CTPAT™
YOUR SUPPLY CHAIN'S STRONGEST LINK.

Minimum Security Criteria and Best Practices for Factories

Kohl's Department Stores is a Tier III member of the Customs Trade Partnership Against Terrorism (CTPAT) program. Membership at the Tier III level provides significant benefits to Kohl's in the form of Supply Chain Predictability. To maintain membership at Tier III, Kohl's and its business partners, must continually look for opportunities to exceed CTPAT criteria.

Factories approved for production of Kohl's Private and Exclusive brands are integral to Kohl's maintaining CTPAT membership. As such, Kohl's expects that all factories implement and maintain a CTPAT program that is in compliance with CTPAT program criteria.

Below are twelve CTPAT minimum security criteria. This should serve as a guideline for development of a CTPAT compliant program. All factories will be evaluated by Kohl's or a third party to ensure compliance with these criteria.

The below Best Practices are provided as a guide for factories to implement processes that exceed the minimum criteria. The Best Practices listed are suggestions for each criterion; however, each factory should evaluate their operations and implement best practices that are manageable, documented and that can be validated.

1) Security Vision and Responsibility

Instilling security as an integral part of a company's culture and ensuring that it is a companywide priority is in large part the responsibility of the company's leadership.

Minimum Security Criteria	Best Practices
• Factory security policies must include a review component. • The companies' point of contact (POC) must be knowledgeable in CTPAT program requirements.	• Review process does not need to be complex. • CTPAT expects the designated POC to be proactive and responsive to their Supply Chain Security Specialist

2) Risk Assessment

Factory must have a process in place to assess risk throughout the supply chain including business process and operations, business partners and shipping/export processes.

Minimum Security Criteria	Best Practices
• Factory has an established Risk Assessment procedure to identify: Terrorism, smuggling, human and drug trafficking, organized crime and internal conspiracy. • Documented process for how Risk Assessment is conducted. • Risk Assessments and Corrective Actions are documented.	• Implemented "5 Step Risk Assessment" • Factory utilizes a computer software risk-based assessment tool. • Factory or Vendor employee is assigned to managing the Risk Assessment process.

3) Business Partner Security

All factories producing goods for Kohl's must have written and verifiable processes for the selection of business partners including, carriers, suppliers, and service providers.

Minimum Security Criteria	Best Practices
• Documented procedure for selecting Business Partners that considers the partner's security controls, financial stability and corporate history. o Must be reviewed by management prior to contract confirmation. • Factories must ensure that business partners develop security processes and procedures consistent with CTPAT security criteria. • Require business partners to provide written/electronic confirmation that they understand and are meeting CTPAT security criteria (e.g., contractual obligations; letter from senior business partner; written statement confirming compliance with CTPAT security criteria). • Factories must have contracts with business partners that include CTPAT criteria.	• Perform periodic audits of business partners commitment to CTPAT security criteria o Require Corrective Action Plans (CAPs) and follow up to ensure compliance. • Provide CTPAT Security Criteria training and expectations to business partners. o Log training activities • Factory communicates Security Policies to Business Partners (letters, brochures, email broadcasts, web site, etc.) • Verify potential Business Partners company business address and how long they have been at that address; check references; request credit report and conduct research on the internet both on the company and its principals.

4) Cybersecurity

With increased connectivity to the internet comes the risk of a breach of a company's information systems. This threat pertains to businesses of all types and sizes. Measures to secure a company's IT and data are of paramount importance and the listed criteria provide a foundation for an overall cybersecurity program.

Minimum Security Criteria	Best Practices
• Facilities must have comprehensive written cybersecurity policies and/or procedures to protect IT systems as applicable. • Facilities using network systems must regularly test the security of their IT infrastructure. • Cybersecurity policies must be reviewed annually. • User access must be restricted based on job description or assigned duties. • Computer and network access must be removed upon employee separation.	• Facilities are encouraged to follow cybersecurity protocols that are based on recognized industry standards. • This can be done by scheduling vulnerability scans. There are many free and commercial versions of vulnerability scanners available. • Following the review, policies and procedures should be updated in necessary.

