2022

Designer Brands / DSW / VCS Group dba Camuto Group

Supply Chain Security Standards for Import Suppliers

INTERNATIONAL LOGISTICS

STEWART HINDMAN III

DESIGNER BRANDS INC. SUPPLY CHAIN SECURITY STANDARDS FOR IMPORT SUPPLIERS

As a participant in the Customs-Trade Partnership Against Terrorism (C-TPAT), Designer Brands/DSW/VCS Group dba Camuto Group "Designer Brands"), is committed to taking appropriate steps to prevent infiltration of unmanifested materials into shipments of its product. While Designer Brands C-TPAT program encompasses the entire supply chain, the Supply Chain Security Standards for Import Suppliers provides specific requirements for all factories that produce finished goods and/or prepare the finished good for shipment for Designer Brands or its subsidiaries, divisions or agents ("Factories").

Designer Brands Group encourages all its supply chain partners – including Factories – to continuously improve supply chain security. All supply chain partners are encouraged to maintain a current understanding of the requirements under the C-TPAT program through reference to the US Customs Border Protection programs at https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat In addition, Factories should consider – and implement where possible – best practices including those identified on the CBP website (https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism/bestpractices).

1. ***Business Partner Requirements***

- ☐ Factories will maintain process for selection of business partners.
- ☐ Factories will require business partners to comply with supply chain security standards.
- ☐ Factories will conduct periodic reviews of business partners' processes and facilities.

2. ***Cyber Security***

- ☐ Factories must have comprehensive written cybersecurity policies and/or procedures to protect technology (IT) systems. The written IT policy, at a minimum, must cover all the individual Cybersecurity criteria.
    - Factories are encouraged to follow cybersecurity protocols that are based on recognized industry framework/standards. This "National Institute of Standards and Technology (NIST) is one example (http://www.nist.gov/cyberframework) that offers voluntary guidance based upon existing standards, guidelines and practices. It can be used to help identify and prioritize actions for reducing cybersecurity risk and it is a tool for aligning policy, business and technological approaches to managing that risk. The Framework completements an organizations risk management process and cybersecurity program.

- ☐ To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in Factories' computer systems. Factories' must ensure that their security software is current and receives regular security updates.
    - Factories' must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or other unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.

- ☐ Factories utilizing network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.
    - Testing records must be maintained.

- ☐ A system must be in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions.

- ☐ Cybersecurity policies and procedures must be reviewed annually, or more frequently, as risk or circumstances dictate. Following the review, policies and procedures must be updated if necessary.

- ☐ User access must be restricted based on job description or assigned duties. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements. Computer and network access must be removed upon employee separation.
- ☐ Individuals with access to Information Technology (IT) systems must use individually assigned

accounts. Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication and user access to IT systems must be safeguarded.

- To guard IT systems against infiltration, user access must be safeguarded by going through an authentication process. Complex login passwords or passphrases, biometric technologies, and electronic ID cards are three different types of authentication processes. Processes that use more than one measure are preferred. These are referred to as two-factor authentication (2FA) or multi-factor authentication (MFA). MFA is the most secure because it requires a user to present two or more pieces of evidence (credentials) to authenticate the person's identity during the log-on process.

- MFAs can assist in closing network intrusions exploited by weak passwords or stolen credentials. MFAs can assist in closing these attack vectors by requiring individuals to augment passwords or passphrases (something you know) with something you have, like a token, or one of your physical features - a biometric.

- If using passwords, they need to be complex. The National Institute of Standards and Technology's (NIST) NIST Special Publication 800-63B: Digital Identity Guidelines, includes password guidelines (https://pages.nist.gov/800-63-3/sp800-63b.html). It recommends the use of long, easy to remember passphrases instead of words with special characters. These longer passphrases (NIST recommends allowing up to 64 characters in length) are considered much harder to crack because they are made up of an easily memorized sentence or phrase.

- Factories that allow their users to remotely connect to a network must employ secure technologies, such as virtual private networks (VPNs), to allow employees to access the company's intranet securely when located outside of the office. Factories must also have procedures designed to prevent remote access from unauthorized users.
  - VPNs are not the only choice to protect remote access to a network. Multi-factor authentication (MFA) is another method. An example of a multi-factor authentication would be a token with a dynamic security code that the employee must type in to access the network.

- If Factories allow employees to use personal devices to conduct company work, all such devices must adhere to the company's cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network.

