

CTPAT 2020 Changes

Part 1: Introduction

Burlington Stores works continuously with U.S. Customs and Border Protection (CBP) and our business partners to strengthen the international supply chain and improve United States border security. Burlington Stores participates in U.S., CBP's cargo security program, Customs-Trade Partnership Against Terrorism (CTPAT). CBP has developed new minimum security criteria for importers, which include the mandate that importers enforce such requirements with respect to their service providers, including vendors, manufacturers, carriers, brokers, warehouses, distribution centers, raw material suppliers, all transportation networks, etc. "). In alignment with CBP's CTPAT Minimum Security Criteria, Burlington has updated our own required security procedures herein for all Burlington Stores' vendors, service providers, and business partners.

Part 2: Mandatory Checklist for all Business Partners

The following must be completed before conducting business with Burlington Stores:

- Read Part 3: CTPAT Minimum Security Criteria below.
 - *The procedures listed in this section are mandated by U.S. CBP. You must observe and follow these procedures in order to be an approved Burlington Stores vendor.*
- Read Part 4: Additional Required CTPAT Criteria below.
 - *The procedures listed in this section are mandated by Burlington Stores. You must observe and follow these procedures in order to be an approved Burlington Stores vendor.*
- If your company is a certified CTPAT Member please send Burlington an invite to follow your company within the CTPAT portal. If a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States (or an approved MRA), please forward a copy of the certification to ctpat@burlington.com.
- CBP and Burlington Stores encourage all business partners to conduct annual or as needed self-assessments based on level of risk.

Part 3: CTPAT Minimum Security Criteria

All business partners **must** have, at a minimum, the following security measures, unless they are able to prove to Burlington's satisfaction that they are not applicable to their particular facilities or industry:

A. Physical Security:

1. Physical barriers and/or deterrents in place to prevent unauthorized access to offices, trailer yards, cargo handling and storage facilities.
2. Gates where vehicles and/or personnel enter or exit manned or monitored.
3. Individuals and vehicles subject to search in accordance with local labor laws.
4. Adequate lighting provided inside and outside the facility.
5. Written policies and procedures governing the use, maintenance, and protection of any security technology used and/or a third party central monitoring station, if applicable.

6. Camera systems deployed, they must be positioned to cover key areas of the facilities and random reviews of the footage must be reviewed to verify that cargo security procedures are being properly followed in accordance to law.
- B. Physical Access Controls:
1. Procedures governing how identification badges and access is granted, changed, and removed.
 2. Visitors, vendors, and service providers must present photo identification upon arrival, be issued temporary identification during the visit to be displayed at all times, and be escorted throughout their visit by a company employee.
 3. Drivers delivering or receiving cargo must be positively identified before cargo is received or released. A cargo pickup log must be kept to register drivers and record the details of their conveyances when picking up cargo.
 4. If security guards are used, work instructions must be in written policies and procedures and compliance with these verified.
- C. Procedural Security:
1. Cargo staging areas must be secure from unauthorized access and inspected on a regular basis to ensure the area remains free of visible pest contamination.
 2. All information used in the clearing of the merchandise/cargo needs to be legible, complete, accurate, protected against loss, and reported on time. Bills of lading (BOLs) must accurately reflect the information provided to the carrier. Shortages and overages must be investigated and resolved.
 3. Relevant personnel must be trained on how to identify suspicious cargo shipments and report any suspicious activities that may affect the supply chain.
 4. Procedures in place to identify, challenge and address unauthorized/unidentified persons and remove them from the premises.
- D. Conveyance Security:
1. Containers must be stored in a secure area to prevent unauthorized access.
 2. Written procedures must be in place for both security and agricultural inspections of containers prior to loading/stuffing/packing. A seven-point inspection must be completed on all empty containers and an eight-point inspection must be completed on all empty refrigerated containers:
 1. Front Wall
 2. Left side
 3. Right Side
 4. Floor
 5. Ceiling/Roof
 6. Inside/Outside doors, including the reliability of the locking mechanisms of the doors
 7. Outside/undercarriage
 8. Fan housing on refrigerated containers
 3. Containers must be equipped with external hardware that can reasonably withstand attempts to remove it.
 4. When threats to a shipment are discovered, business partners must be alerted as soon as feasibly possible.
- E. Personnel Security:
1. Written procedures for screening prospective employees and for performing checks on current employees.
 2. An employee code of conduct that includes expectations and defines acceptable

behaviors. Employees and contractors must be required to acknowledge that they have read and understand the Code of Conduct.

