## BRANCH HOANG THONG WOOD ONE MEMBER COMPANY LIMITED

Block 2D3-2D4, CN3-CN8-CN10 Street, Tan Binh Industrial Park, Tan Binh Ward, Tan Uyen District, Tan Binh Ward, Binh Duong Province, Vietnam 820000 (+84) 333 880 338

# SCAN SUPPLY CHAIN SECURITY AUDIT (YEAR 2 SELF AUDIT)

| | |
|---|---|
| Report # | SAC-2026-07-0625-CAPA-V2 |
| Audit Submitted | Jul 23, 2026 |
| Compliance Score | 99% |
| Audit Type | SELF AUDIT |
| Audit Status | Reviewed |
| Audit Expiration Date | Jul 22, 2027 |

## Location Information

### Branch Hoang Thong Wood One Member Company Limited

Block 2D3-2D4, CN3-CN8-CN10 Street, Tan Binh Industrial Park, Tan Binh Ward, Tan Uyen District, Tan Binh Ward, Binh Duong Province, Vietnam 820000 (+84) 333 880 338

| | |
|---|---|
| SCAN ID | VN67979K35HO |
| Point of Contact Name | Alex Nguyen |
| Point of Contact Email | thien.nguyen@furniturehth.com |

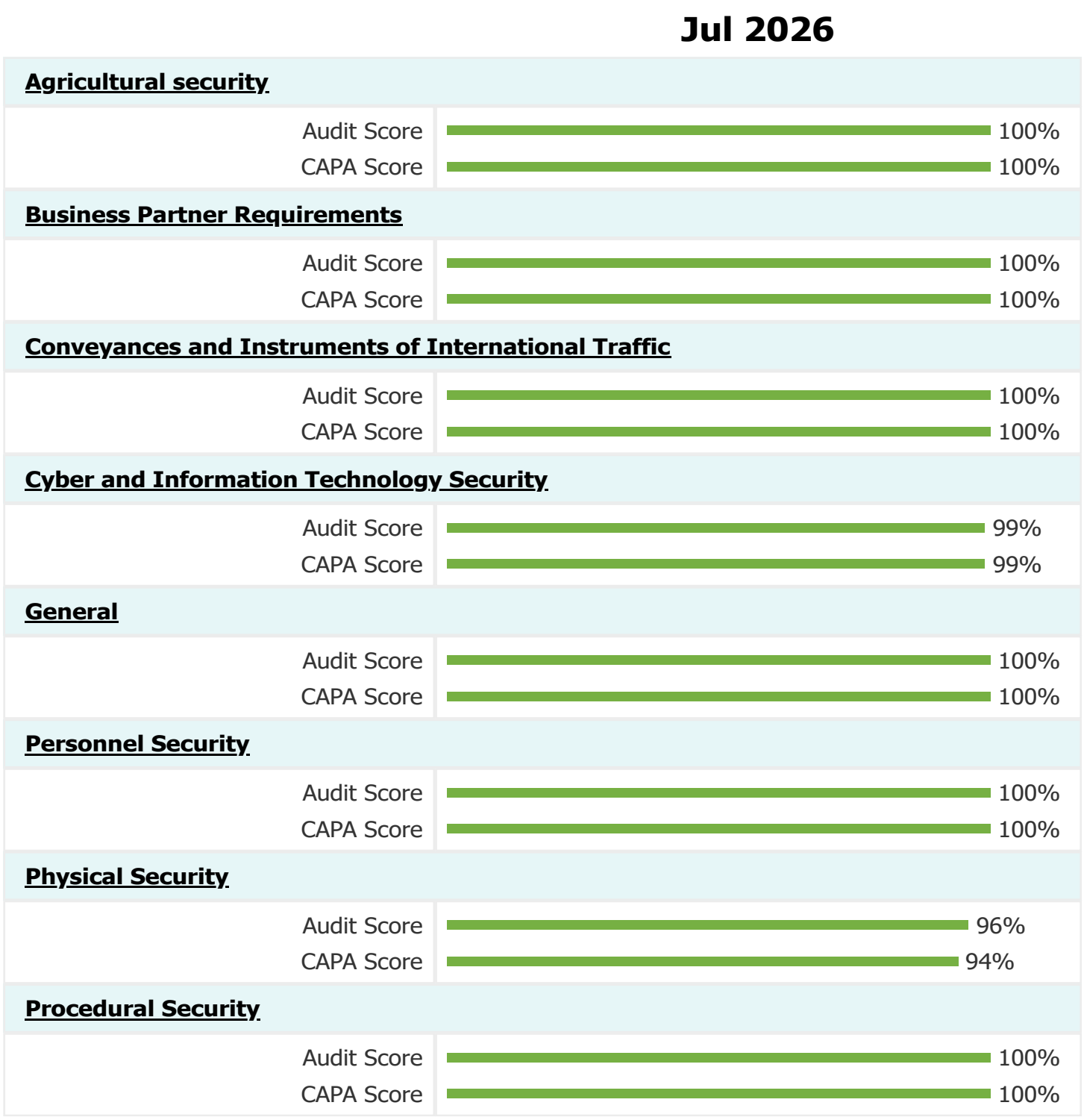
| Contact Name | Phone | Email |
|---|---|---|
| | | Compliance@LivingStyle.com |

| | |
|---|---|
| Location | Branch Hoang Thong Wood One Member Company Limited |
| Primary Location | Yes |
| Critical Location | No |
| Assigned Auditor | *Not provided* |
| Schedule Date | Unscheduled |

## Audit Summary

| | Submitted Date | Compliance Score |
|---|---|---|
| **Pre-CAPA** | Jul 23, 2026 | 99% |
| **Post-CAPA** | Jul 29, 2026 | 99% |

### Compliance by Category



## Risk Assessment

| | |
|---|---|
| Audit Score | 100% |
| CAPA Score | 100% |

## Seal Security

| | |
|---|---|
| Audit Score | 100% |
| CAPA Score | 100% |

## Security Training & Threat Awareness

| | |
|---|---|
| Audit Score | 100% |
| CAPA Score | 100% |

## Pre CAPA Correct and Incorrect Response Count

| ClassificationType | Total | CorrectResponses | | IncorrectResponses | |
|---|---|---|---|---|---|
| | | Scored | NonScored | Scored | NonScored |
| **Total** | **131** | **129** | **0** | **2** | **0** |
| Critical | 33 | 32 | 0 | 1 | 0 |
| Material | 32 | 32 | 0 | 0 | 0 |
| Must | 66 | 65 | 0 | 1 | 0 |

## Business Profile Information

| | |
|---|---|
| Does the facility participate in any government, local customs, or World Customs Organization (WCO) accredited facility security programs? | No |
| Does the facility hold a Government Supply Chain Security Certification? | No |
| Has the facility been reviewed or audited by this program? | Yes |
| Primary Industry of Operations | Furniture |
| Product Type / Commodity | Tables, Beds, wardrobes |
| Year Established | 2018 |
| Grounds Size (Square Meters) | 54000 |
| Number of Buildings | 2 |
| Were all buildings included in audit? If not, please explain which buildings were not included and why. | Yes |
| Facility Size (Square Meters) | 30648.86 |
| Number of access points? (i.e. gates, exterior doors) | 1 |
| Hours of Operation | 7:30am- 16:30pm |
| Number of Employees | 101 - 500 |
| Number of Contract Employees | 486 |
| Number of Inhouse Security Guards | 0 |
| Number of Contract Security Guards | 4 |
| Number of Migrant Workers | 0 |
| Annual Revenue | 10 - 50 Million |
| Does the facility outsource any manufacturing services? | No |
| If yes to outsourcing any manufacturing services, please describe services outsourced and country location. | No |
| What countries does this facility export to? | USA, Australia, Canada |
| Identify affiliate locations where any work is conducted or product stored. | No |
| Does the facility outsource any transportation services? | Yes |

| Company Name | Contact Email | Contact Email | Percentage of time |
|---|---|---|---|
| CÔNG TY TNHH XUẤT NHẬP KHẨU LÊ PHAN | Le Khanh Linh | lephan.ops@nhl.vn | 100 |

| | |
|---|---|
| Does this facility partner with any sales agent or vendor representatives? | No |
| Enter location address as it appears on the business license for this location. | Lot 2D3, 2D4, CN3, CN8 and CN10 Streets, Tan Binh Industrial Park, Vinh Tan Ward, Ho Chi Minh City, Vietnam |
| Name of onsite Factory Representative (First and Last Name) and email address | Alex Nguyen |
| Factory Representative Email Address | thien.nguyen@furniturehth.com |

## Audit Responses

| Audit Assigned | Due Date | Overall Compliance Score |
|---|---|---|
| **Jul 15, 2026** | **Aug 14, 2026** | **99%** |

### General — 100%

1 None Does the Business License match the current location name and address as listed on the audit sheet? Please attach photo of Business License.

**Question Guidance:** Verification of the Business License information is required. If the license does not match, please attach current scanned copy or picture of the facility's Business License. Any differences must be documented. A copy of the business license needs to be attached. When reviewing the address information and comparing to the address in the Audit Template, it is acceptable if the Audit Template address is more specific, but the main address must be similar to the address on the Business License. (i.e. if there are specific buildings referenced in the Audit Template, but the main address is the same, this would be considered a match)

- (●) Yes
- ( ) No

PDF GPKD Chi Nhánh.pdf

**Comments:** *No comments were provided*

2 Must Is there a primary point of contact (POC) identified regarding security matters?

**Question Guidance:** A primary point of contact (POC) regarding security matters must be identified. The security point of contact can be the same or different than the primary point of contact for business issues. Provide in the comments the first and last name of the POC, their business phone or mobile phone number, and email contact information. (POC must be knowledgeable about CTPAT program requirements)
(CTPAT MSC 1.4)

- (●) Yes - Provide the name, phone number and email address of the POC
- ( ) No

**Comments:** Alex Nguyen- phone number: +84 969893529-email: thien.nguyen@furniturehth.com

3 Critical Has the audited location recently (within the last 12 months) completed the included SCAN Factory and Supplier Training online training module?

**Question Guidance:** Ask leadership if they participated in this training within the last 12 months. If yes, obtain and upload a copy of the provided certificate and list how many employees participated along with their job positions/work areas.

- (●) Yes - Please attach photo of training certificate
- ( ) No

Chứng nhân hoc.jpg

**Comments:** Mr. Vu Quang Vo

4 Material Has there been a Social Compliance or Responsible Sourcing Audit completed at this location in the last 24 months that addresses the facility's employment practices?

**Question Guidance:** Auditor may only view (not retain) a copy of the facility's audit report and notate the following information: Audit date and Audit score / rating.

*Do not upload any images or attachments

(CTPAT MSC 3.9)

- (●) Yes - Please provide audit date and audit score / rating
- ( ) No - Audit Report on file is older than 24 months
- ( ) Never conducted/no record on file

**Comments:** Smeta 4P: SGS audit, date : 14/March, 2026

5 Material Does the facility have a documented social compliance program?

**Question Guidance:** A social compliance program is a set of policies and practices through which a company seeks to ensure maximum adherence to the elements of its code of conduct that cover social and labor issues. Social compliance refers to how a business addresses its responsibilities in protecting the environment, as well as the health, safety, and rights of its employees, the communities in which they operate, and the lives and communities of workers along their supply chains.

(CTPAT MSC 3.9)

- (●) Yes
- ( ) No

**Comments:** Factory had a social compliance program to ensure maximum adherence to the elements of its code of conduct that cover social and labor issues

**Risk Assessment** 100%

6 Must Does the facility conduct and document a risk assessment of their supply chain, including security vulnerabilities related to policy and procedure adherence, as well as identifying any potential geographical threats?

**Question Guidance:** Facility must have a risk assessment that identifies and addresses any vulnerabilities in their supply chain/processes. It must include facility's own security practices, any business partner(s)/supplier(s) vetting and security practices, and all the vulnerabilities that may create issues/challenges that could prevent completion of business contracts. Examples of risks include labor shortages, weather concerns such as frequent typhoons, unreliable utilities, and criminal or terrorist activity, etc. Auditor to review the risk assessment and/or a business continuity plan.
(CTPAT MSC 2.1)

- (●) Yes - Example of completed risk assessment reviewed
- ( ) No - Examples were not able to be provided / risk assessments are not conducted

**Comments:** Facility had a risk assessment that identifies and addresses any vulnerabilities in their supply chain/processes.

7 Must Is the facility risk assessment shared with business partners and contractors?

**Question Guidance:** Facility must share risk assessment with business partners and contractors. Sharing risk assessments allows business partners to know and improve upon vulnerabilities, and enhances business continuity. Auditor to request a list of primary vendors and suppliers that should be provided a copy of the facility risk assessment and whom should be consulted on developing a risk assessment/business continuity plan.

- (●) Yes
- ( ) No - Assessment is not shared
- ( ) No risk assessment is conducted

**Comments:** *No comments were provided*

8 Material Does the facility risk assessment include vulnerabilities specific to contractors, seasonal employees, service providers etc.?

**Question Guidance:** Risk Assessments should capture any risks associated with business partners, contractors, and any lessons learned from incidents, business disruptions, etc. Auditor to review the risk assessment to determine if critical business partner's vulnerabilities are

included. This is a best practice and is encouraged.

(CTPAT MSC 2.2)

- (●) Yes
- ( ) No - Specific vulnerabilities not included
- ( ) No risk assessment is conducted

**Comments:** *No comments were provided*

9 Must Is the facility risk assessment updated periodically?

**Question Guidance:** The risk assessment must be documented and updated every year, at a minimum, or more frequently as risks dictate. Auditor to review the date of creation or last review/update that should appear on the risk assessment/business continuity document. Auditor should question factory management on what would trigger an update.

(CTPAT MSC 2.3)

- (●) Last update within the past 12 months
- ( ) Last update between 12 months and 18 months
- ( ) Last update between 18 months and 24 months
- ( ) No updates noted or last update greater than 24 months ago
- ( ) No risk assessment is conducted

**Comments:** *No comments were provided*

10 Material Does the facility have an implemented process for cargo movement management? (Select all that apply)

Only select NA if the cargo movement is not managed or facilitated by the facility.

**Question Guidance:** Facilities should include cargo maps in their risk assessment to document the movement of all cargo associated with the facility. Besides identifying risks, the cargo map should serve to find areas where a supply chain is at risk. Cargo mapping should include how cargo moves in and out of the facility and note when/if cargo is "at rest". Auditor to review document that highlights the cargo map and includes points of transfer, transit times and potential points where freight may be at rest, thus at risk. This is a best practice and is encouraged. NA is only to be used if the facility does not manage any of the cargo movement activities. Please explain in the comments.

(CTPAT MSC 2.2)

- [x] A documented cargo process is available
- [x] The cargo process includes transit times from origin to final Instrument of International Traffic (IIT) yard
- [x] The cargo process includes locations where freight may be at rest
- [x] Implemented cargo process maps are available for review
- [ ] No documented cargo management process is available
- [ ] NA

**Comments:** *No comments were provided*

11 Material Define the facility's crisis plan. (Select all that apply)

**Question Guidance:** Otherwise known as a business continuity plan. A crisis can be a disruption of the movement of trade data due to a cyber attack, a fire or a carrier driver being hijacked. Based on your risk, a crisis plan should include any additional security measures that are taken when a crisis happens. This should include how you communicate a crisis to business partners and importers. This is a best practice and is encouraged. Auditor to review the facility's crisis plan and ensure it includes: types of crises and how the facility would respond, communication to business partners of crisis related issues, and potential alternative locations if facility is rendered unusable.