5) Conveyance and Instruments of International Traffic Security

Factories must ensure that container and trailer integrity is maintained to protect against the introduction of contraband, unauthorized materials, pest contaminants, plant material and/or persons.

Minimum Security Criteria	**Best Practices**
Containers and Trailers • Only closed-end trucks and shipping containers are used for transporting goods. • Factory must ensure secure container storage (empty and full) to prevent unauthorized access and/or manipulation. • Perform and document the 7-point container inspection to verify physical integrity of the container structure prior to stuffing including verifying there are no pest contaminants, plant material or mold. • Written procedure including the inspection, control and storage of containers. • LCL/CFS shipments must be transported directly to the CFS in a closed box truck. • LCL trucks are sealed through to the CFS. • Loading of containers is captured on CCTV. • FCL shipment move directly to Port.	*Containers and Trailers* • Utilize laser measuring devices to detect false walls, compartments and hidden contraband. • Photograph loaded container including digital images of container with seal. These photos are maintained in the shipping records. • Empty containers are sealed at all times. • Intrusion alarms are used to notify security or factory personnel of container tampering. • Use tamper-indicative security labels attached to or covering doors and hinges on containers. • Container/trailer loading is monitored by more than one person including security or a supervisor/manager • Multiple seals or security devices are used on each container/trailer.

6) Seal Security

The sealing of trailers and containers to attain continuous seal integrity continues to be a crucial element of a secure supply chain.

Minimum Security Criteria	**Best Practices**
High Security Seals • High security container seals must be used (meet or exceed PAS ISO 17712:2013). • Seal verification includes VVTT procedure. • Procedure must include recognizing and reporting compromised seals. • Unused container seals kept in a secure place. • Outbound container contents are manifested and seal numbers are recorded. • Written procedure must include the use, control, storage and log of all seals.	*High Security Seals* • Incorporate additional tamper-indicative security labels covering hinges and/or the two doors of the container. • Incorporate additional bolt seals or cast iron J-bar devices to the locking bar that requires a specialized tool for removal.

7) Procedural Security

Procedural Security encompasses many aspects of the import-export process, documentation and cargo storage and handling requirements.

Minimum Security Criteria	Best Practices
• When cargo is staged overnight or for an extended period of time, measures must be taken to secure the cargo from unauthorized access. • Cargo staging areas and the immediate surrounding areas must be inspected on a regular basis to ensure these areas remain free of visible pest contamination. • Facilities must have written procedures for reporting an incident, which includes a description of the facility's internal escalation process.	• Preventative pest control methods such as baits, traps or other barriers can be used as necessary. Removal of weeds or reduction of vegetation is also suggested. • Internal problems such as theft, fraud and internal conspiracies may be reported more readily if the reporting party knows the concern may be reported anonymously.

8) Agricultural Security

Agriculture is an industry threatened by the introduction of foreign animal and plant contaminants such as soil, seeds, plant and animal material with may harbor invasive and destructive pests and diseases.

Minimum Security Criteria	Best Practices
• Facilities must have written procedures designed to prevent visible pest contamination to include Wood Packaging Materials. • Visible pest prevention measures must be adhered to throughout the supply chain.	• When completing the 7 point inspection before filling the trailer or container, facilities should also be checking the corners, walls, floor and ceiling for insects, nests, webs, dirt, plant material or mold.

9) Physical Access Controls

Factories must have procedures and controls in place that prevent unauthorized entry to the factory and that manage access of employees and visitors to controlled areas within the factory.

