A Message Regarding Security Procedures Guidelines for
Warehouse Operators

Kingchem Life Science LLC is a participant in the Customs-Trade Partnership Against Terrorism (CTPAT) program of the United States Customs & Border Patrol agency (CBP).

CTPAT is a voluntary joint government-business initiative to build cooperative relationships that strengthen the overall supply chain and border security. Everyone involved in logistics, distribution, or supply chain management will be impacted by ongoing efforts to create a more secure global trading system.

Importers such as our company are expected to complete a security assessment of our entire supply chain. The assessment must include the security-related subjects of:

Access Control
Agricultural Procedures
Business Partners
Conveyance Security
Information Technology
Personnel Security
Physical Security
Procedural Security
Security Awareness Training
Trade-Based Money Laundering
Upper Management Responsibility

It is very important that our business partners have strong, written security-procedures programs that are actively followed in daily their operations. Consequently, we need to request that you complete and return to us a completed Warehouse Operators security-procedures questionnaire.

Please provide this information to us as soon as you receive this letter. If you should have any questions, please contact us by replying to the email by which you received this message, or at telephone number: +1-201-825-9988 (fax number: +1-201-825-9148).

Thank you for your assistance with this very important matter.

Best regards,
Kingchem Life Science LLC

Warehouse Operators

Security-Procedures Guidelines

It is very important that our business partners have strong, written security-procedures programs that are actively followed in daily their operations. To build a robust Supply Chain Security Program, a company should incorporate representatives from all of the relevant departments into a cross-functional team. The below guidelines should be followed carefully by that team.

The supply chain security program should also be designed with, supported by, and implemented by an appropriate written review component. The purpose of this review component is to document that a system is in place whereby personnel are held accountable for their responsibilities and all security procedures outlined by the security program are being carried out as designed. The review plan must be updated as needed based on pertinent changes in an organization's operations and level of risk.

Business Partner Requirements

- The warehouse operator must exercise due diligence regarding the screening and selection of business partners(contractors, carriers, and vendors) to ensure that contracted or outsource companies who provide transportation, cargo handling security and other services commit to adhering to strong CTPAT-like security-procedures guidelines.
- For those business partners eligible for CTPAT certification (importers, ports, terminals, brokers) the warehouse operator must have documentation indicating whether these business partners are, or are not, CTPAT certified. Non-CTPAT business partners should be subject to additional scrutiny by the warehouse operator.
- Periodic reviews should be performed on service providers to detect weakness, or potential weakness, in their security procedures. A factor that your company should include in this process is checks on activity related to money laundering and terrorist funding. To assist with this process, please consult CTPAT's Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities, as published by the CBP (see below section on trade-based money laundering).

Conveyances and Instruments of International Traffic (IIT)

Container and conveyance (tractor and trailer) integrity procedures must be maintained to protect against the introduction of unauthorized personnel and material.

- **Unsealing International Container Arrivals:**
  The sealing of containers and the continued integrity of the seal throughout the entire international trip are crucial elements of a secure supply chain. Consequently, arriving international container seals must be inspected for damage or tampering. The inspection must be documented, and the document signed by the person conducting the inspection. Kingchem must be notified immediately if the seal is damaged, appears to have been tampered with, is missing, or the seal

numbers do not match the number provided by Kingchem on the advance shipment notice (a.k.a. expected receipts order, etc.). This is critical.

Container and Trailer Seals: Import and Export
The sealing of trailers and containers, to include continuous seal integrity, are crucial elements of a secure supply chain. Any warehouse responsible for loading containers or trailers for import to, or export from, the United States must ensure that all seals meet or exceed the current PAS ISO 17712 standards for high security seals.

Written procedures must stipulate how seals are to be controlled and affixed to loaded containers and trailers, to include procedures for recognizing and reporting compromised seals and/or containers/trailers to Kingchem, the US Customs and Border Protection agency or the appropriate foreign authority. Only designated employees should have access to and distribute seals.

- **Container and Trailer Storage**
  Containers and trailers under warehouse control must be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures must be in place for reporting and neutralizing unauthorized entry into containers/trailers or container/trailer storage areas.

Physical Access Controls

Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets. Access controls must include the positive identification of all employees, visitors, and vendors at all points of entry.

- **Employee Badges**
  For facilities of over 50 employees, an employee identification system must be in place for positive identification and access control purposes. Company management or security personnel must adequately control the issuance and removal of employee, visitor, and vendor identification badges.

- **Employee Access**
  Employees should also only be given access to those secure areas needed for the performance of their duties. Procedures for the issuance, removal, and changing of access devices (e.g. keys, key cards, etc.) must be documented.