(CTPAT MSC 2.4)

- [x] Documented crisis plan available
- [x] Crisis plan includes reporting crisis-related issues to business partners as necessary
- [x] Crisis plan includes alternative locations if facility is rendered unusable
- [ ] No documented crisis plan available

**Comments:** *No comments were provided*

12 Material To ensure a robust supply chain security program, has the facility incorporated representatives from all of the relevant departments into a cross-functional team?

**Question Guidance:** Examples of departments that should be included: representatives from Human Resources, Information Technology, Import/Export offices, Shipping, receiving, warehouse, security operations and senior leadership.

(CTPAT MSC 1.2)

- (●) Yes
- ( ) No

**Comments:** The factory has established a Security Committee, comprising representatives from key departments: Human Resources, Information Technology, Import-Export, Shipping & Receiving, Warehousing, Security Operations, and Senior Management.

## Business Partner Requirements 100%

13 None Does the facility contract services such as security, transportation or manufacturing labor?

**Question Guidance:** (CTPAT MSC 3.5)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

14 Must Does the facility review and provide copies of security criteria to business partners, particularly those that support international supply chain activities?

**Question Guidance:** Copies of security criteria must be reviewed and provided to business partners and must clearly state what actions are acceptable and unacceptable regarding the production and transportation of goods. Proof of review (date, time, name(s), business partner type, topics reviewed) should be maintained by the facility. Auditor to question the facility staff to understand how these requirements are communicated and shared with business partners involved in the international supply chain. In addition, in the situation that the country has its own language along with English as the business language, and all documentations are in English, the auditor should also verify during the audit if the facility staff can understand English or not, then provide a proper selection for this question.

- (●) Yes - Security criteria reviewed and provided in local language
- ( ) Yes - Security criteria reviewed and provided in English only
- ( ) Yes - Security criteria is reviewed but not provided to business partners
- ( ) No - Security criteria is not reviewed with all business partners

**Comments:** *No comments were provided*

15 Must Does the facility have documented procedures used in the selection of business partners including: material suppliers, manufacturers, and logistics service providers? (Select all that apply)

**Question Guidance:** Facilities must have a documented, risk-based process on how new business partners are selected and current business partners are screened annually. The process must include detailed screening criteria, including: preventing money laundering and terrorism

funding, financial stability, security training, verifying company's business address and length of time at address. The policy must be shown to the auditor. Auditor to determine if the screening and selection process includes verifying the business profile, financial status, ability to accomplish the requirement of the proposed business, and standards for employee hiring and security training. Examples of business partners that need to be screened are direct business partners such as manufacturers, suppliers, service providers, and logistics providers. How in-depth to make the screening depends on the level of risk in the supply chain.
(CTPAT MSC 3.1, 3.4)

- [x] Documented screening process is available
- [x] Screening process is done on an annual basis
- [x] Screening process includes looking for evidence of money laundering and terrorism funding
- [x] Screening process includes monitoring for financial stability
- [x] Screening process checks for CTPAT / AEO status
- [ ] No screening process takes place

**Comments:** *No comments were provided*

16 Must Are the facility's contracted business partners required to conduct an annual security risk assessment of their operations?

**Question Guidance:** Contracted partners must conduct their own security risk assessment annually and provide their results to the facility. Facility should be able to provide proof of annual assessment received from business partners. Auditor to review a business partner contract and determine if an annual risk assessment is required and completed.
(CTPAT MSC 2.3, 3.5, 3.7)

- (●) Yes - Annually
- ( ) Yes - Every 2 years
- ( ) Yes - At time of contract initiation only
- ( ) No

**Comments:** *No comments were provided*

17 Must Does the facility require business partners to provide a signed compliance statement or complete a questionnaire highlighting CTPAT Minimum Security Requirements that are in place? Is the statement or questionnaire renewed annually? (Select all that apply)

**Question Guidance:** Facilities that outsource services must assess their business partners' security practices annually, using either a security questionnaire or a signed compliance statement aligned with the facility's risk assessment. As part of this evaluation, the auditor should request to see a signed agreement between the facility and its business partners confirming their commitment to meet or exceed the facility's security requirements. Alternatively, a spreadsheet documenting business partner acknowledgments is also acceptable evidence. Regularly reviewing these security assessments is essential to confirm that each business partner maintains an effective security program. Without periodic updates, the facility may remain unaware of any deterioration in a partner's security practices—potentially exposing the supply chain to increased risk.
(CTPAT MSC 3.5, 3.7)

- [x] Signed compliance statement or security questionnaire required
- [x] Renewed annually
- [ ] No - Nothing available / required

**Comments:** *No comments were provided*

18 Must If a security questionnaire is provided, and there are areas of non-compliance found on the questionnaire, does the facility require corrective action plans from the business partner with evidence of implementation?

Select NA if a Signed Compliance Statement is used in place of a Questionnaire.

**Question Guidance:** If the facility uses a security questionnaire to evaluate business partners and identifies areas of non-compliance, it must require the submission of corrective action plans (CAPs) from those partners. These CAPs must include evidence of implementation along with completion dates.
- The facility must also maintain a documented process outlining how these questionnaires are:
- Reviewed for completeness and accuracy
- Validated against the facility's minimum security requirements
- Recorded and stored for reference and audit purposes
Auditors should engage with management to understand how CAPs are monitored and verified to ensure that all required security standards are met and maintained.
(CTPAT MSC 3.6)

- (●) Yes
- ( ) No
- ( ) NA

**Comments:** *No comments were provided*

## Cyber and Information Technology Security 99%

19 None Does this facility have internet and computer network systems?

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

20 Must Does the facility have a documented policy and procedure manual that covers all the areas necessary for a comprehensive Cyber Security / Information Security program?

The documented IT policy, at a minimum, must cover all of the individual Cyber Security criteria in this Cyber and Information Technology Security audit section.

**Question Guidance:** Facilities are required to maintain comprehensive, documented cybersecurity policies and procedures that protect their IT systems. These policies must, at a minimum, address all individual cybersecurity criteria outlined in this audit section. It is strongly recommended that facilities align their cybersecurity practices with recognized industry frameworks—such as those provided by the National Institute of Standards and Technology (NIST). NIST's guidance supports organizations in managing and reducing cybersecurity risks and can complement an existing risk management program. For facilities without an existing cybersecurity framework, the NIST Framework serves as a reliable foundation for developing one.

(CTPAT MSC 4.1)

- (●) All Areas are Documented
- ( ) 1 Area is missing
- ( ) 2 - 3 Areas are missing
- ( ) More than 3 areas are missing
- ( ) There are no documented policies or procedures in place

**Comments:** *No comments were provided*

21 Must Does the facility have a documented cyber security policy to protect information technology systems that is reviewed and updated annually?

**Question Guidance:** Facilities must have a comprehensive, documented cybersecurity policy that lists steps to protect IT systems, and identify and resolve threats. Policy must be reviewed and updated annually at a minimum. 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.

(CTPAT MSC 4.2, 4.6)

- (●) Policy is documented and was updated within the past 12 months
- ( ) Policy is documented and was updated within the past 12-18 months
- ( ) Policy is documented but last update was greater than 18 months ago
- ( ) No documented policy is available

**Comments:** *No comments were provided*

22 Must Does the facility have firewall and anti-malware software installed to identify, protect, detect, respond and recover their network? (Select all that apply)

**Question Guidance:** Protection must include use and management of firewall and malware software. To defend Information Technology (IT) systems against common cybersecurity threats, the facility must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in facility's computer systems. This must be addressed in the question above that references the documented policy and procedure documentation collection.

(CTPAT MSC 4.2)

- [x] Firewall deployed
- [x] Anti-malware software installed
- [ ] No firewall or anti-malware software deployed

**Comments:** *No comments were provided*

23 Must How frequently are updates performed on firewall and malware software?

**Question Guidance:** In order to maintain your firewall and malware, it is important to update your software when enhancements are made by the providers. Factories must ensure that their security software is current and receives regular security updates. This must be addressed in the question above that references the documented policy and procedure documentation collection.

Note: it is not necessary to share exact dates of updates.

(CTPAT MSC 4.2)

- ○ Software updates are automatically deployed from the software providers
- ◉ Manual updates installed by on site IT services as needed
- ○ No updating is performed
- ○ No firewall or anti-malware software deployed

**Comments:** *No comments were provided*

24 Must Does the facility have a documented procedure to prevent attacks via social engineering?

**Question Guidance:** This must be addressed in the question above that references the documented policy and procedure documentation collection. Definition of social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

(CTPAT MSC 4.2)

- ◉ Yes
- ○ No

**Comments:** *No comments were provided*

25 Must If a data breach occurs or another unseen event results in the loss of data and/or equipment, does the facility have procedures to include the recovery (or replacement) of IT systems and/or data?

**Question Guidance:** This must be addressed in the question above that references the documented policy and procedure documentation collection.

(CTPAT MSC 4.2)

- ◉ Yes
- ○ No

**Comments:** *No comments were provided*

26 Must Are test scenarios conducted at least annually to identify open ports and IP addresses that create vulnerable access to the internal network?

**Question Guidance:** IT infrastructure must be tested regularly to identify vulnerabilities to a facility's internal network. A documented IT process should include which personnel should be conducting these tests as well as frequency. This must be addressed in the question above that

references the documented policy and procedure documentation collection.
(CTPAT MSC 4.3)

- (●) Vulnerability tests are conducted by IT personnel at least annually
- ( ) No vulnerability tests are conducted

**Comments:** *No comments were provided*

27 Must Are corrective actions taken when problems are identified while testing firewall, malware, and other network vulnerabilities? Please explain how problems would be addressed.

**Question Guidance:** The IT procedure should communicate what to do when problems are identified. A secure computer network is of paramount importance to a business, and ensuring that it is protected requires testing on a regular basis. This can be done by scheduling vulnerability scans. Just like a security guard checks for open doors and windows at a business, a vulnerability scan (VS) identifies openings on your computers (open ports and IP addresses), their operating systems, and software through which a hacker could gain access to the company's IT system. The frequency of the testing will depend on various factors including the company's business model and level of risk. This must be addressed in the question above that references the documented policy and procedure documentation collection.
(CTPAT MSC 4.3)

- (●) Yes
- ( ) No
- ( ) No vulnerability tests are conducted

**Comments:** When vulnerabilities or issues are identified during testing (e.g., firewall audits, malware scans, or network penetration tests), the factory follows a structured Corrective Action procedure to address them effectively:

Risk Identification & Assessment:
Upon receiving test results, the IT/Security team immediately logs and categorizes identified vulnerabilities based on their severity levels (Critical, High, Medium, Low).

Root Cause Analysis (RCA):
The IT team conducts a root cause analysis to determine why the vulnerability occurred (e.g., outdated software patches, misconfigured firewall rules, or lack of system updates).

Remediation & Patching:

Critical / High risks: Addressed within 24–48 hours by applying system patches, updating malware signatures, or revising firewall access policies.

Medium / Low risks: Scheduled for correction within a defined timeframe (e.g., 7–14 days).

Re-testing & Verification:
Once corrective actions are applied, the team re-runs the vulnerability scans or testing protocols to verify that the issue is completely resolved and no new risks were introduced.

Documentation & Reporting:
All findings, corrective actions taken, and re-test verification logs are documented and submitted to Senior Management for final review and approval.

28 Material To whom does the facility report cybersecurity threats and attempts at unapproved access to network systems? (Select all that apply)

**Question Guidance:** Employees must know how to identify and report cybersecurity incidents, including: What to report, Who to report an incident to, How to report, and How to resolve an incident, if applicable. External business partners includes customers, suppliers, logistics, etc. This is a best practice and is encouraged that this should be addressed in the question above that references the documented policy and procedure documentation collection. Factories are encouraged to share information on cybersecurity threats with the government and business partners within their supply chain.
(CTPAT MSC 4.4)

- [x] Senior management
- [x] Internal business partners
- [x] External business partners
- [x] Government agencies
- [ ] No reporting process and procedure in place

**Comments:** *No comments were provided*

29 Must Are automated systems in place to monitor and prevent attempts of unauthorized access and tampering with systems and/or electronic data?

**Question Guidance:** An organization typically uses an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) to identify unauthorized access to IT systems and data.

This must be addressed in the question above that references the documented policy and procedure documentation collection.
(CTPAT MSC 4.5)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

30 Must Is disciplinary action taken against anyone identified violating IT systems policies and procedures?

**Question Guidance:** This must be addressed in the question above that references the documented policy and procedure documentation collection.
(CTPAT MSC 4.5)

- (●) Yes
- ( ) No

**Comments:** Upon detecting a breach (e.g., unauthorized system access, sharing login credentials, disabling security controls, or downloading unauthorized software), the IT/Security team will document the incident and report it to Human Resources (HR) and senior management for handling according to company policy.

31 Must Does management regularly review the users who have network access in order to restrict access to only those applications required to perform current job requirements?

**Question Guidance:** Management must review employee access 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. This process must be documented with a defined frequency for management reviews. This must be addressed in the question above that references the documented policy and procedure documentation collection.
(CTPAT MSC 4.7)

- (●) Management reviews monthly
- ( ) Management reviews quarterly
- ( ) Management reviews annually
- ( ) No management review conducted

**Comments:** *No comments were provided*

32 Must Is there a documented procedure to remove network access for employees who are terminated or on leave longer than vacation?

**Question Guidance:** Documented procedures must be in place that include when and how to remove network access for employees who are terminated or on leave for an extended period of time. Procedures should include when to grant access back to employees who come back from extended leave and/or suspension. Procedures should state how and who to notify to grant access. This must be addressed in the question above that references the documented policy and procedure documentation collection.

(CTPAT MSC 4.7)

- (●) Yes, the documented process includes long term leave and terminated employee's access removal
- ( ) Yes, the documented process is available, but it does not include long term leave, only terminated employee's access removal
- ( ) No documented process was available for removing network access for terminated employees at the time of audit

**Comments:** *No comments were provided*

33 Must How is computer access managed at the factory?

**Question Guidance:** 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. This must be addressed in the question above that references the documented policy and procedure documentation collection.

(CTPAT MSC 4.8)

- (●) Passwords and or Passphrases
- ( ) Biometrics
- ( ) Electronic ID cards
- ( ) Multi- Factor Authentication (MFA)
- ( ) No credentials are required

**Comments:** *No comments were provided*

34 Must If passwords or passphrases are implemented, are they considered complex and changed periodically? (select all that apply)

Select NA if passwords or passphrases are not utilized.

**Question Guidance:** 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. This must be addressed in the question above that references the documented policy and procedure documentation collection.

(CTPAT MSC 4.8)

- [x] Passwords must be complex
- [x] Passwords are changed periodically
- [ ] No requirement of passwords being complex or changed out periodically
- [ ] NA

**Comments:** *No comments were provided*

35 Must Are workstations set up for individually assigned accounts?

**Question Guidance:** Individuals with access to Information Technology (IT) systems must use individually assigned accounts. This must be addressed in the question above that references the documented policy and procedure documentation collection.

(CTPAT MSC 4.8)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

36 Must If employees and/or contractors are permitted to access information technology (IT) systems remotely, is a virtual private network (VPN) or similar software used to control access?