F. Education, Training, and Awareness:

1. Security training must be provided to employees and required based on their functions and position. A security training log must be kept. Personnel in sensitive positions need to receive additional specialized training geared towards the responsibilities that the position holds.
2. Drivers and other personnel that conduct security and agricultural inspections of empty conveyances must be trained on how to inspect containers for both security and agricultural purposes, such as visible pest contamination.
3. Employees must be trained on operating and managing security technology systems, how to identify the warning indicators of trade based money laundering and terrorism financing, as well as how to report security incidents and suspicious activities.

G. Cybersecurity:

1. Comprehensive written cybersecurity policies and/or procedures that are reviewed annually to protect information technology (IT) systems and have them regularly updated, how to recover loss of data and/or equipment in the event of a breach, and how to address vulnerabilities.
2. A system to identify the abuse of IT including improper access, tampering, or the altering of business data. All systems violators must be subject to appropriate disciplinary actions for abuse.
3. Authorized access must be restricted based on assigned duties, and reviewed on a regular basis to ensure access to sensitive systems is based on job requirements.
4. Individuals with access to IT systems need 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.
5. When users are allowed to remotely connect to a network or use personal devices to conduct company work, secure technologies must be employed to allow employees to access the company's intranet securely when located outside of the office.
6. All media, hardware, or other IT equipment that contains sensitive information must be accounted for through regular inventories and properly sanitized and/or destroyed in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization or other appropriate industry guidelines, when necessary.

H. Agricultural Security:

1. Written procedures must be in place to prevent visible pest contamination throughout the supply chain to include compliance with Wood Packaging Materials (WPM) regulations. The measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15).

I. Seal Security:

1. Written seal controls need to include procedures on how to control/restrict access, secure storage, conduct and document audits to account for inventory, distribution, tracking seal information in a log, issuance, etc. of seals. Written procedures must be kept on how to handle and report seal discrepancies.

2. All shipments must be sealed and secured immediately after loading/stuffing/packing with a high security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high security seals. All seals must be affixed properly to containers, which can be tested using the VTTT process: View, Tug, Twist, and Turn.

Part 4: Additional Required CTPAT Criteria

1. Burlington Stores reserves the right to visit or have a contracted third party visit international proprietary (or contracted) facilities.
2. Vendor agrees to work with Burlington Stores to meet and/or exceed all CTPAT required minimum security criteria via a Corrective Action Plan (CAP) report, if necessary.
3. All stuffing location and factory information including addresses, contact information, telephone number and email address, must be disclosed at the time of booking with MCS/MOL. Burlington Stores will not accept any bookings of shipments without disclosure of this information.
4. All inland carriers are required to acknowledge in writing the quantity of cartons, by marks and number, picked up from vendor.
5. Consolidators and international carriers are required to acknowledge to the inland carrier that they received the cartons that the inland carriers received from the vendor in sealed condition.
6. Records relating to cargo security are to be maintained for a period of one year and produced upon request.
7. All vendors are required to provide a production schedule that identifies, by name, address, and production steps, all sub-contractors that will be used to manufacture the merchandise. Vendors must ensure that their sub-contractors and vendors of materials, etc., are also in compliance with our security standards.
8. Before a vendor is permitted to change the country of origin or delivery schedule, a detailed explanation must be provided and approved by the company. All discussions regarding these changes should be recorded and dated in the purchase order file.
9. If any security changes are implemented to your business to conform to Burlington Stores minimum security requirements mentioned, please inform us of such changes in writing by contacting ctpat@burlington.com.