- All media, hardware, or other IT equipment that contains sensitive information regarding the import/export process must be accounted for through regular inventories. When disposed, they must be 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.

3. ***Conveyance and Instruments of International Traffic Security***

- ☐ Containers / trailers must be stored in a secure area to prevent unauthorized access (both loaded and empty).
- ☐ Factories will ensure all containers (both empty and loaded) are inspected for concealed contraband, damage and agricultural contaminates prior to loading/unloading. Factories must utilize 7 Point Container Inspection and documented. Refer to
- ☐ If Factory discovers credible (or detected) threat to security of a container/trailer they MUST alert (as soon as possible) any business partners in the supply chain that may be affected as well as any law enforcement agencies as appropriate.
- ☐ Conveyances and Instruments of International Traffic (as appropriate) must be equipped with external hardware that can reasonably withstand attempts to remove it. The door, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device.

4. ***Seal Security***

- ☐ Written procedures must stipulate how seals are to be controlled and affixed to loaded containers, including procedures for how to recognize and report compromised seals and containers. Additionally, these procedures must include VVTT procedures:
  - V – View the seal and container locking devices to ensure no physical damage
  - V – Verify that the seal number matches the shipping documentation
  - T – Tug on the seal to make sure it is affixed properly
  - T – Twist and turn the seal to make sure it does not unscrew
- ☐ Only designated employees (Management) can be allowed to distribute container seals for integrity purposes.
- ☐ Seals must always be stored in a designated and locked area during the loading process or anytime they are not in use with access controls for Management only.
- ☐ All seals must be recorded along with container numbers for inbound and outbound cargo
- ☐ Factory shipments that can be sealed with a high security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high security seals.
- ☐ Factories will ensure all outbound containers and trucks are sealed by security personnel or factory management.

5. ***Procedural Security***

- ☐ A documented Security Policy and Procedures should be in place that include all element of the CTPAT Minimum Security Criteria for Foreign Manufacturers (refer to www.cbp.gov/ctpat).
- ☐ Factory's Security Policy and Procedures will include protocols for reporting abnormalities from the factory to local government or enforcement agencies.
- ☐ Consistent with Vendor Guidelines, Factories will ensure all manifest information legible, complete and accurate.
  - All cartons must be properly marked, weighed and counted.
- ☐ All shortages, overages, and other significant discrepancies or anomalies must be investigated and resolved, as appropriate.

- When cargo is staged overnight, or for an extended period, 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.
    - Preventative measures such as the use of baits, traps, or other barriers can be used as necessary. Removal of weeds or reduction of overgrown vegetation may help in the elimination of pest habitat within staging areas.
- Factories will segregate packing areas from the manufacturing, shipping and receiving areas.
- Factories will limit access to packing, shipping and receiving areas to assigned and authorized employment.
- Factories will ensure packing is supervised by security personnel or factory management.
- Factories will segregate packed cargo in a secure area.
- Factories will ensure all inbound and outbound cargo is inspected by either security personnel or factory management. In addition, Factories will periodically screen packages – including mail – before distribution.
- Only security officers or designated personnel (factory management) should be allowed to inspect the container loading and unloading of containers/trailers.
- Factories will maintain a list – including the name and address – of current and active providers used to transport cargo to the consolidator, freight forwarder or carrier.
- An outbound shipment log should be used to records details of all shipments departing the Factories facility. Outbound logs should be maintained for at least 90 Days.
- Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons. Personnel must know the protocol to challenge an unknown/unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises.

6. Agricultural Security

- Designer Brands Group does NOT allow Wood Packing Material (WPM) to be shipped within containers bound into the US. By not allowing WPM the risk of pest contamination is reduced.

7. Physical Security

- All cargo handling and storage facilities, including trailer yards and offices must have physical barriers and/or deterrents that prevent unauthorized access.
- Perimeter fencing should enclose the areas around cargo handling and storage facilities. If a facility handles cargo, interior fencing should be used to secure cargo and cargo handling areas.
    - Based on risk, additional interior fencing should segregate various types of cargo such as domestic, international, high value, and/or hazardous materials. Fencing should be regularly inspected for integrity and damage by designated personnel.
    - If damage is found in the fencing, repairs should be made as soon as possible.
- Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and conveyances.