**Question Guidance:** Facilities 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. Facilities 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. Multifactor 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. This must be addressed in the question above that references the documented policy and procedure documentation collection. (CTPAT MSC 4.9)

- ○ Remote access is permitted and VPN or similar software is used
- ○ Remote access is permitted but no VPN or similar software is used to control access
- ◉ Remote access is not permitted

**Comments:** *No comments were provided*

37 Must Do all cyber security policies apply to personal devices that connect to the network?

**Question Guidance:** All personal devices must adhere to the facility's cybersecurity policies and procedures to include regular security updates and a method to securely access the company's network. This must be documented in the facility's procedure. If Facilities 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. Personal devices include storage media like CDs, DVDs, and USB flash drives. Care must be taken if employees are allowed to connect their personal media to individual systems since these data storage devices may be infected with malware that could propagate using the company's network. This must be addressed in the question above that references the documented policy and procedure documentation collection. (CTPAT MSC 4.10)

- ○ All security policies apply to personal devices and the Facility does not permit personal devices to connect to the network without using a VPN or similar software
- ◉ Facility does not permit the use of any personal devices to access the network
- ○ All security policies apply to personal devices, but does not require VPN or similar software
- ○ Security policies do not apply to personal devices, personal devices are allowed to use on the facility's network

**Comments:** *No comments were provided*

38 Material Does IT security limit and monitor the downloading of software and access to external websites?

**Question Guidance:** This is a best practice and is encouraged that the IT policy includes measures to prevent the use of counterfeit technology products and how to limit access to non-internal sites. The facility may want to have a policy that requires product key labels and

certificates of authenticity to be kept when new media is purchased. CDs, DVDs, and USB media include holographic security features to help ensure you receive authentic products and to protect against counterfeiting. This is a best practice and is encouraged that this should be addressed in the question above that references the documented policy and procedure documentation collection.
(CTPAT MSC 4.11)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

39 Material How frequently is data backed up for this facility?

**Question Guidance:** Data backups should take place as data loss may affect individuals within an organization differently. Daily backups are also recommended in case production or shared servers are compromised/lose data. Individual systems may require less frequent backups, depending on what type of information is involved. This is a best practice and is encouraged that this should be addressed in the question above that references the documented policy and procedure documentation collection.
(CTPAT MSC 4.12)

- (●) Data is backed up daily
- ( ) Data is backed up weekly
- ( ) Data is backed up monthly
- ( ) No data backups are performed

**Comments:** *No comments were provided*

40 Material Is the data backup stored offsite and encrypted? (Select all that apply)

**Question Guidance:** Media used to store backups should preferably be stored at a facility offsite. Devices used for backing up data should not be on the same network as the one used for production work. Backing up data to a cloud is acceptable as an "offsite" facility. IT policy should include where data backup is located. This is a best practice and auditor should ask facility to provide proof of data backup storage location and encryption to confirm implementation. The data backup can be stored in a physical site outside of the facility, or in a cloud storage platform whose server is outside of the facility. This is a best practice and is encouraged that this should be addressed in the question above that references the

documented policy and procedure documentation collection.

(CTPAT MSC 4.12)

- [x] Data backup is stored offsite
- [x] Data backup is encrypted
- [ ] Data is not stored offsite nor encrypted
- [ ] No data backups are performed

**Comments:** *No comments were provided*

41 Must Is there a documented procedure to address returning equipment slated for disposal back to IT?

**Question Guidance:** IT policy must include addressing all IT equipment being returned back to the IT department for proper disposal and documentation as required. This must be addressed in the question above that references the documented policy and procedure documentation collection.

(CTPAT MSC 4.13)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

42 Must Is there a process to properly sanitize or destroy IT equipment in accordance with appropriate industry guidelines?

**Question Guidance:** 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. This must be addressed in the question above that references the documented policy and procedure documentation collection.

(CTPAT MSC 4.13)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

**Conveyances and Instruments of International Traffic** 100%

43 None Does the facility load Instruments of International Traffic (IIT)?

**Question Guidance:** Instruments of International Traffic (IIT) – IIT includes containers, trailers, flatbeds, unit load devices (ULDs), lift vans, cargo vans, shipping tanks, bins, skids, pallets, caul boards, cores for textile fabrics, or other specialized containers arriving (loaded or empty), in use or to be used in the shipment of merchandise in international trade. If the unit of transport is destined to a domestic CFS (Container Freight Station) location from this location's facility, the answer to this question should be "Yes" as it then would be considered an IIT.

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

44 Critical While in the facility's control, or in transit, are IIT stored in a secured manner whether on-site or off-site? (Select all that apply) Please attach photos of each applicable area.

**Question Guidance:** While in the facility's control, Instruments of International Traffic (IIT) must be stored in a designated, secured area regardless if the area is on- or off-site. The area must only be for empty and/or full IIT; no other vehicle parking or other storage allowed. All loaded IIT stored for any period of time must be closed and secured with a seal that meets requirements outlined in the seal security section. Multiple ways to secure the area are acceptable, such as perimeter fencing, gates, CCTV, perimeter alarms, lighting, security guards patrolling 24 hours x 7 days, etc. Other methods can be accepted if it is confirmed workable, factory should explain in details how IIT are secured. (Perimeter alarms are exterior perimeters of property, while anti intrusion alarms are for interior buildings) A documented procedure must indicate how the facility will follow requirements. Auditor should question personnel regarding how IIT are monitored during storage.
(CTPAT MSC 5.1, 7.1, 9.5)

- [x] IIT storage area is free from personal vehicle parking and any other storage
- [x] IIT storage area is secured and/ or monitored (please describe)
- [x] Stored, loaded IIT are secured with a seal
- [x] Documented procedure available for securing IIT while in facility's control
- [ ] IIT storage does not meet minimum security requirements (please describe)

Kv lưu cont.jpg

**Comments:** Instruments of International Traffic (IIT) must be stored in a designated, secured area regardless. All loaded IIT stored for any period of time must be closed by fencing, gates, CCTV, security guards patrolling 24 hours x 7 days, etc.

45 Critical Were you able to observe a IIT inspection in process or a previously completed IIT inspection via CCTV recordings?

**Question Guidance:** Prior to arrival at the audit site, advise the factory to be prepared to have the auditor observe an Instruments of International Traffic (IIT) loading live or plan to provide CCTV recording of a previously loaded IIT.

- (●) Yes
- ( ) No

**Comments:** The IIT inspection process is continuously monitored and verified via CCTV recording

46 Critical Is there a documented procedure in place to inspect the security integrity of an IIT prior to loading that includes all the minimal requirements?

**Question Guidance:** Review the policy that covers how Instruments of International Traffic (IIT) integrity is determined. Please attach a picture or a scanned copy of page one. Procedure must include a process to refuse to load damaged or dirty IIT. The type of inspection depends on the type of cargo movement (cross-border on land, or ocean/air modes). It must include at a minimum: refusal of damaged/dirty IIT; inspection checklist that records size of IIT, IIT number, name of person conducting inspection, time and date of inspection, and condition of the floor, roof, inside/outside walls, undercarriage; inspection for pest contamination (e.g. eggs, nests, dirt, seeds); tools utilized for inspections; who is responsible for inspections; and training responsible employees on inspections.
(CTPAT MSC 5.2)

- (●) Yes - Please attach image of page 1
- ( ) No documented procedure in place
- ( ) Documented procedure only contains partial requirements indicated in guidance

49.pdf

**Comments:** *No comments were provided*

47 Critical Does the documented inspection of an IIT conducted prior to loading include all minimally required areas? (Select all that apply)

**Question Guidance:** Security and agricultural inspections are conducted on Instruments of International Traffic (IIT) and conveyances to ensure their structures have not been modified to conceal contraband or have been contaminated with visible agricultural pests. An inspection checklist that records the size of IIT, IIT number, name of person conducting inspection, time and date of inspection, condition of the following: floor, roof, inside/outside walls, undercarriage, Inspection for pest contamination (e.g. eggs, nests, dirt, seeds) must be used. Pest contamination includes visible forms of animals, insects or other invertebrates, or any organic material of animal origin; viable or non-viable plants or plant products ; or other organic material, including fungi; or soil, or water; where such products are not the manifested cargo. The checklist can be either paper or electronic; however, proof of checklist usage and completion must be provided upon request.
(CTPAT MSC 5.3, 5.5)

biểu kiểm cont.jpg

- [x] Checklist is utilized (please attach photo of checklist)
- [x] Size of IIT
- [x] IIT number
- [x] Name of person performing the inspections
- [x] Date and time of inspection
- [x] Floor and roof of IIT intact, no holes or leaks
- [x] Inside/outside walls, undercarriage free of damage
- [x] Inspection for invasive species (e.g. eggs, nests, dirt, seeds) included
- [x] Supervisor's signature
- [ ] No inspections completed or documented

**Comments:** *No comments were provided*

48 Must Does the documented inspection process include inspection of the external hardware of the IIT to ensure that it is properly equipped to withstand attempts of removal?

**Question Guidance:** Conveyances and Instruments of International Traffic (IIT)(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 IIT's locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device. Consider using IIT with tamper resistant hinges. Members may also place protective plates or pins on at least two of the hinges

of the doors and/or place adhesive seal/tape over at least one hinge on each side.
(CTPAT MSC 5.4)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

49 Material Are photos and/or CCTV videos taken during the IIT loading process? (Select all that apply)

**Question Guidance:** This is a best practice and is encouraged that CCTV or photos be available of the Instruments of International Traffic (IIT) loading process. Images must include the before, during and after cargo loading stages and must capture the entire secured area and the inside of IIT from tail to nose.
(CTPAT MSC 9.16, 5.6)

- [x] Photos are captured
- [x] Video is captured
- [ ] No video or photos are captured, or does not cover required areas

**Comments:** *No comments were provided*

50 Critical Does the shipping area use appropriate equipment to conduct a 7-point IIT inspection? (Select all that apply)
Please attach a photo of all equipment used to conduct this IIT inspection.

**Question Guidance:** Specific equipment is required to conduct Instruments of International Traffic (IIT) inspections, including: A measurement tool, such as a laser distance measurer, pre-measured string, or tape measure; A mirror specifically designed for inspecting vehicle undercarriages. Both convex and concave mirrors are acceptable, provided they are appropriately sized for inspecting the IIT. Other types of mirrors, such as makeup mirrors, are not acceptable; A mallet or hammer for testing walls; A tool for cleaning or sweeping the inside of the IIT, such as a broom, blower air hose, shop vacuum, etc.; All tools must be available for review upon request. The auditor should document the details of the tools used in the notes section.
NOTE: If tools are available, but no IIT inspections are being conducted, only select the answer option "No IIT Inspections are Conducted" and provide comments on any tools that may be available.

- [x] Measurement tool
- [x] Mirrors for undercarriage
- [x] Tap test tool
- [x] IIT interior cleaning tool
- [ ] No tools available/tools do not meet requirements
- [ ] No IIT inspections are conducted

dụng cụ kiểm c... jpg

**Comments:** *No comments were provided*

51 Must Are IIT inspections conducted in a secure area and in view of CCTV cameras? (Select all that apply)

**Question Guidance:** All security inspections of Instruments of International Traffic (IIT) should be performed in an area of controlled access and, if available, monitored via a CCTV system. This is a best practice and is encouraged that photos must be taken of the IIT inspection processes. CCTV recordings must capture entire secured area, and inside of IIT from tail to nose.
(CTPAT MSC 5.6)

- [x] IIT inspection area is visible on CCTV
- [x] Inside of IIT is visible from tail to nose on CCTV
- [x] Inspections are conducted in a secured area
- [ ] Inspections are not captured on CCTV nor in a secured area
- [ ] No IIT inspections are conducted

**Comments:** *No comments were provided*

52 Must Does the facility maintain training records indicating which employees are trained to perform a 7-point IIT inspection?

**Question Guidance:** The facility must have records showing employees are trained/re-trained as needed on Instruments of International Traffic (IIT) inspections. Training materials and documentation must be kept and available upon request.

- (●) Yes
- ( ) No
- ( ) No IIT inspections are conducted

**Comments:** *No comments were provided*

53 Material Is there a procedure where management or supervision conducts follow up IIT inspections?

**Question Guidance:** This is a best practice and is encouraged that the facility should have a documented procedure that indicates how frequent management conducts follow-up inspections to ensure Instruments of International Traffic (IIT) inspection processes are accurately followed. Based on risk, management personnel should conduct random searches of conveyances after the transportation staff have conducted conveyance/Instruments of International Traffic inspections. The searches of the conveyance should be done periodically, with a higher frequency based on risk. The searches should be conducted at random without warning, so they will not become predictable. The inspections should be conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the United States border.
(CTPAT MSC 5.8)

- (●) Yes
- ( ) No
- ( ) No IIT inspections are conducted

**Comments:** *No comments were provided*

54 Material Are all IIT inspections and loading of IIT supervised?

**Question Guidance:** Best practice dictates that all Instruments of International Traffic (IIT) inspections as well as the loading of IIT be supervised and that supervisors should also sign the inspection checklist. Evidence should be provided to the SCAN auditor to show how factory management plays a role in the inspection of IIT, supervision of loading of IIT including frequency and if inspections are announced or unannounced. For the loading of IIT, it is acceptable if a security officer or other designated personnel is supervising the process.
(CTPAT MSC 7.4)

- (●) Yes - all are supervised
- ( ) Yes - some, random inspections and loading of IIT are supervised
- ( ) No

**Comments:** *No comments were provided*

55 None Does the facility directly contract transportation service providers for any of their customers or business partners?

**Question Guidance:** Question who is responsible for contracting transportation services at origin. This includes the movement to a consolidation location or between multiple production or storage facilities prior to export.

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

56 Material Does the facility have a documented procedure to require confirmation of arrival at destination (IIT yard or freight forwarder's location) for items shipped?

**Question Guidance:** This is a best practice and is encouraged that the facility should work with their transportation providers to track conveyances from origin to final destination point. Requirements should include confirmation of items shipped arriving at Instruments of International Traffic (IIT) yard/freight forwarder's warehouse/location; requiring confirmation via phone of cargo arrival at destination from driver or carrier dispatch; tracking shipment via GPS (CTPAT MSC 5.14)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

57 Material What tracking technologies does the facility require to be used by the contracted transportation company to monitor movement and confirm cargo arrival?

**Question Guidance:** This is a best practice and is encouraged that the factory should have documented procedures that list what tracking technologies are required to be used by transportation providers. Examples include GPS controlled by either the carrier or shipper, required cell phone checks by carrier dispatch, etc. (Carrier is the transportation service provider; Shipper is the factory and/ or the vendor). If facility uses a different type of tracking not listed in answers, please describe in notes.
(CTPAT MSC 5.15)

- ( ) GPS carrier controlled
- ( ) GPS shipper controlled
- ( ) Cell phone check by carrier dispatch
- ( ) Cell phone confirmation by driver

- (●) Two or more of the above options - Please describe
- ( ) Other - Please describe
- ( ) No tracking technologies used

**Comments:** Including: GPS controlled and required cell phone checks by carrier dispatch

58 Material Where possible, are transit routes from the facility to the port or next destination location randomly changed to minimize predictability?

**Question Guidance:** Evidence should be provided to the auditor to show how transit routes from the facility to the next destination are randomly changed, if applicable. The route scheduling is to be made by authorized team members from the organization or the transit operation team (not at the discretion of the driver). Routes need to be pre planned and coordinated accordingly in advance of the transportation day. This is a best practice and is encouraged.

- (●) Yes
- ( ) No
- ( ) Only one route is available

**Comments:** *No comments were provided*

59 Material Does the facility provide documented instructions to transportation service drivers detailing that only required stops are permitted? ( i.e. inspections by governmental agencies, refueling etc.)

Only select NA if this facility is strictly leveraging only small packages via consolidator carriers.