- **Visitor Controls**
  Upon arrival, visitors must present photo identification for documentation purposes. All visitors should be escorted and visibly display temporary identification.

- **Deliveries and Vendor Access**
  Upon arrival, vendor ID and/or photo identification must be presented for documentation purposes by all vendors.

- **Challenging and Removing Unauthorized Persons**
  Procedures must be in place to identify, challenge, and address unauthorized/unidentified persons.

Personnel Security

Processes must be in place to screen prospective employees and to periodically check current employees. Maintain a current permanent employee list (foreign and domestic), which includes the name, date of birth, national identification number or social security number, and position held, and submit such information to CBP upon written request, to the extent permitted by law.

- **Pre-Employment Verification**
  Application information, such as employment history and references, must be verified prior to employment.

- **Background checks / investigations**
  Consistent with foreign, federal, state and local regulations, background checks and investigations should be conducted for prospective employees.

  Employee background screening should include verification of the employee's identity and criminal history that encompass City, State, Provincial, and Country databases. Employers should factor in the results of background checks, as permitted by local statutes, in making hiring decisions. Background checks are not limited to verification of identity and criminal records. In areas of greater risk, it may warrant more in-depth investigations.

  Periodic checks and reinvestigations should be performed based on cause and/or the sensitivity of the employee's position.

- **Personnel Termination Procedures**
  Companies must have procedures in place to remove identification, facility and system access and other equipment from terminated employees. The distribution and retrieval of such should be recorded in the employee's Human Resources file.

Procedural Security

Security measures must be in place to ensure the integrity and security of processes relevant to the transportation, handling, and storage of cargo in the supply chain.

- **Documentation Processing**
  Procedures must be in place to ensure that all documentation used in the clearing of merchandise/cargo is legible, complete, accurate, and securely protected against the exchange, loss, or introduction of erroneous information. Documentation control must include safeguarding computer access and information.

Relevant personnel must be trained on how to identify information in shipping documents, such as manifests, that might indicate a suspicious shipment.

Based on risk, document handlers should consider key warning indicators for money laundering and terrorism financing activities most applicable to the functions that they and/or their business entities perform in the supply chain.

- **Manifesting Procedures**
  To help ensure the integrity of cargo received from abroad, procedures must be in place to ensure that information received from business partners is reported accurately and in a timely manner.

- **Cargo Discrepancies**
  All shortages, overages, and other significant discrepancies or anomalies must be resolved and/or investigated appropriately. CBP and/or other appropriate law enforcement agencies must be notified if illegal or suspicious activities are detected.

Security Training and Threat Awareness

Employees who understand why security measures are in place are more likely to adhere to them. One of the key aspects of a security program is training. A threat awareness program should be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists and criminals at each point in the supply chain. Through training, employees must be made aware of the procedures the company has in place to address a situation and how to report it.

- Personnel must receive training on situational reporting, that is, the procedures to follow if something is found during a conveyance inspection or if a security incident takes place.

- Members must retain evidence of all training through training logs, sign in sheets (roster), or electronic training records. Training records should include the date of the training, names of attendees, and the topics of the training.

- Additional training should be provided to employees in sensitive areas.

- Additionally, specific training should be offered to assist employees in recognizing internal conspiracies and protecting access controls. These programs should offer incentives for active employee participation.

Physical Security

All cargo handling and storage facilities, including trailer yards and offices must have physical barriers and/or deterrents that prevent unauthorized access.

Warehouses should incorporate the following CTPAT physical security guidelines throughout their facilities as applicable:

- **Fencing**
  Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo.

- **Gates and Gate Houses**
  Gates through which vehicles and/or personnel enter or exit must be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety.

- **Parking**
  Private passenger vehicles should be prohibited from parking in, or adjacent to, cargo handling and storage areas.

- **Building Structure**
  Buildings must be constructed of materials that resist unlawful entry. The integrity of structures must be maintained by documented, periodic inspection and repair.

- **Locking Devices and Key Controls**
  All external and internal windows, gates, and fences must be secured with locking devices. Management or security personnel must control the issuance of all locks and keys.

- **Lighting**
  Adequate lighting must be provided inside and outside the facility including the following areas: entrances and exits, fence lines and parking areas.

- **Alarms Systems & Video Surveillance Cameras**
  Security technology should be used to monitor premises and prevent unauthorized access to sensitive areas. Alarm systems and video surveillance cameras should be used to monitor premises and prevent unauthorized cargo handling and storage areas.