Minimum Security Criteria	Best Practices
Visitors: • Photo ID required for all visitors upon arrival • Visitor log maintained • All visitors are provided a visitor badge • All visitors are escorted by factory employee *Employees:* • All employees are issued ID badges and must be required to be visible at all times. • Documented procedures for the issuance, removal and changing of access devices (i.e. ID Badges, keys, etc.). • Procedures in place to identify, challenge and address unauthorized/unidentified personnel. • Photos of authorized employees are posted in restricted areas. • Procedures must be in place to restrict access to packing, finished goods and shipping areas.	*Visitors:* • Issue thermal-activated visitor ID badges featuring expiration after 8 hours. • Visitors are required to provide advance information prior to factory visit. • All visitors are given a pamphlet and/or visitor ID with security rules to be followed while on premises. • Factory creates new visitor badges once it is determined that 25% of the visitor badges have been lost or damaged. • Visitors are subject to metal detector and/or x-ray to gain access to the factory. *Employees:* • Employees scan ID when entering the factory and their photo is displayed on a monitor for security to verify the employee. • Photos of all terminated employees are displayed at entrance points to avoid unauthorized access. • Employees observed/monitored for suspicious activities and/or behavior.

10) Physical Security

Factories must incorporate controls for manufacturing, cargo handling and storage facilities that include physical barriers and deterrents that guard against unauthorized access.

Minimum Security Criteria	Best Practices
• Buildings constructed of durable materials that resist unlawful entry. • Regularly inspect perimeter wall/fencing for integrity and/or damage. • Factory maintains full-time or contract security guards and has documented procedures. • Gates are manned/monitored. • Visitor or vehicle parking should not be located near cargo handling or storage areas. • External gates, fences, doors and windows secured with locking devices. • Control of the issuance of all locks and keys by management or security personnel. • Physical barriers and deterrents that guard against unauthorized access to building, cargo handling and storage areas. • Adequate internal and external lighting. • CCTV coverage of access points, finished goods, loading, unloading, and storage areas. • CCTV tapes must be maintained for 45 days. • CCTV cameras monitored by designated employee/guard monitor at all times. • Alarms/automatic intrusion detection systems should be utilized and tested to prevent unauthorized access to the building and finished goods area.	• Factory install double-layered perimeter fence. • Factory security includes Guard view towers at each corner. • Incorporate alarm systems including motion sensors or door/window contact sensors to signal security. • Factory has emergency power source/generator. • Gates and perimeter are monitored by guard during non-operating hours. • Gates and perimeter are monitored by CCTV during non-operating hours. • Guard station is equipped with a hidden duress (panic) button to alert community law enforcement to a security threat. • Factory has installed an electronic check system to record scheduled security check of internal and external perimeter points. • Guard's radios are equipped with a body alarm function. • Visitors' vehicles are searched and recorded, and a parking pass is provided.

11) Personnel Security

Factories must have processes in place to screen prospective employees and perform periodic checks on employees. Security breaches all have one thing in common…*PEOPLE*.

Minimum Security Criteria	Best Practices
• Processes in place to screen prospective employees. • Verification of application information, such as employment history and references, prior to employment. • Periodic background checks are performed. • Employee files are maintained that include application, work history, background check and photos. • Documented procedures to remove identification, facility and system access for terminated employees.	• Conduct exit interviews with employees with a focus on evaluating the potential for retaliation from the terminated employee. • Employees are encouraged to report irregularities through phone number/hotline, suggestion box or other means. • Factory provides an incentive program to reward employees who report security irregularities. • Factory requires background checks for security guards. • Factory incorporates security as part of job descriptions.

12) Education, Training and Awareness

Factory must have a Threat Awareness training program that is provided to all new and existing employees on how to recognize and report security threats.

Minimum Security Criteria	Best Practices
• Factory must have a training program in place for all employees that will provide awareness of security procedures. • Training must be provided that informs all employees on identifying illegal conduct/activities, unauthorized persons, and insertion of illegal/unauthorized materials. • Additional training must be provided to security personnel and shipping/receiving employees. • Training must be provided in local language, documented and attendance recorded.	• Photos of training sessions are maintained with training history log. • Employees are tested on understanding of CTPAT requirements following training. • Employees are provided with an Employee Handbook that includes CTPAT/security procedures. • Factory conducts security mock drills.