**Question Guidance:** Cargo at rest is cargo at risk. Scheduled stops would not be covered by this policy, but would have to be considered in an overall tracking and monitoring procedure. This is a best practice and is encouraged. Best practice dictates a “no-stop” policy should be implemented with regard to unscheduled stops. Review facility's requirements timeline. It must include types of stops permitted; examples include but not limited to: inspections by government agencies, fueling, etc.; reporting of unscheduled or other unpermitted stops must be reported to facility.
(CTPAT MSC 5.16)

- (●) Yes
- ( ) No

- [ ] NA

**Comments:** *No comments were provided*

60 Critical Does the facility document driver information for arriving and departing material movements? (Select all that apply)

**Question Guidance:** 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. If presenting a government-issued photo identification is not feasible, the facility employee may accept a recognizable form of photo identification issued by the carrier company that employs the driver picking up the load. This process must be documented in the factory's SOP.
(CTPAT MSC 10.3, 10.4)

- [x] Driver log is maintained (please attach photo of driver log in use)
- [x] Tractor/IIT number listed
- [x] Photo ID required of drivers
- [x] Carrier name
- [x] Date
- [x] Arrival Time
- [x] Departure Time
- [x] Seal verification information for IIT departure
- [ ] No driver log available

sổ theo dõi cont... jpg

**Comments:** *No comments were provided*

61 Material Does the facility require carriers to provide advance notification of the estimated time of arrival for scheduled pickups, including the driver's name and truck number?

**Question Guidance:** Where operationally feasible, the facility should allow deliveries and pickups by appointment only. This criterion will help shippers and carriers to avoid fictitious pickups. Fictitious pick-ups are criminal schemes that result in the theft of cargo by deception that includes truck drivers using fake IDs and/or fictitious businesses set up for the purpose of cargo theft. When a carrier has regular drivers that pick up goods from a certain facility, a good practice is for the facility to maintain a list of the drivers with their pictures. Therefore, if it is not feasible to let the company know which driver is coming, the company will still be able to verify

that the driver is approved to pick up cargo from the facility.

(CTPAT 10.7)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

62 None Does the facility ship less than container load (LCL)?

- ( ) Yes
- (●) No

**Comments:** *No comments were provided*

64 None Does the facility make air shipments?

- ( ) Yes
- (●) No

**Comments:** *No comments were provided*

66 None Does the facility make any shipments in open top, open sided, ventilated (livestock), soft sided containers?

- ( ) Yes
- (●) No

**Comments:** *No comments were provided*

68 Critical Are international shipments sealed with an ISO 17712:2013 compliant high-security seal immediately after the IIT is loaded?

Only select NA if this facility is strictly leveraging only small packages via consolidator or carriers.

**Question Guidance:** All shipments must be secured immediately after loading/ stuffing/ packing with a high-security seal that meets or exceeds the most current International Organization for Standardization (ISO) 17712 standard for high-security seals. This must be documented in the factory's SOP.

(CTPAT 6.2)

- (●) Yes (please attach photo of ISO approved seal utilized)
- ( ) No
- ( ) NA


Y-189 ISO certi... pdf

**Comments:** *No comments were provided*

69 Critical Does the facility have documented and verifiable procedures to ensure that security seals are controlled? (Select all that apply)

Only select NA if the seals are provided by a 3rd party such as a consolidator or carrier.

**Question Guidance:** Review the policy and if possible observe the sealing of an Instruments of International Traffic (IIT) on site. Pay careful attention to the policy to insure that all requirements are covered. Review the facility's seal process. It must include at a minimum that only designated employees can access seal storage and apply seals to IITs.

(CTPAT 6.1)

- [x] Policy is documented (please attach photo of applicable section of procedure)
- [x] Seals are secured in storage
- [x] Specific employees are listed who have access to seal storage
- [ ] No documented policy is available
- [ ] NA

45.pdf

**Comments:** *No comments were provided*

70 Must Is there a documented process for the facility to promptly notify any business partners and relevant law enforcement agencies in the supply chain about security threats or shipment breaches, as appropriate?

**Question Guidance:** If a credible (or detected) threat to the security of a shipment or conveyance is discovered, is there a documented process where the facility alerts (as soon as feasibly possible) any business partners in the supply chain that may be affected and any law enforcement agencies, as appropriate?

(CTPAT MSC 5.29)

- (•) Yes
- ( ) No

**Comments:** *No comments were provided*

71 Material Prior to border crossings, or load transitions, is there a documented procedure for checking IIT conveyances for signs of tampering to include physical inspections and VVTT?

Only select NA if this facility is strictly leveraging only small packages via consolidator carriers.

**Question Guidance:** Properly trained individuals should conduct the inspections.

V – View seal and Instruments of International Traffic (IIT) locking mechanisms; ensure they are OK;

V – Verify seal number against shipment documents for accuracy;

T – Tug on seal to make sure it is affixed properly;

T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose.

(CTPAT MSC 5.24)

- (●) Yes
- ( ) No
- ( ) NA

**Comments:** *No comments were provided*

## Agricultural security 100%

72 Must Does this facility have documented procedures designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations?

Only select NA if this facility does not use any wood or wood packaging material in their manufacturing or shipping processes.

**Question Guidance:** Visible pest prevention measures must be adhered to throughout the supply chain. Measures regarding WPM must meet the International Plant Protection Convention's (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15). Wood packaging material (WPM) refers to wood products (excluding paper products) like pallets, crates, boxes, reels, and dunnage used in supporting or transporting goods. These items, often made from raw wood, can harbor pests if not properly processed or treated. The International Plant Protection Convention (IPPC), overseen by the UN's Food and Agriculture Organization, aims to prevent the spread of pests globally. ISPM 15, a standard under IPPC, mandates that WPM must be debarked, heat-treated, or fumigated with methyl bromide and marked with the IPPC "wheat stamp" to indicate compliance. Exemptions include materials like paper, metal, plastic, and engineered wood products.

(CTPAT MSC 8.1)

- (●) Yes
- ( ) No
- ( ) NA

**Comments:** *No comments were provided*

73 Must Does this facility have a documented process to address removing pest contamination and other debris from an IIT's exterior and interior prior to loading? Documented process must include 1 year retention policy.

Only select NA if this facility is strictly leveraging only small packages via consolidator or carriers.
**Question Guidance:** To prevent invasive pests and debris, a best practice is to run water over the outside of the IIT prior to loading and before departure from the facility. An inspection for dirt and evidence of pests should also be conducted. Both processes should be documented. Retain for one year documentation demonstrating compliance with any records related to type of contaminants found, where they were found and how the contaminants were eliminated. NA is used to address if shipments are being added to a Less than Truckload shipment from this facility via small package consolidator or carrier.
(CTPAT 8.1, 5.7)

- (●) Yes - Please attach a photo of the section in the process
- ( ) No documented process and/or inadequate retention policy
- ( ) NA

47.pdf

**Comments:** *No comments were provided*

74 Material Does the facility remove pest contamination and other debris from IIT exterior and interior prior to loading?

Only select NA if this facility is strictly leveraging only small packages via consolidator or carrier.
**Question Guidance:** To prevent invasive pests and debris, a best practice is to run water over the outside of the IIT prior to loading and before departure from the facility. An inspection for dirt and evidence of pests should also be conducted. NA is used to address if shipments are being added to a Less than Truckload shipment from this facility via small package consolidator or carrier.

- (●) Yes - Please advise how verification was conducted

- ○ No
- ○ Dirty IIT are refused
- ○ NA

**Comments:** To prevent insect infestations and debris, the factory sweeps and rinses the outside of the containerized in-line equipment (IIT) before loading and before it leaves the facility.

75 Material Does the facility have a documented procedure to inspect and review evidence of pest access such as baited traps, periodic extermination, and removal of debris from shipping and storage facilities?

**Question Guidance:** The facility should have a documented procedure that indicates how pests are controlled. This could include the use of bait stations, having a regular extermination service complete preventative care and established routine practices for employees to follow that indicates all IIT and storage areas are free from trash, bugs, food, etc. 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.
(CTPAT MSC 7.2)

- ◉ Yes - and is implemented (please advise how verification was conducted)
- ○ Yes
- ○ No

**Comments:** The factory has documented procedures outlining pest control methods such as the use of bait stations, regular extermination services performing preventative care, and established routine procedures for staff to follow.

76 Must For international shipments, is wood packaging material heat treated or fumigated to kill pests and limit the potential for introduction of pests at the IIT stuffing location? (Select all that apply)

Only select NA if the facility is not using wood packing material for international shipments.

**Question Guidance:** In order to prevent unwanted pests in the supply chain, a documented procedure must be established to heat treat or fumigate wood packaging material at the IIT stuffing location. The procedure must indicate what methods are conducted, how often and the party responsible. As long as factory uses wood packing materials, used for international shipments, those must be heat treated or fumigated in order to be in compliance.
(CTPAT MSC 8.1)

- [ ] Only heat treated or otherwise treated packaging material is utilized at this location
- [ ] Origins of all wood used in the manufacturing process is documented and provided to the receiver
- [ ] Factory cannot detail how wood packaging material is treated prior to utilization
- [x] NA

**Comments:** the facility is not using wood packing material for international shipments.

77 Must For international shipments, are wood pallets used in the shipping process heat treated or fumigated to kill pests and limit the possible introduction of pests at the loading facility? Are pallets stored inside the facility to limit the exposure to seeds, dirt and other forms of contamination? (Select all that apply)

Only select NA if the facility is not using wood pallets for international shipments.

**Question Guidance:** The wood pallets used in shipping must be heat treated or fumigated at the loading facility. A documented procedure must indicate who is responsible for conducting the heat treatment and also how pallets are stored inside the facility to limit exposure to any contaminants.

If pallets are stored outdoors or are not heat-treated, request an explanation from the facility team regarding why this practice is being followed or allowed.

(CTPAT MSC 8.1)

- [ ] Pallets are heat treated or fumigated
- [ ] Pallets are marked with a heat treated stamp or a Phytosanitary inspection certificate is issued with each pallet delivery
- [ ] Pallets are stored inside the building
- [ ] Documented process is available
- [ ] Pallets are observed stored outside and on the ground
- [ ] Pallets are not heat treated nor fumigated
- [x] NA

**Comments:** the facility is not using wood packing material for international shipments.

## Seal Security 100%

78 Must Does the facility have documented, detailed high-security seal procedures that describe how seals are issued and controlled at the facility and during transit? (Select all that apply)

Only select NA if this facility is strictly leveraging only small packages via consolidator or carrier, using seals that are provided by the 3rd party provider.

**Question Guidance:** Written procedures must be maintained locally for accessibility, reviewed annually, and updated as needed. Access Control: Limit seal management to authorized personnel and store seals securely. Inventory & Tracking: Maintain a seal log to record receipt, issuance, and affixation by trained personnel. In-Transit Controls: Verify seal integrity and match seal numbers with shipping documents. Seal Breakage: Document and report seal changes immediately, ensuring proper notification and log updates. Discrepancies & Investigations: Retain tampered seals, investigate discrepancies, take corrective action, and report compromised seals to CBP and foreign authorities if necessary.
(CTPAT MSC 6.1)

- [x] Controlling Access to Seals
- [x] Inventory, Distribution and Tracking (Seal Log)
- [x] Controlling Seals in Transit
- [x] Seals Broken in Transit
- [x] Seal Discrepancies
- [x] Procedures are reviewed annually
- [ ] Documentation not available
- [ ] Gaps in implementation were observed (please provide comments)
- [ ] NA

**Comments:** *No comments were provided*

79 Critical Are security seals stored in a secured location?

Only select NA if this facility is strictly leveraging only small packages via consolidator or carrier, using seals that are provided by the 3rd party provider.

**Question Guidance:** Seals must be stored and maintained in a secured location such as a locked cabinet/drawer that cannot be easily removed from an area (a lock box is not appropriate since it can be picked up).
(CTPAT MSC 6.1)

- (●) Yes (please attach photo of seal storage location)
- ( ) No

- ○ NA

tů seal.jpg

**Comments:** *No comments were provided*

80 Critical Does the facility have documented test reports or statements from the seal vendor to validate that the seals utilized meet (or exceed) the most recent ISO 17712 criteria?

Only select NA if this facility is strictly leveraging only small packages via consolidator or carrier, using seals that are provided by the 3rd party provider.

**Question Guidance:** Acceptable evidence of compliance is a copy of a laboratory testing certificate that demonstrates compliance with the ISO high-security seal standard. Test reports should be maintained to show compliance with ISO 17712 criteria. Factories must request new test documentation to show compliance for every batch of seals they receive. This process must be documented in the facility's procedure.

(CTPAT MSC 6.5)

- ◉ Yes (please attach photo of test report)
- ○ No
- ○ NA

**Comments:** *No comments were provided*

81 Must Is there a documented procedure in place requiring management level personnel to conduct periodic audits of the seal inventory, seal log, shipping documents and conveyances to validate that the seal controls are being followed. All steps must be documented. (Select all that apply)

Only select NA if this facility is strictly leveraging only small packages via consolidator or carrier, using seals that are provided by the 3rd party provider.

**Question Guidance:** A procedure must be documented that requires a defined frequency for management personnel to conduct audits of seal inventory, the seal log and shipping documentation. The procedure must also list how management is to document these audits to show compliance to the auditor. If selecting NA, the seals are provided by the consolidator or small package carriers.

(CTPAT MSC 6.6)

- ☑ A documented procedure is available
- ☑ Audits are conducted and documented

- [ ] No documented procedure or practice is in place
- [ ] NA

**Comments:** *No comments were provided*

82 Critical Describe the facility's seal application process. (Select all that apply)

Only select NA if this facility is strictly leveraging only small packages via consolidator or carrier, using seals that are provided by the 3rd party provider.

**Question Guidance:** CTPAT's seal verification process must be followed to ensure all high-security seals (bolt/cable) have been affixed properly to the IIT and are operating as designed. The procedure is known as the VVTT process:

V – View seal and IIT locking mechanisms; ensure they are OK;

V – Verify seal number against shipment documents for accuracy;

T – Tug on seal to make sure it is affixed properly;

T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose.

The VVTT process for cable seals needs to ensure the cables are taut. Once it has been properly applied, tug and pull the cable in order to determine if there is any cable slippage within the locking body. This process must be documented in internal procedures.

(CTPAT MSC 6.7 / 7.5 / 7.29 / 7.30)

- [x] VVTT process included in seal application procedure
- [x] Secondary testing and validation is checked by supervisors or security guard at time of exit from the facility
- [x] Seal numbers are electronically documented on shipping documents
- [x] Testing procedure recorded on CCTV footage
- [x] Seal numbers are communicated or otherwise transmitted to the consignee
- [x] Facility is advised when seal numbers are changed prior to departure from port of origin
- [x] Process is documented
- [ ] No seal application process was available
- [ ] NA

**Comments:** *No comments were provided*

## Procedural Security 100%

83 Critical Is the area adjacent to the shipping and receiving areas enclosed or otherwise monitored?

**Question Guidance:** Cargo handling and storage areas must be enclosed by perimeter fencing. Facilities managing cargo must also use interior fencing to secure cargo and handling zones. Where fencing is not feasible, effective barriers such as solid walls, steep terrain, or dense vegetation must be used. If the area cannot be fully enclosed, it must be actively monitored. Acceptable monitoring methods include continuous observation, CCTV coverage of entry/exit and loading zones, electronic card/badge access systems, or access rosters with employee names, photos, and authorized times or roles.

- (●) Yes (please attach photo showing enclosure and/ or monitoring method)
- ( ) No

Kv lưu cont.jpg

**Comments:** *No comments were provided*

84 Critical Is a documented procedure in place to report unauthorized access to a IIT, and/or product storage areas within the facility including whom to notify?