- ☐ Gates where vehicles and/or personnel enter or exit (as well as other points of egress) must be manned or monitored.
- ☐ Adequate lighting must be provided inside and outside the facility including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas.
- ☐ Security technology should be used to monitor premises and prevent unauthorized access to sensitive areas.
    - Written policies and procedures governing the use, maintenance, and protection of this technology.
- ☐ Access to the locations where the technology is controlled or managed is limited to authorized personnel.
    - Procedures that have been implemented to test/inspect the technology on a regular basis. The inspections should include verification that all the equipment is working properly and is positioned correctly.
- ☐ Security technology policies and procedures must be reviewed and updated annually, or more frequently, as risk or circumstances dictate.
- ☐ Security technology infrastructure must be physically secured from unauthorized access.
- ☐ If camera systems are deployed, cameras must be positioned to cover key areas of facilities that pertain to the import/export process.
- ☐ Cameras should be programmed to record at the highest picture quality setting available and be set to record on a 24/7 basis.
    - Periodic, random reviews of the camera footage must be conducted (by management, or security) to verify that cargo security procedures are being properly followed. The results must be maintained for a sufficient time for audit purposes.

8. ***Physical Access Controls***

- ☐ Factory must have written procedures governing how identification badges and access devices are granted, changed, and removed.
- ☐ Factories will ensure that all visitors are recorded in a visitor log upon arrival, which should detail:
    - Date of Visit
    - Visitors Name
    - Verification of photo ID
    - Company points of contact
    - Time of Arrival / Time of Departure
- ☐ Factories will provide visitors with Visitors badge that must be worn at all time while in the facility.
- ☐ Drivers delivering or receiving cargo must be positively identified before cargo is received or released. Drivers must present government-issued photo identification to the facility employee granting access to verify their identity.

- A cargo pickup log must be kept registering drivers and record the details of their conveyances when picking up cargo. When drivers arrive to pick up cargo at a facility, a facility employee must register them in the cargo pickup log. Upon departure, drivers must be logged out. The cargo log must be kept secured, and drivers must not be allowed access to it.
    - Drivers Name
    - Date and time of arrival
    - Employer, truck number/trailer number
    - Time of departure
    - Seal number affixed to the shipment at time of departure
- If security guards are used, work instructions for security guards must be contained in written policies and procedures. Management must periodically verify compliance and appropriateness with these procedures through audits and policy reviews.

9. ***Personnel Security***

- Factories will pre-screen prospective employees for position in the packing, shipping or receiving areas.
- Factories will perform background checks – where permitted by local law – part of the pre-screening of all prospective facility security employees and management employees in the packing, shipping and receiving areas.
- Factories will re-perform background checks on a periodic basis.

10. ***Education, Training and Awareness***

- Factories must establish and maintain a security training and awareness program to recognize and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain.
- Factories must retain evidence of training such as training logs, sign in sheets or electronic training. Included should be the date of training, names of attendees and topics of training.
- Drivers and other personnel that conduct security and agricultural inspections of empty containers/trailers must be trained to inspect their conveyances/IIT for both security and agricultural purposes. Inspection training must include the following topics:
    - Signs of hidden compartments
    - Concealed contraband in naturally occurring compartments
    - Signs of pest contamination
- Training must be provided to applicable personnel on preventing visible pest contamination. Training must encompass pest prevention measures, regulatory requirements applicable to wood packaging materials (WPM), and identification of infested wood.
- As applicable based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access.
- Personnel operating and managing security technology systems must have received training in their operation and maintenance. Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable.
- Personnel must be trained on how to report security incidents and suspicious activities.

Agreement to Strengthen Supply Chain Security Consistent with C-TPAT Guidelines

The Factory agrees to develop and implement, within a framework consistent with the Custom-Trade Partnership Against Terrorism (C-TPAT) security criteria, a verifiable, documented program to enhance security procedures throughout its supply chain process, including, but not limited to, its manufacturing business partners. Where the Factory does not exercise control of production facility, transportation or distribution entity, or process in the supply chain, the Factory agrees to communicate the C-TPAT security criteria to its manufactures and transportation/distribution service providers and, where practical, condition its relationship to those entities on the acceptance and implementation of the C-TPAT security criteria.

The Factory agrees to communicate Designer Brands supply chain security and C-TPAT procedures to its manufacturers in a documented and verifiable format that can be made available upon request, and it understands that failure to do so may jeopardize its business relationship with Designer Brands.

Factories MUST complete the " 2022 C-TPAT Questionnaire" at the time on onboarding in the Designer Brands Inc., systems as an approved supplier. The questionnaire speaks to the specific criteria in this form and MUST be signed by factory management familiar with processes.