  Members who rely on security technology for physical security must have written policies and procedures governing the use, maintenance, and protection of this technology. At a minimum, these policies and procedures must stipulate:

  - That access to the locations where the technology is controlled or managed is limited to authorized personnel.
  - The procedures that have been implemented to test/inspect the technology on a regular basis.
  - That the inspections include verifications that all of the equipment is working properly, and if applicable, that the equipment is positioned correctly.
  - That the results of the inspections and performance testing is documented.
  - That if corrective actions are necessary, they are to be implemented as soon as possible and the corrective actions are documented.
  - That the documented results of these inspections be maintained for a

sufficient time for audit purposes.

- If a third-party central monitoring station (off-site) is used, the warehouse operator must have written procedures stipulating critical systems functionality and authentication protocols such as (but not limited to) security code changes, adding or subtracting authorized personnel, password revisions, and systems access or denials.
- Security technology policies and procedures must be reviewed and updated annually, or more frequently, as risk or circumstances dictate.
- All security technology infrastructure must be physically secured from unauthorized access.
- Security technology systems should be configured with an alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power.
- If camera systems are deployed, cameras should monitor a facility's premises and sensitive areas to deter unauthorized access. Alarms should be used to alert a company to unauthorized access into sensitive areas.
- If camera systems are deployed, cameras should have an alarm/notification feature, which would signal a "failure to operate/record" condition.

- **Security Guards**
  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.

- **Building & Facilities Inspections**
  Written standard operational procedures (SOPs) should exist requiring regular, documented inspections of building structure, perimeter barriers, fencing, gates, lights, CCTV systems, alarms, locks, windows and doors.

Cybersecurity

CTPAT Members must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual Cybersecurity criteria below. Information Technology (IT) integrity must be maintained at all times to protect data from unauthorized access or manipulation.

- **Network Protection**
  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 Members' computer systems. Members must ensure that their security software is current and receives regular security updates. Members must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or another unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.

- **Testing**
  CTPAT Members using network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.

- **User Access**
  User access must be restricted based on job description or assigned duties. Individuals with access to Information Technology (IT) systems must use individually assigned accounts. 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.

- **Accountability & Identification of Abuse**
  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

- **Password Protection**
  Automated systems must use individually assigned accounts that require a periodic change of password. IT security policies, procedures, and standards must be in place and training provided to employees. 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. Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists.

- **VPNs**
  Members that allow their users to remotely connect to a network must employ secure technologies such as virtual private networks (VPNs) or multi-factor authentication (MFA) to allow employees to access the company’s intranet securely when located outside of the office. Members must also have procedures designed to prevent remote access from unauthorized users.

- **Data**
  Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.

Trade-Based Money Laundering

Trade-Based Money Laundering occurs when criminals use the international trade system to disguise illicit proceeds by altering Customs and banking paperwork to make transactions appear legitimate. These proceeds are then used to finance additional criminal activity, which may include funding terrorist activities or organizations.

CTPAT Members and their business partners must have a written, risk-based process for

screening new business partners and for monitoring current partners. A factor that Members should include in this process is checks on activity related to money laundering and criminal funding as there is a marked overlap between the two. Specialized training should be provided annually to personnel who may be able to identify the warning indicators of Trade-Based Money Laundering and Terrorism Financing (examples of personnel who should receive this training include those responsible for trade compliance, security, procurement,
finance, shipping, and receiving).

To assist with this process, please consult, for example, the document *CTPAT's Warning Indicators for Trade-Based Money Laundering and Terrorism Financing Activities*, as found on the Kingchem Life Science web site or as provided on the internet by the CBP

The following are examples of some of the vetting elements that can help determine if a company is legitimate:

- Verifying the company's business address and how long they have been at that address.
- Conducting research on the internet on both the company and its principals.
- Checking business references.
- Requesting a credit report.

Upper Management Responsibility

The role of a company's upper management in security procedures is to provide support and oversight to ensure the creation and maintenance of the company's Supply Chain Security Program. To this end, the designated company head of security or security coordinator should provide regular updates regarding the progress or outcomes of any audits, exercises, or validations to upper management.

To promote a culture of security, a letter of commitment to comprehensive supply-chain security should be signed by a senior company official and displayed in appropriate company locations.

Wood Packaging Materials, Pallets (Agricultural Procedures)

Visible pest contamination is to include compliance with Wood Packaging Materials (WPM) regulations. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). This is a firm requirement of the CBP's CTPAT program as visible pest prevention measures <u>must</u> be adhered to throughout the supply chain.

[end document]

For more information:	Please contact Kingchem Life Science at email address: customer-service@kingchem.com
Document:	Warehouse Operators Security Procedures Guidelines
Issue Date:	2020-05-13
Source:	https://www.kingchem.com/beyond-the-chemistry/ctpat/