**Question Guidance:** Facilities must implement a documented policy to prevent and respond to unauthorized access to IIT and storage areas. This includes defining unauthorized access, conducting inspections, managing security breaches, and establishing reporting protocols. Reportable incidents include tampering, hidden compartments, unauthorized seals, smuggling, illegal access to transport vehicles, and incidents of coercion or misuse of business identifiers. (CTPAT MSC 5.29, 7.23, 7.24)

- (●) Yes (please attach photo of applicable section of procedure)
- ( ) No

35.pdf

**Comments:** *No comments were provided*

85 Critical Is a documented procedure in place to monitor and limit access to critical operational areas of the facility, such as warehouse picking, final packing or packaging, shipping and receiving?

**Question Guidance:** Facilities must have a documented policy to limit access to critical operational areas to only authorized personnel. The policy must define critical operational areas (warehouse picking, final packing/packaging, and shipping/receiving at a minimum). Describe how access is limited.

- (●) Yes (please attach photo of applicable section of procedure)

- ○ No
- ○ Yes - But gaps in implementation were observed

34.pdf

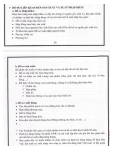
**Comments:** *No comments were provided*

86 Critical Is a documented procedure in place that requires all information used in the shipping documents for merchandise/cargo to be legible, complete, and accurate?

**Question Guidance:** Facilities must have a documented process for ensuring shipping documents are legible, complete, and accurate.

(CTPAT MSC 7.6)

- ◉ Yes (please attach photo of applicable section of procedure)
- ○ No
- ○ Yes - But gaps in implementation were observed



QT hồ sơ chính... png

**Comments:** *No comments were provided*

87 Critical Is a documented procedure in place to investigate and resolve a carton count shortage, overage, or any documentation issue found during IIT loading; or after the shipment has departed the facility?

**Question Guidance:** All shortages, overages, and other significant discrepancies or anomalies must be investigated and resolved, as appropriate. Facilities that load Instruments of International Traffic (IIT) must have a documented process in place for counting cartons during the loading process and identifying and resolving shortages, overages, and/or documentation issues.

(CTPAT MSC 7.27)

- ◉ Yes (please attach photo of applicable section of procedure)
- ○ No
- ○ Yes - But gaps in implementation were observed

53.pdf

**Comments:** *No comments were provided*

88 Critical Is a documented procedure in place for international shipments to be marked, counted, weighed, and properly reported on shipping documents?

Select NA if no international shipments happen from this facility.

**Question Guidance:** Facilities that load Instruments of International Traffic (IIT) must have a documented process that dictates that cargo must be marked, counted weighed, and properly reported on commercial invoice and bill of lading.

- (●) Yes (please attach photo of applicable section of procedure)
- ( ) No
- ( ) Yes - But gaps in implementation were observed
- ( ) NA

48.pdf

**Comments:** *No comments were provided*

89 Critical Is a documented procedure in place that restricts access to shipping and receiving documentation?

**Question Guidance:** A documented procedure must be established to outline: the roles or positions responsible for creating and processing shipping documents; the individuals or positions designated to review documents for completeness and accuracy; and the controlled access measures ensuring that only authorized personnel involved in document creation, processing, and usage can access shipping records.

- (●) Yes (please attach photo of applicable section of procedure)
- ( ) No
- ( ) Yes - But gaps in implementation were observed

48.pdf

**Comments:** *No comments were provided*

90 Material Are pre-printed paper documents/forms used to prepare commercial documents and properly secured?

**Question Guidance:** Best practice dictates if paper documents are used, facility must describe steps taken to secure them in a documented procedure.

(CTPAT MSC 7.7)

- (●) Pre-printed documents/forms are secured
- ( ) Pre-printed documents/forms are not secured
- ( ) Pre-printed paper documents/forms are not utilized

**Comments:** *No comments were provided*

91 Material Are shared network printers password protected when used to prepare export documents?

Only select NA if there are no shared network printers being utilized.

**Question Guidance:** This is a best practice and is encouraged that the access to shared network printers should be controlled via individually assigned passwords.

- (●) Yes
- ( ) No
- ( ) NA

**Comments:** *No comments were provided*

92 Critical Is there a documented procedure in place to require commercial document packets be sent at time of shipment departure? Please explain process.

**Question Guidance:** Document packets must be sent with shipment at time of departure once information is verified as correct. This can be either hard copy or electronic but must be documented in a procedure.

- (●) Yes
- ( ) No
- ( ) Yes - But gaps in implementation were observed

**Comments:** The factory will send the commercial documentation to the customer via email at the same time as the goods are shipped.

93 Critical Is a documented procedure in place to notify local law enforcement and the customer when illegal shipping activity or any abnormality is suspected or detected?

**Question Guidance:** Procedures to report security incidents or illegal shipping activity are extremely important aspects of a security program. Procedures must include what to report, to whom, how to report the incident, and what to do after the report is completed. Security issues include but are not limited to attempted or completed: theft, fraud, internal conspiracies, stowaways, tampering of cartons/IIT, discovering hidden compartments in IIT during inspection, unauthorized entry into IIT/facility property, extortion, bribes, threats, etc.
(CTPAT MSC 5.29, 7.23)

- (●) Yes (please attach photo of applicable section of procedure)
- ( ) No

31.pdf

**Comments:** *No comments were provided*

94 Critical Are documented access control procedures and devices used to ensure that only authorized employees have access to the facility?

**Question Guidance:** Facility must have a comprehensive policy for controlling access to the buildings and property. Access controls prevent unauthorized access into facilities/areas, help maintain control of employees and visitors, and protect company assets. Access controls include the positive identification of all employees, visitors, service providers, and vendors at all points of entry.

- (●) Yes (please attach photo of applicable documentation section and device)
- ( ) No
- ( ) Yes - But gaps in implementation were observed

03.pdf

**Comments:** *No comments were provided*

95 Critical Is there a documented procedure in place to notify Business Partners of security issues such as attempted theft, fraud or internal conspiracies?

**Question Guidance:** Procedures to report attempted theft, fraud or internal conspiracies are extremely important aspects of a security program. Procedures must include notification to Business Partners, how to report the incident, and what to do after the report is completed. Business Partners include any suppliers, service providers, subcontractors, etc.

- (●) Yes (please attach photo of applicable section of procedure)
- ( ) No

31.pdf

**Comments:** *No comments were provided*

96 Material Is there a documented procedure in place to request the shipping department to validate the freight being loaded against the Purchase Order prior to departure?

**Question Guidance:** Departing cargo should be verified against purchase or delivery orders. As a best practice, this expectation should be documented in a procedure and include how this completed.

- (●) Yes
- ( ) No
- ( ) Yes - But gaps in implementation were observed

48.pdf

**Comments:** *No comments were provided*

97 Critical Is a documented procedure in place to control the issue, removal, and changing of access devices such as ID badge, door and lock keys, access cards, and security alarm codes?

**Question Guidance:** Facilities must implement a documented policy to regulate the issuance, modification, and revocation of access devices, ensuring secure and controlled access to restricted areas. This policy should define various access devices, including photo ID badges, keys, access cards, and alarm codes, and establish guidelines for their distribution. Temporary identification should be provided for seasonal or temporary employees, while permanent staff receive access based on their specific job responsibilities. When employees transition to new roles, their access credentials must be updated accordingly, and upon termination, all access devices must be promptly collected and deactivated. To maintain accurate records, a checklist should be utilized to track the issuance and removal of access devices, reinforcing security and accountability within the facility.

- (●) Yes (please attach photo of applicable section of procedure)
- ( ) No

22.pdf

**Comments:** *No comments were provided*

98 None Do you have dedicated security staff/guards on site?

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

99 Must Are documented job descriptions in place outlining the roles and responsibilities of security staff or staff performing dual roles that include security functions?

**Question Guidance:** Procedures must be in place that list job descriptions outlining roles and responsibilities for all security staff and any staff performing dual roles that include security functions. Job descriptions must be available to the auditor upon request.

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

100 Must Does the facility require the security staff or contractors to “patrol” the facility during off business hours and “patrols" are documented either with CCTV surveillance, electronic recordings or with paper check lists?

**Question Guidance:** A documented procedure must be in place to require all security staff and security contractors to patrol and document the facility at all times of day. The patrols should be documented either via CCTV, electronic recordings or through paper check lists. Auditor to review the documented procedure and the recordings to confirm patrols are conducted and documented.

- (●) Patrols are required; documented electronically or via CCTV
- ( ) Patrols are required; documented via paper only
- ( ) Patrols are required; no documentation available
- ( ) Patrols are not required nor documented

**Comments:** *No comments were provided*

101 Must Does management verify compliance with security staff/guard work instructions and policies?

**Question Guidance:** Documented reviews on security work instructions and policies should be conducted by management. Any discrepancies found should be documented and corrective actions should be taken.
(CTPAT MSC 10.10)

- (●) Yes
- ( ) No
- ( ) Yes - But gaps in implementation were observed

**Comments:** *No comments were provided*

102 Must Are there documented procedures in place to ensure that Bills of Lading (BOLs), Forwarders Cargo Receipt (FCR) and manifests accurately reflect the information provided to the carrier?

**Question Guidance:** The shipper or its agent must ensure that bill of ladings (BOLs) and/or manifests accurately reflect the information provided to the carrier, and carriers must exercise due diligence to ensure these documents are accurate. BOLs and manifests must be filed with Customs in a timely manner. BOL information filed with Customs must show the first foreign location/facility where the carrier takes possession of the cargo destined for the United States.

The weight and piece count must be accurate.

(CTPAT MSC 7.8)

- (●) Yes
- ( ) No
- ( ) Yes - But gaps in implementation were observed

**Comments:** *No comments were provided*

---

103 Must Is there a documented procedure to promptly initiate and record an internal investigation upon discovering a security-related incident (e.g., terrorism, narcotics, stowaways, theft)?

**Question Guidance:** Members must initiate their own internal investigations of any security-related incidents (terrorism, narcotics, stowaways, absconders, etc.) immediately after becoming aware of the incident. The company investigation must not impede/interfere with any investigation conducted by a government law enforcement agency. The internal company investigation must be documented, completed as soon as feasibly possible, and made available to Customs and any other law enforcement agency, as appropriate, upon request.

(CTPAT MSC 7.37)

- (●) Yes
- ( ) No
- ( ) Yes - But gaps in implementation were observed

**Comments:** *No comments were provided*

## Physical Security 94%

104 Critical Is there a designated employee and visitor vehicle parking area separate from the shipping and receiving area?

**Question Guidance:** Facilities must establish designated parking areas for employees and visitors, ensuring they remain separate from shipping and receiving zones. Clear signage must be posted to identify parking locations, and a physical barrier must be in place to distinguish these areas from shipping and receiving operations. Access to shipping and receiving zones should be strictly controlled in accordance with the facility's access control policy. To maintain security and operational efficiency, personal vehicles are not permitted in shipping or receiving areas.

(CTPAT MSC 9.5)

- (●) Yes (please attach photo of applicable area)
- ( ) No
- ( ) Yes - But gaps in implementation were observed

kv đậu xe khách.jpg

**Comments:** *No comments were provided*

---

105 Material Are appropriate controls in place to segregate domestic goods from goods intended for international shipment?

**Question Guidance:** This is a best practice and is encouraged that the cargo must be separated based on domestic, international, high value and/or hazardous goods. If fencing is used, it must be inspected regularly.
(CTPAT MSC 9.2)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

---

106 Material Is a preventative maintenance procedure in place that requires a regular inspection of perimeter fencing or other barriers, buildings, and structures? (Select all that apply)

**Question Guidance:** Best practice dictates the perimeter fencing/barrier should be inspected regularly. This process must be documented. If damage is discovered it must be repaired as soon as possible.
(CTPAT MSC 9.2)

- [x] Procedure is documented
- [x] Regular inspections are documented
- [x] Preventative maintenance logs are kept
- [ ] Nothing in place

**Comments:** *No comments were provided*

---

107 Critical Are there any barriers to limit the ingress and egress to the facility by vehicles and personnel? Please attach photos of applicable areas.

**Question Guidance:** Facilities must have a barrier controlling vehicle and personnel access. Barriers must be monitored in some way at all times. When open, uniformed guards must be present. Physical Security – Cargo handling and storage facilities, Instruments of International Traffic storage areas, and facilities where import/export documentation is prepared in domestic

and foreign locations must have physical barriers and deterrents that guard against unauthorized access. All cargo handling and storage facilities, including trailer yards and offices must have physical barriers and/or deterrents that prevent unauthorized access. Other acceptable barriers may be used instead of fencing, such as a dividing wall or natural features that are impenetrable or, otherwise, impede access such as a steep cliff or dense thickets.
(CTPAT MSC 9.1, 9.4)


hàng rào cổng.jpg

- ( ) Physical barriers
- ( ) Environmental barriers
- (•) Combination of Physical and Environmental barriers
- ( ) No barriers

**Comments:** Factory have  physical and Environmental barriers

108 Critical Are gates secured and monitored when not in use?

Only select NA if gates are not present at the facility.

**Question Guidance:** Gates must be locked when not in use. CCTV should also monitor gates at all times.
(CTPAT MSC 9.4)


hàng rào cổng.jpg

- (•) Yes - Gates are locked/secured when not in use and monitored by CCTV (please attach photo of applicable areas)
- ( ) Yes - Gates are locked/secured when not in use (please attach photo of applicable areas)
- ( ) No
- ( ) NA

**Comments:** *No comments were provided*

109 Must Does the facility have sufficient lighting at entrances, exits, cargo handling and storage areas, along fence lines, and in parking areas to detect movement during periods of darkness?

**Question Guidance:** Facilities must have sufficient interior and exterior lighting. Lighting must cover at a minimum: at all entrances, exits, cargo handling, storage, along fence lines, loading/unloading areas, and in all parking areas. This must be shown on recorded video to the auditor that lighting is installed and operational during nighttime periods.
(CTPAT MSC 9.6)

- (•) Yes

- [ ] No

**Comments:** *No comments were provided*

---

110 Must Which of the following security technologies does the facility incorporate as part of its systems and controls? (Select all that apply)

**Question Guidance:** Facility should be able to show auditor security controls available including but not limited to CCTV, security alarms, intrusion detection systems, etc. If selecting "other" detail type of system/controls in notes. Examples: License plate readers, metal detectors.

(CTPAT MSC 9.7)

- [x] CCTV
- [x] Access Control
- [ ] Security Alarm
- [ ] Other Technologies Used
- [ ] No Security Technology Used

**Comments:** *No comments were provided*

---

CAPA Assigned **2026/07/24** | Due Date **2026/09/22** Included in scoring

**CAPA:** Establish and document a procedure that requires the installation and use of security technology at the facility.

- If you have already implemented, please describe in the comment section when and how you completed the corrective action or implemented the process. Please attach a photo of the process with the title and description of document.

- If you will implement, please provide your corrective action plan and the timeline (future date) for completion and implementation of the process in the comment section.

**CAPA Guidance:** The documented procedure must include, at a minimum:

- A requirement that security technologies (for example CCTV, Access Controls, Security Alarms) be utilized and documented, installed and maintained to safeguard the facility, personnel, cargo, and critical areas.

- The specific locations or zones where each technology must be deployed (e.g., loading docks, storage areas, perimeter gates)

- Assignment of responsibility for the installation, maintenance, and monitoring of each system

- Installation verification and ongoing functionality checks to ensure equipment operates effectively

- A policy requiring upgrades or replacements as technology becomes outdated or when vulnerabilities are identified

The comments section must detail actions that have been completed or are planned to be taken. If a document is attached, please specify the page number where the relevant process begins.
CAUTION: Selecting option "Will not implement/ will not comply with corrective action request" is indicating that you acknowledge that your final score for this question will lose points and may be negatively viewed by SCAN Members.

