers are no longer issued by US Customs to C-TPAT certified companies. C-TPAT certified companies can monitor one another's C-TPAT status via their C-TPAT portal accounts, but non-C-TPAT certified don't have access to a portal account that will allow them to do this. Therefore, the screen-shot of the certified company's C-TPAT accounts page is the current best option.

5.3 For Category 2 business partners authorized staff must perform the following tasks.

5.3.1 A Security Questionnaire must be is sent to the business partner via e-

mail.

5.3.2 You must require our business partners to complete the questionnaire and return them to us via e-mail.

5.3.3 The completed forms must be reviewed for acceptable responses.

5.3.4 If a completed security questionnaire contains inadequate or unacceptable responses a follow up process must be initiated to advise the business partner of the minimum requirement and to secure compliance.

5.3.5 Completed security questionnaires that contain only acceptable answers must be formally approved and kept on file.

5.3.6 This process must be repeated annually.

5.4 Your company or its assigned representative should make on-site visits to selected business partners whenever possible. During those visits a security audit is conducted. The security audit should include verification of the responses on the most recently completed security questionnaire.

5.5 Your company must communicate the importance of supply chain security and maintaining chain of custody to it's supply chain business partners.