- ○ Already implemented
- ◉ Will implement
- ○ Will not implement/ will not comply with corrective action request

**Comments:** We  will implementing this process in September, 2026.
Mr. Vu- IT staff will be charge of this procedure Our procedure will be included at a minimum:
- A requirement that security technologies (for example CCTV, Access Controls, Security Alarms) be utilized and documented, installed and maintained to safeguard the facility, personnel, cargo, and critical areas.
- The specific locations or zones where each technology must be deployed (e.g., loading docks, storage areas, perimeter gates)
- Assignment of responsibility for the installation, maintenance, and monitoring of each system
- Installation verification and ongoing functionality checks to ensure equipment operates effectively
- A policy requiring upgrades or replacements as technology becomes outdated or when vulnerabilities are identified

111 Must Do you have documented procedures governing the use of the security technology?

**Question Guidance:** Facilities must maintain a documented policy outlining the use, maintenance, and protection of security technology, such as burglary alarm systems and intrusion detection systems. This policy should define a regular schedule for testing and inspections to ensure all equipment is properly installed and functioning. Only authorized personnel should manage and oversee the security systems. Inspection results must be documented, including any identified issues and the corrective actions taken to maintain system integrity.
(CTPAT MSC 9.8)

- ◉ Yes
- ○ No Documented Procedure
- ○ No Security Technology Used

**Comments:** *No comments were provided*

112 Material Was security equipment installed by a licensed/certified contractor?

**Question Guidance:** Any security technology used at the facility must be installed by a licensed, certified, or otherwise authentic source as a best practice.
(CTPAT MSC 9.9)

- (●) Yes
- ( ) No
- ( ) No Security Technology Used

**Comments:** *No comments were provided*

113 Material Do you have maintenance contracts in place for your security systems?

**Question Guidance:** As a best practice, facilities are encouraged to implement regular security technology maintenance. Additionally, facilities should provide a maintenance contract as proof of compliance with this standard.

- (●) Yes, current contracts are in place
- ( ) No current contracts in place
- ( ) No Security Technology Used

**Comments:** *No comments were provided*

114 Must Are Critical Security Infrastructure locations secured and authorized access limited to only those whose jobs require access?

**Question Guidance:** Observe the locations of alarm, CCTV infrastructure and control locations to determine if access is limited. Also question management on whom is permitted access.
(CTPAT MSC 9.10)

- (●) Yes
- ( ) No
- ( ) No Security Technology Used

**Comments:** *No comments were provided*

115 Material In the event of a power outage, does the facility have an alternate electrical power system to ensure uninterrupted operation of electronic security systems?

**Question Guidance:** Discuss with management the capability at the facility to produce adequate electrical power during a local power outage to support security systems, lighting, and computer systems. This is a best practice and is encouraged. (Please note battery backup or

onsite generators qualify.)

(CTPAT MSC 9.11)

- (●) Yes
- ( ) No
- ( ) No Security Technology Used

**Comments:** *No comments were provided*

---

11 6 Critical Is a CCTV system used to monitor the facility and premises' including entrances, exits, cargo storage, shipping, packing and other loading/unloading areas? (Select all that apply)

**Question Guidance:** Upload a picture of the CCTV control room and monitors. Determine the facility's use of a closed circuit television system. If used, review recordings from the previous day and night to determine if all cameras are working properly with camera coverage of perimeter, entrances, exits, cargo storage, shipping, packing and other loading/unloading areas. (CTPAT MSC 9.4, 9.12, 9.13)

- [x] All entrance(s) / exits
- [x] Cargo storage / shipping
- [x] Loading / unloading area(s)
- [x] Packing area
- [x] Perimeter
- [ ] CCTV monitoring alarms if unauthorized access is detected
- [ ] No CCTV

**Comments:** *No comments were provided*

---

CAPA Assigned **2026/07/24** | Due Date **2026/09/22** Included in scoring

**CAPA:** Establish and document a procedure requiring the use of a CCTV system to monitor the facility, premises, and all critical operational areas.

Describe in the comment section when and how you completed the corrective action or implemented the process. Please attach a photo of the process with the title and description of document.

**CAPA Guidance:** The documented procedure must include, at a minimum:

- CCTV must monitor all facility entrances and exits, perimeter fencing, cargo handling and storage areas, shipping/receiving docks, and other critical areas identified by the facility
- Require periodic inspection (at least annually) and maintenance to ensure cameras are functioning properly and recordings are being captured and stored as intended
- CCTV system must be kept in a secure area; only authorized personnel can access it

The comments section must detail actions that have been completed. If a document is attached, please specify the page number where the relevant process begins.

CAUTION: Selecting option "Will not implement/ will not comply with corrective action request" is indicating that you acknowledge that your final score for this question will lose points and may be negatively viewed by SCAN Members.

- (●) Already implemented
- ( ) Will not implement/ will not comply with corrective action request

CCTV SYSTEM ... pdf

**Comments:** Mr Vu- IT staff established  a procedure requiring the use of a CCTV system to monitor the facility, premises, and all critical operational areas. The procedure was approved and issued on July 24th, 2026.

Our procedure was included:

- CCTV must monitor all facility entrances and exits, perimeter fencing, cargo handling and storage areas, shipping/receiving docks, and other critical areas identified by the facility
- Require periodic inspection (at least annually) and maintenance to ensure cameras are functioning properly and recordings are being captured and stored as intended
- CCTV system must be kept in a secure area; only authorized personnel can access it

11 7 Material Does your CCTV system have a failure alarm that indicates when the system is off line or no recording is underway?

**Question Guidance:** Auditor should question management to determine how CCTV recording is validated as functioning properly. This is a best practice and is encouraged that the CCTV system must have a failure alarm or other indication that alerts facility of operational issues. (CTPAT MSC 9.14)

- (●) Yes
- ( ) No
- ( ) No CCTV

**Comments:** The surveillance camera system will send notifications to your email or CCTV management app when the system is offline or no recording is being made.

118 Critical Does the CCTV system run 24 hours per day 7 days per week?

**Question Guidance:** Auditor should question management and ask to see CCTV footage from at least one week prior. View 4 time segments 6 hours apart to ensure 24 hour coverage. (CTPAT MSC 9.13)

- (●) Yes (please attach photo of applicable area)

cctv.jpg

- ○ No
- ○ No CCTV

**Comments:** *No comments were provided*

119 Must Is the facility's CCTV system recording at the highest quality picture setting available?

**Question Guidance:** Auditor should ask what the resolution of the CCTV system is and when the last time system was serviced or upgraded. Also review some footage to see if things like license plate numbers and faces are recognizable when zoomed in on.

(CTPAT MSC 9.13)

- ◉ Yes
- ○ No
- ○ No CCTV

**Comments:** *No comments were provided*

120 Must Does the facility's management team conduct random and documented reviews of CCTV footage periodically to ensure security procedures are being followed?

**Question Guidance:** Auditor should request to see management review documentation of CCTV. Also question management on frequency of reviews and what was an example of the last unusual occurrence that required some type of corrective action. Recorded video must be reviewed frequently by management to ensure documented policies are being followed. Facility must be able to provide evidence showing they are conducing CCTV reviews. Evidence must include the following information: Date, who reviewed it, what was reviewed, whether process was being followed, corrective action plan if needed must be logged. Frequency of review determined on facility's risk assessment and prior review findings. The policy must state the review frequency.

(CTPAT MSC 9.15)

- ◉ Yes
- ○ No
- ○ No CCTV

**Comments:** *No comments were provided*

121 Critical How many days are CCTV recordings kept?

**Question Guidance:** Auditor should review CCTV footage from one, two, and three months ago to determine available recall achievability. A minimum of 90 days or more is preferred. (CTPAT MSC 9.16)

- ○ 90 or more days
- ◉ 45 - 89 days
- ○ Less than 45 days
- ○ Recordings not retained
- ○ No CCTV

**Comments:** *No comments were provided*

122 Must Do employees display their ID badge at all times while at the facility?

**Question Guidance:** Observe if employees display their ID badge anytime while at the facility. The badge must be visibly displayed and cannot be in a pocket or wallet.

- ◉ Yes
- ○ IDs carried but not displayed
- ○ No

**Comments:** *No comments were provided*

123 Critical Is a documented procedure in place to require visitors to present photo identification upon arrival and have security or other authorized employee record their information in a log? (Select all that apply)

**Question Guidance:** Facilities must maintain a documented policy for managing visitor access to ensure security and accountability. An authorized employee or security personnel must verify the identity of each visitor upon arrival and record their details in a visitor log. The log should include the visitor's name, date and time of arrival, purpose of the visit, and departure time. Additionally, facilities should determine whether visitors are required to present a photo ID for identity verification. A digital record or photograph of the visitor log book should be maintained as part of the facility's security procedures.
(CTPAT MSC 10.2)

- ☑ Documented procedure is available
- ☑ Photo ID are checked
- ☑ Visitor Log is utilized

- [ ] No documented process is in place

**Comments:** *No comments were provided*

---

124 Must Is a documented procedure in place to inspect a visitor's bag before entering and leaving the manufacturing, production or shipping area of the facility?

**Question Guidance:** Upon arrival and exit of facility all visitor bags should be checked by guards, management, or other authorized personnel.

- (•) Yes
- ( ) No
- ( ) Yes - But gaps in implementation were observed

**Comments:** *No comments were provided*

---

125 Critical Is there a documented procedure in place requiring a visitor to be issued a numbered visitor badge which is displayed while at the facility?

**Question Guidance:** Visitors must be given and wear a facility-issued visitor, numbered badge/identification while at the facility. This process must be included in the documented physical security policy.

(CTPAT MSC 10.2)

- (•) Yes (please attach photo of applicable item)
- ( ) No
- ( ) Yes - But gaps in implementation were observed

08.pdf

**Comments:** *No comments were provided*

---

126 Critical Is there a documented policy that requires a visitor to be escorted at all times while at the facility?

**Question Guidance:** All visitors must be escorted by management or other authorized employee while at the facility. This process must be included in the documented physical security policy.

(CTPAT MSC 10.2)

- (•) Yes
- ( ) No
- ( ) Yes - But gaps in implementation were observed

**Comments:** *No comments were provided*

127 Material Is a documented procedure in place to inspect incoming mail and packages prior to distribution?

**Question Guidance:** This is a best practice. Verify that the facility has an established and documented procedure for inspecting all incoming packages and mail to enhance security and prevent the introduction of prohibited, hazardous, or suspicious materials. The documented procedure must include, at a minimum:

-A designated secure area for receiving and inspecting all incoming mail and packages.

-Visual inspection protocols to identify signs of tampering, leakage, or suspicious labeling.

-Clear criteria for recognizing suspicious packages and instructions for escalating concerns to security or management.

-A logging system to record sender, recipient, date/time received, and inspection results for each package.

-Evidence of training provided to employees who handle incoming mail, covering safe handling practices and how to identify and respond to suspicious packages.

(CTPAT MSC 10.8)

- (●) Yes
- ( ) No
- ( ) Yes - But gaps in implementation were observed

**Comments:** *No comments were provided*

128 Material Are hazardous materials or high value goods segregated when stored at the facility?

Only select NA if there are no high value or hazardous material items at the facility.

**Question Guidance:** Cargo must be separated based on domestic, international, high value and/or hazardous. This is a best practice and is encouraged.

(CTPAT MSC 9.2)

- ( ) Yes
- ( ) No
- (●) NA

**Comments:** there are no high value or hazardous material items at the facility.

129 Must Does the facility have a documented procedure in place to validate information provided on an employment application, such as an address, previous employment history, education, personal or professional references, and any applicable certification (as applicable by local law)?

**Question Guidance:** Facilities are required to maintain a documented policy for verifying information provided in employment applications. This process must include validation of addresses, previous employment history, education, personal and professional references, and certifications. Reference checks, a common practice during the hiring process, involve gathering insights about a candidate from individuals who have had professional or personal interactions with them in the past. Documented procedures must be established to screen prospective employees and periodically review current employees. Verification of application details, such as employment history and references, must be conducted prior to employment, as far as feasible and permissible by law.

(CTPAT MSC 11.1)

- (●) Policy is documented
- ( ) Nothing in place
- ( ) Yes - But gaps in implementation were observed

**Comments:** *No comments were provided*

130 Must Does the facility have a documented policy requiring permanent and temporary job applicants to submit a written employment application and provide proof of identity?

**Question Guidance:** Facilities must have a documented policy for validating employment application information. All job applicants must submit a written application and provide proof of their identity. Partial processes are not acceptable - if both are not present and implemented, select the option for not required or collected.

(CTPAT MSC 11.1)

- (●) Yes - Written application and Government issued ID required and collected
- ( ) No - A written application and Government issued ID are not required or collected (partial process is not acceptable)

**Comments:** *No comments were provided*

131 Must If permitted by local law, is there a documented procedure to conduct background checks on applicants and employees working in sensitive areas of the facility, such as personnel, shipping, or

computer systems? This requirement also applies to contract employees.

Only select N/A if background checks are prohibited by local law.

**Question Guidance:** Review the documented procedure for conducting background checks on new hires and current employees, and discuss with HR the methods they use to perform these checks. HR's actions should align closely with the documented procedure's requirements. If background checks are not applicable, the auditor must request the facility to provide evidence, such as local legal provisions or documentation from local law enforcement, confirming that conducting background checks is prohibited under local law.

(CTPAT MSC 11.2)

- (●) Yes, a documented procedure is in place
- ( ) No procedure is in place
- ( ) Yes - But gaps in implementation were observed
- ( ) NA

**Comments:** *No comments were provided*

132 None Which type of check is conducted? (Select all that apply)

- [x] Criminal Check
- [ ] Credit Check
- [ ] Other

**Comments:** *No comments were provided*

133 Must Does the facility have an Employee Code of Conduct that requires employees and contractors to provide a signed acknowledgment, outlining expectations, acceptable behaviors, and penalties or disciplinary procedures?

**Question Guidance:** A Code of Conduct serves to protect the business while clearly outlining expectations for employees. Its primary goal is to establish and uphold a standard of behavior that aligns with the company's values. By doing so, it helps build a professional image and foster a strong ethical culture.

(CTPAT MSC 11.5)

- (●) Yes
- ( ) No
- ( ) Yes - But gaps in implementation were observed

**Comments:** *No comments were provided*

## Security Training & Threat Awareness 100%

134 Must Is a security threat awareness training provided to all new employees and an annual refresher course for current employees? (Select all that apply)

**Question Guidance:** Verify whether the facility has a Threat Awareness program in place. If such a program exists, review training records to confirm that new employees receive initial training and that all employees participate in refresher training annually. Training topics may cover safeguarding access controls, identifying internal conspiracies, and reporting procedures for suspicious activities and security incidents. Whenever possible, specialized training should incorporate hands-on demonstrations, allowing trainees the opportunity to practice and demonstrate the procedures. For CTPAT compliance, sensitive positions include employees handling import/export cargo or related documentation, as well as those responsible for managing access to secure areas or equipment. These roles may include shipping and receiving personnel, mailroom staff, drivers, dispatchers, security guards, and employees involved in load assignments, conveyance tracking, and seal controls.
(CTPAT MSC 12.1)

- [x] Training program is in place
- [x] Training logs are kept to ensure required personnel attend the training
- [x] Management personnel randomly reviews documentation
- [x] Training provided annually for all employees
- [x] Training provided for new employees
- [ ] There is no Threat Awareness training in place

**Comments:** *No comments were provided*

135 Must Is there an evaluation of understanding included at the end of a training session? (Select all that apply)

**Question Guidance:** Auditor should question management to determine if there is an evaluation of effectiveness of understanding. If a minimum score is not achieved, retraining is required. This process should be documented in the training policy.
(CTPAT MSC 12.4)

- [x] Evaluations are conducted

- [x] Retraining is required if a successful score is not achieved
- [ ] No evaluations are conducted

**Comments:** *No comments were provided*

136 Must Does the facility provide training to employees who conduct security and agricultural inspections? (Select all that apply)

**Question Guidance:** Employees in sensitive positions must receive specialized training tailored to their job responsibilities. This training should cover key areas such as IIT inspections, including identifying agricultural security risks, recognizing hidden compartments, and detecting signs of pest contamination. Additional topics include proper cargo handling procedures, verifying the legitimacy of shipping documents, and understanding the specific duties of security personnel. Training must also address procedural security measures related to trade-based money laundering and terrorism financing, as well as cybersecurity protocols and the management of security technology systems. To ensure compliance and accountability, a training log must be maintained, documenting the date of training, names of attendees, and the topics covered.
(CTPAT MSC 12.2, 12.7)

- [x] Training material lists specific requirements
- [x] Training includes all required topics
- [x] Training logs list employees working in this area
- [x] Training provided for new employees with this job function
- [x] Training provided annually for existing employees with this job function
- [ ] No training logs for this specific criteria
- [ ] No training material for this specific criteria

**Comments:** *No comments were provided*

137 Must Does training include security criteria for restricted areas of the facility such as final packing, shipping and receiving? (Select all that apply)

**Question Guidance:** Employees involved in final packing, shipping, and receiving must receive specialized training tailored to their job roles. This training should include access control requirements for sensitive areas, identification of facility-designated sensitive areas requiring restricted access, and an explanation of why these security measures must be followed. Additionally, the training should highlight the risks associated with failing to adhere to access

control protocols. To ensure compliance, a training log must be maintained, documenting the date of training, names of attendees, and topics covered.

- [x] Training material lists specific requirements
- [x] Training logs list employees working in this area
- [x] Training provided for new employees with this job function
- [x] Training provided annually for existing employees with this job function
- [ ] No training logs for this specific criteria
- [ ] No training material for this specific criteria

**Comments:** *No comments were provided*

138 Must Does Threat Awareness training inform employees of procedures to report suspicious activity or a security incident?

**Question Guidance:** If a facility has a Threat Awareness program, it must ensure that employees are trained to recognize and report suspicious activities or security concerns. The training should clearly outline the types of incidents that require reporting, identify the appropriate personnel or department to notify, and provide detailed procedures for submitting a report. Additionally, employees should understand the necessary steps for addressing and resolving security incidents when applicable.
(CTPAT MSC 12.10)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

139 Must Does Threat Awareness training provide additional instruction to shipping and receiving employees regarding access controls, IIT inspections, and security seal control procedures? (Select all that apply)

**Question Guidance:** If the facility has a Threat Awareness program, determine if training provides additional security information pertaining to shipments to include Instruments of International Traffic (IIT) load, inspections, security seals and issues.

- [x] Training includes shipping & receiving controls
- [x] Training includes how to conduct IIT inspections
- [x] Training includes IIT sealing practices

- [x] Training includes how to control seals
- [ ] No specific additional training is in place for shipping & receiving personnel

**Comments:** *No comments were provided*

---

140 Must Does the training program include Threat Awareness, Contraband, Human Smuggling and Terrorism?

**Question Guidance:** Employees must be trained to recognize and report security incidents, including understanding what constitutes a reportable incident, who to notify, and the proper reporting procedures. When applicable, employees should also be informed of the steps to take in resolving an incident. Additionally, the training must cover specific topics such as identifying signs of human smuggling, contraband, and potential terrorism threats.

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

---

141 Must Does the facility have a program to recognize an employee when reporting a security incident or recommending improvements?

**Question Guidance:** Determine if the facility has a program to provide an incentive or recognition to an employee who reports suspicious activity or a suggestion to improve security. This should be documented in a policy. This is a best practice and is encouraged.

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

---

142 Must Does training include identifying pest contamination?

**Question Guidance:** Auditor should question management to determine if agriculture contamination specific training is included. Review the training document/description of training and any sign-in sheets to validate participation.

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

---

143 Must Is there a documented training outlining the risks of Cybersecurity?

**Question Guidance:** Cybersecurity is key to safeguarding a company's assets – intellectual property, customer information, financial and trade data, and employee records, among others. With increased connectivity to the internet comes the risk of a breach of information systems. This risk pertains to businesses of all types and sizes. Measures to secure information technology (IT) and data are important, and employees should be trained on risks of cybersecurity.
(CTPAT MSC 12.8)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

144 Must Is there documented training that specifies the requirement for personnel managing and operating security technology systems to receive operations and maintenance training relevant to their specific areas?

**Question Guidance:** Verify that the facility has an established and documented training program for all personnel responsible for operating and maintaining security technology systems. This includes, but is not limited to, CCTV, access control, alarm systems, and related infrastructure.
(CTPAT MSC 12.9)

- (●) Yes
- ( ) No

**Comments:** *No comments were provided*

## Misc

NA

145 None Describe the front of the factory building including any signage. Please attach a picture.

*No options available*

cổng.jpg

**Comments:** The factory is located in Block 2D3-2D4, CN3-CN8-CN10 Street,Tan Binh Industrial Park, Tan Binh Ward, Bac Tan Uyen, Binh Duong province, Viet Nam. It was fully secured with 6 security guards at 1 main gate, 64 cameras. The facility name is in front of the facility main gate.

146 None Describe the guard station and facility access gates. Please attach a picture.

*No options available*

phòng bv.jpg

**Comments:** There is 1 main gates at the factory with 6 security guard assigned entire packing area, warehouse and the other areas in the factory. Security room is next to the facility gate, the security guards sit in the room, there are internal phones in the security room.

147 None Describe the buildings and structures at this location. Confirm which buildings were included in the audit and which were not. Please attach an overview image of the site and clearly mark the buildings that were visited.

*No options available*

rào xung quanh.jpg

**Comments:** The factory was built with concrete/cement, brick, and metal. There were sufficient CCTV and lighting systems installed. The buildings were locked by proper locking device when not being occupied.

148 None Describe the shipping and receiving areas. Please attach a picture.

*No options available*

kv cont, nhận h... jpg

**Comments:** Shipping area and receiving areas were separated to other areas. They were next to finished good warehouse, monitored by CCTV and patrol by safety guard regularly.

149 None Describe how the perimeter of the facility is protected from unauthorized access. Please attach pictures

*No options available*

an ninh kv.jpg

**Comments:** The perimeter of the facility was monitored by CCTV, safety guard patrol regularly, lighting was provided sufficiently along the facility.

150 None Describe the final packaging area. Please attach a picture.

*No options available*

đóng gói.jpg

**Comments:** Final packing area was separated from the other areas with monitoring by supervisors and CCTV as well.

15 1 None Describe any Instruments of International Traffic (IIT) storage and vehicle parking areas and please attach picture.

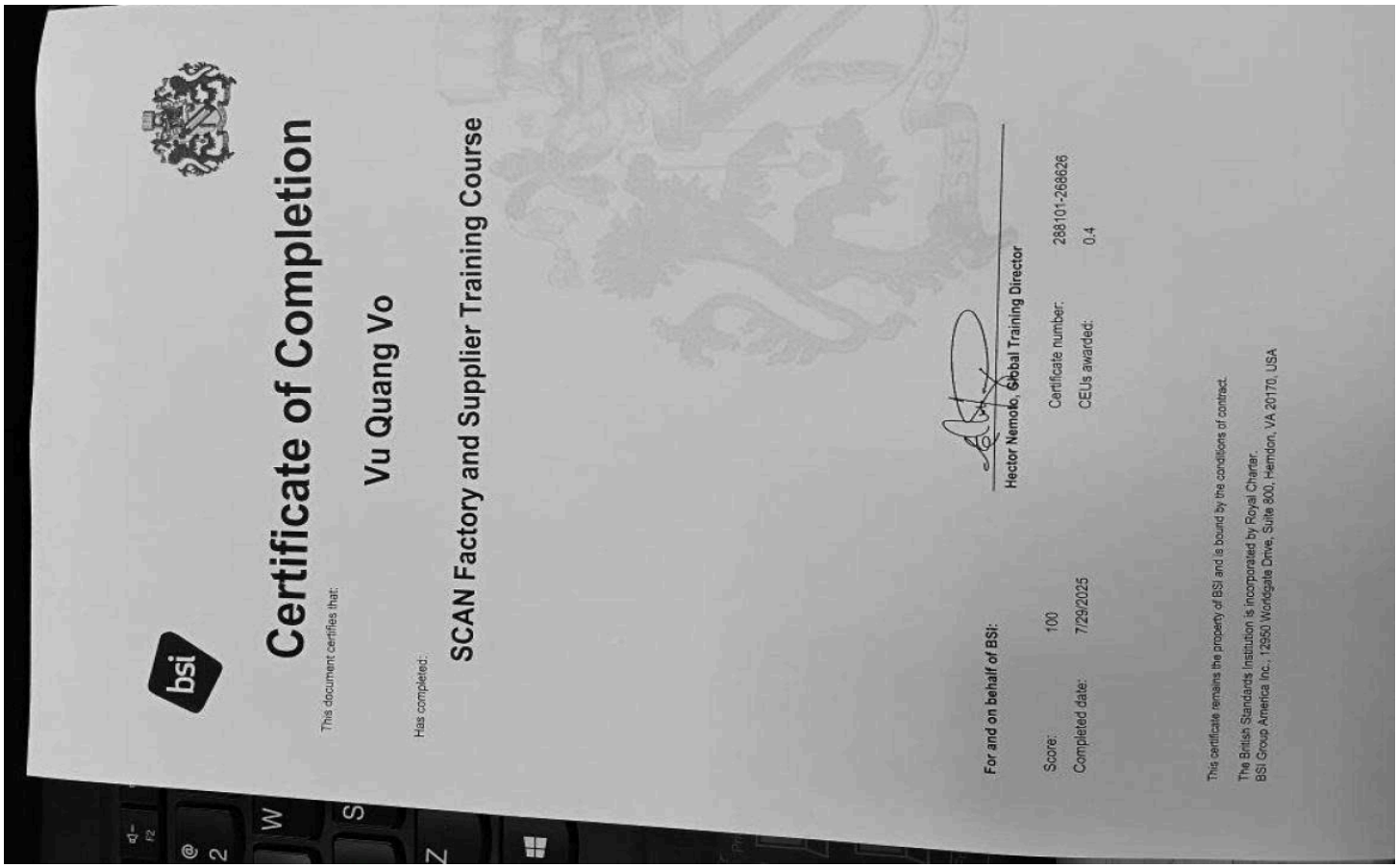
*No options available*

cctv khu lên cont.jpg

**Comments:** Vehicle parking area is in front of security room, with secured by CCTV and safety guards

## Attached Documentation - Photos

### General - Question # 3

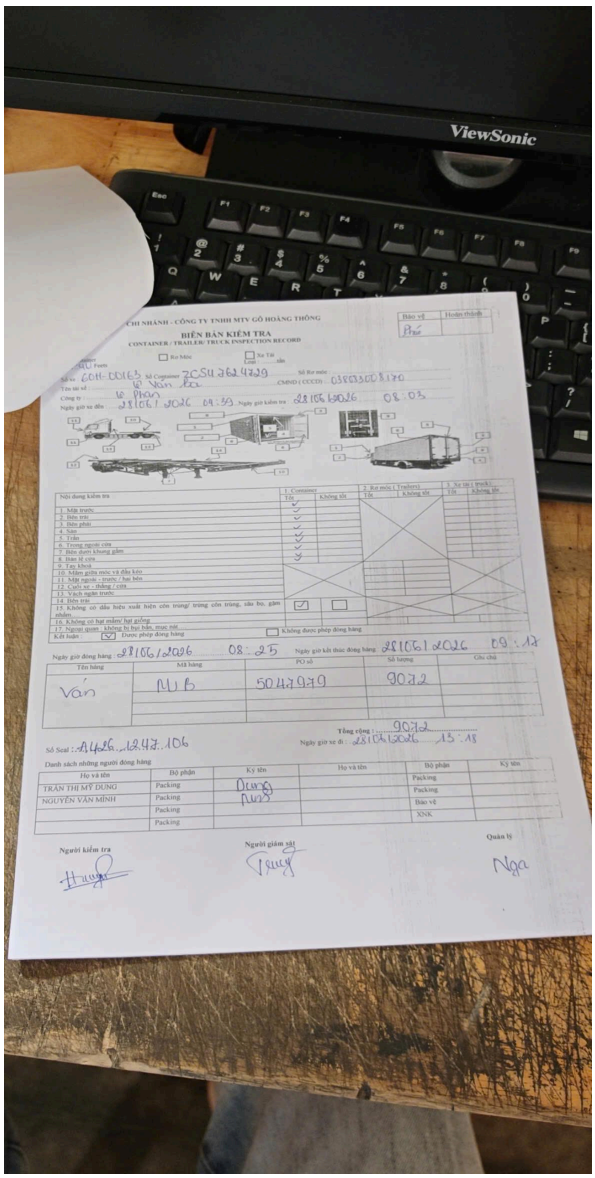



Chứng nhận học.jpg

### Conveyances and Instruments of International Traffic - Question # 44

Kv lưu cont.jpg

**Conveyances and Instruments of International Traffic - Question # 47**

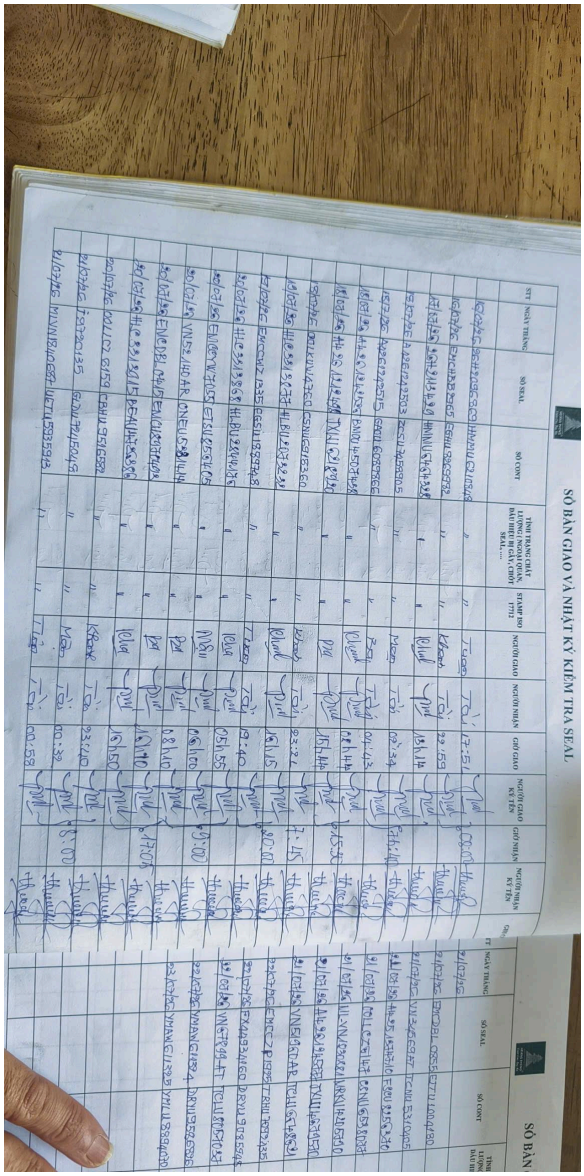



biểu kiểm cont.jpg

**Conveyances and Instruments of International Traffic - Question # 50**

dụng cụ kiểm cont.jpg

**Conveyances and Instruments of International Traffic - Question # 60**




sổ theo dõi cont, seal.jpg

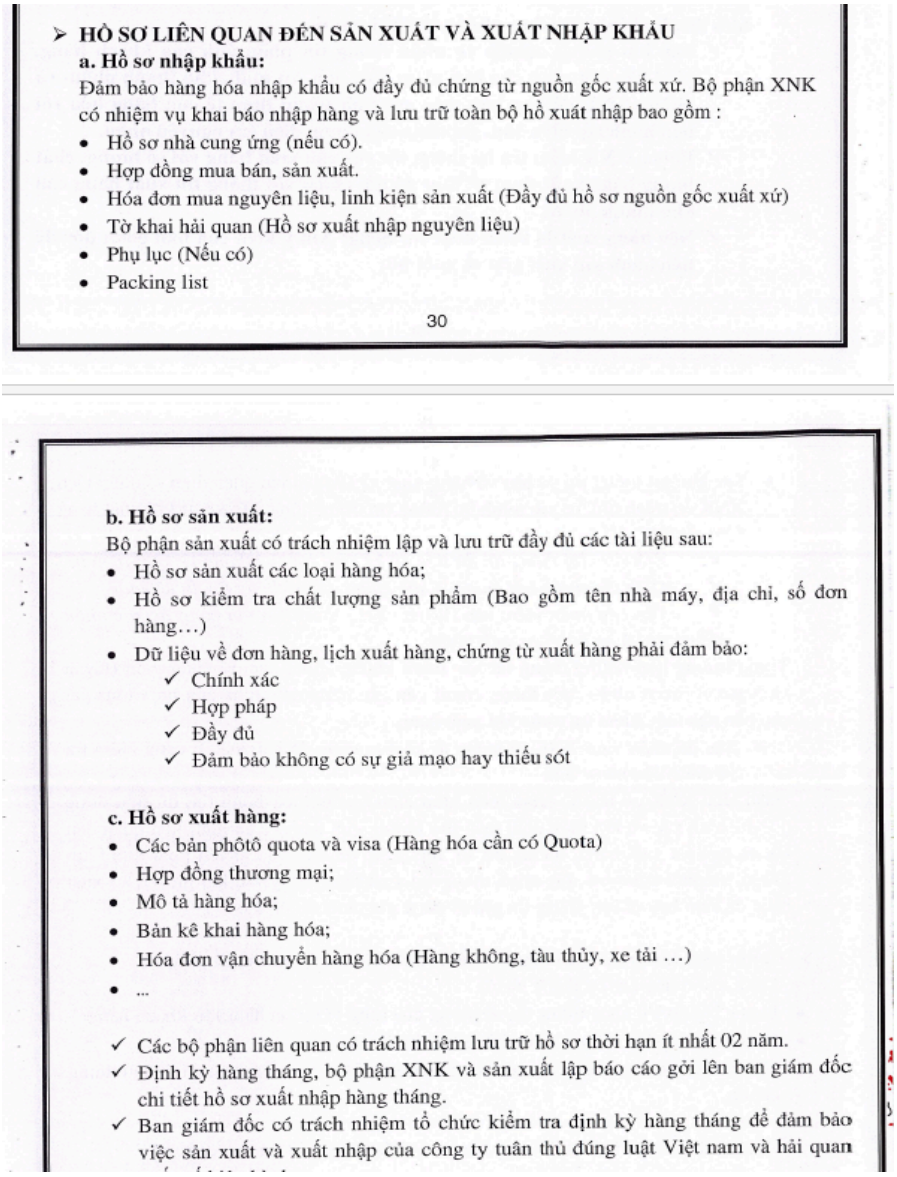
**Seal Security - Question # 79**


tủ seal.jpg

**Procedural Security - Question # 83**

Kv lưu cont.jpg

**Procedural Security - Question # 86**



➢ **HỒ SƠ LIÊN QUAN ĐẾN SẢN XUẤT VÀ XUẤT NHẬP KHẨU**

**a. Hồ sơ nhập khẩu:**

Đảm bảo hàng hóa nhập khẩu có đầy đủ chứng từ nguồn gốc xuất xứ. Bộ phận XNK có nhiệm vụ khai báo nhập hàng và lưu trữ toàn bộ hồ xuất nhập bao gồm :

- Hồ sơ nhà cung ứng (nếu có).
- Hợp đồng mua bán, sản xuất.
- Hóa đơn mua nguyên liệu, linh kiện sản xuất (Đầy đủ hồ sơ nguồn gốc xuất xứ)
- Tờ khai hải quan (Hồ sơ xuất nhập nguyên liệu)
- Phụ lục (Nếu có)
- Packing list

30

**b. Hồ sơ sản xuất:**

Bộ phận sản xuất có trách nhiệm lập và lưu trữ đầy đủ các tài liệu sau:

- Hồ sơ sản xuất các loại hàng hóa;
- Hồ sơ kiểm tra chất lượng sản phẩm (Bao gồm tên nhà máy, địa chỉ, số đơn hàng…)
- Dữ liệu về đơn hàng, lịch xuất hàng, chứng từ xuất hàng phải đảm bảo:
  - ✓ Chính xác
  - ✓ Hợp pháp
  - ✓ Đầy đủ
  - ✓ Đảm bảo không có sự giả mạo hay thiếu sót

**c. Hồ sơ xuất hàng:**

- Các bản phôtô quota và visa (Hàng hóa cần có Quota)
- Hợp đồng thương mại;
- Mô tả hàng hóa;
- Bản kê khai hàng hóa;
- Hóa đơn vận chuyển hàng hóa (Hàng không, tàu thủy, xe tải …)
- ...

✓ Các bộ phận liên quan có trách nhiệm lưu trữ hồ sơ thời hạn ít nhất 02 năm.

✓ Định kỳ hàng tháng, bộ phận XNK và sản xuất lập báo cáo gởi lên ban giám đốc chi tiết hồ sơ xuất nhập hàng tháng.

✓ Ban giám đốc có trách nhiệm tổ chức kiểm tra định kỳ hàng tháng để đảm bảo việc sản xuất và xuất nhập của công ty tuân thủ đúng luật Việt nam và hải quan

QT hồ sơ chính xác.png

**Physical Security - Question # 104**


kv đậu xe khách.jpg

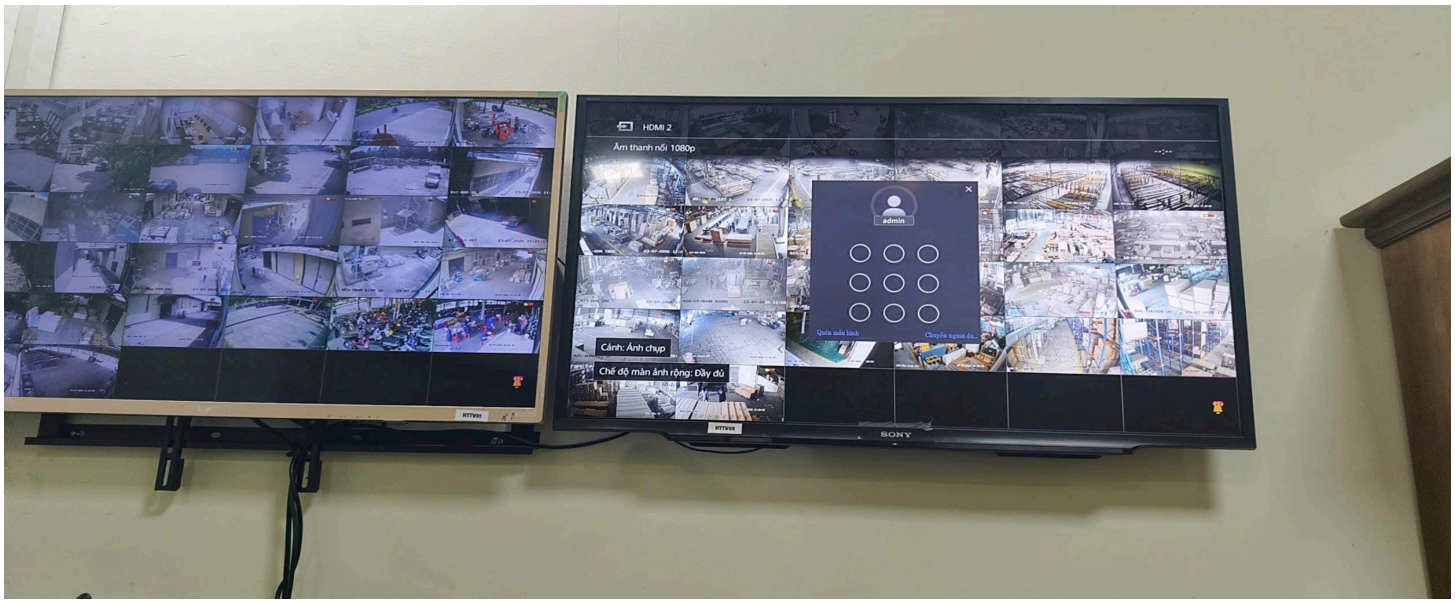
**Physical Security - Question # 107**

hàng rào cổng.jpg

**Physical Security - Question # 108**

hàng rào cổng.jpg

**Physical Security - Question # 118**




cctv.jpg

**Misc - Question # 145**


cổng.jpg

**Misc - Question # 146**


phòng bv.jpg

**Misc - Question # 147**

rào xung quanh.jpg

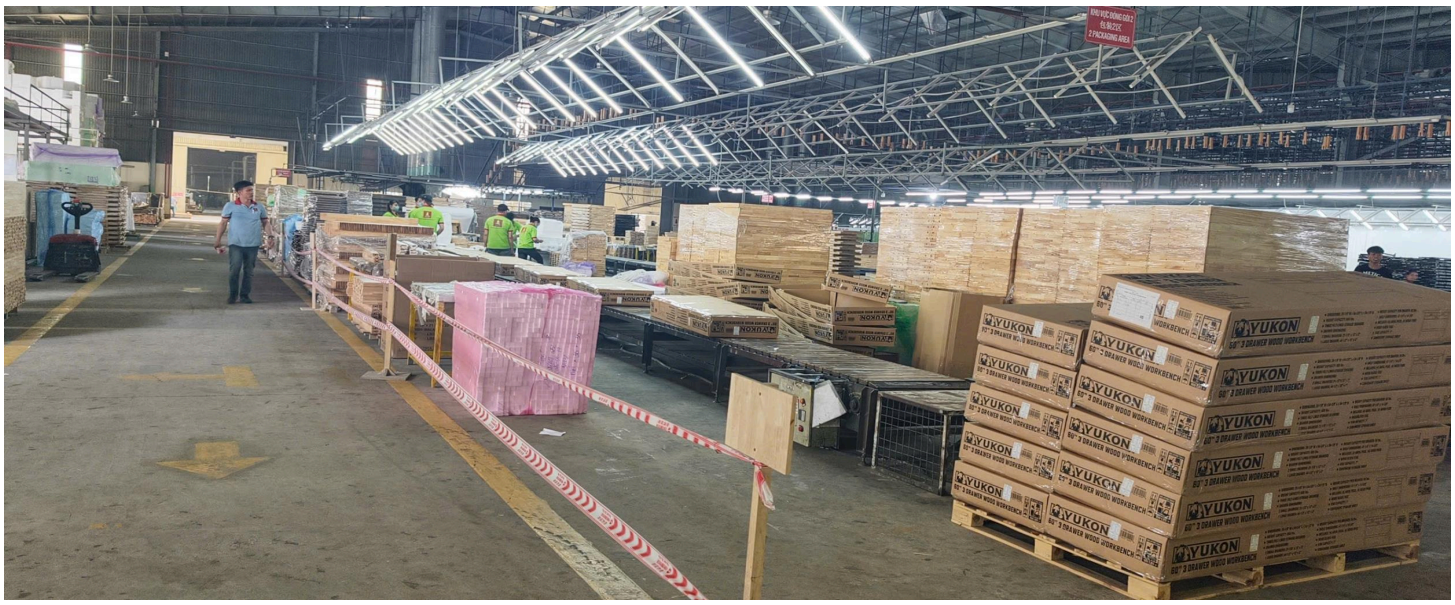
**Misc - Question # 148**


kv cont, nhận hàng.jpg

**Misc - Question # 149**

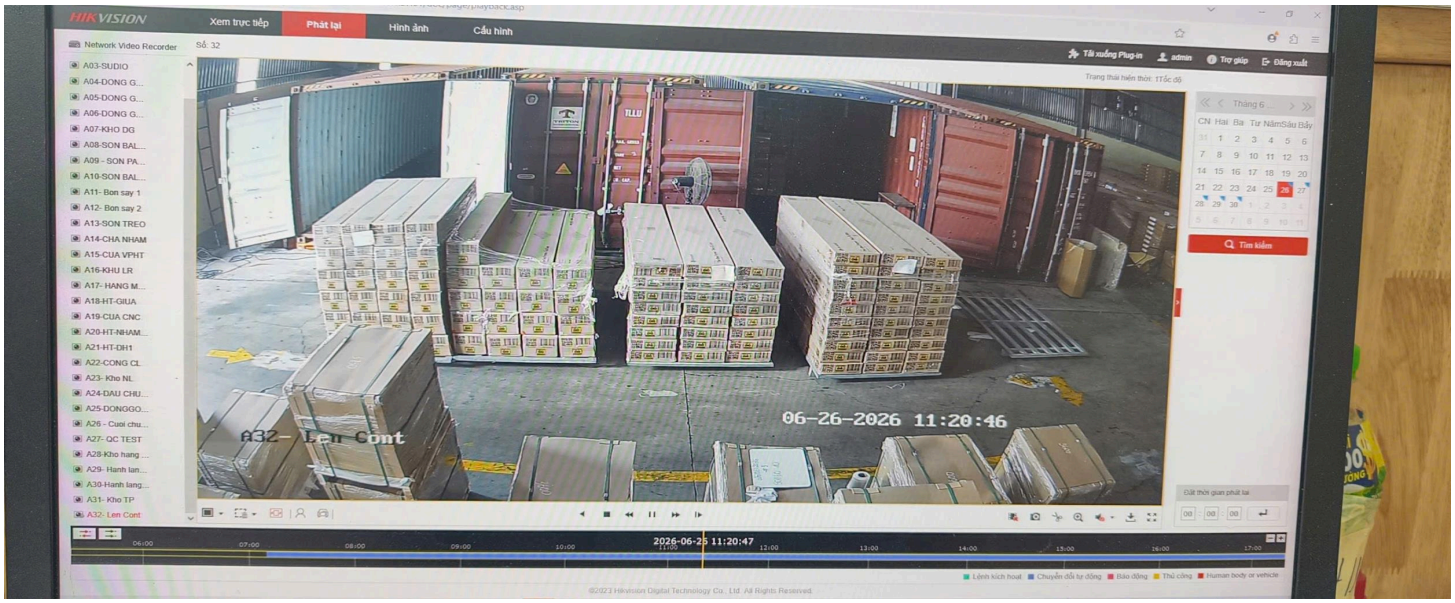
an ninh kv.jpg

**Misc - Question # 150**




đóng gói.jpg

## Misc - Question # 151




cctv khu lên cont.jpg