SCAN
Supplier Compliance Audit Network

DONGGUAN MI-HO PLASTIC ELECTRONIC TECHNOLOGY CO., LTD.

1~3 Floor, Building A, No.139 Yuquan Road, Huangdong Village, Fenggang Town, Dongguan, Guangdong, China 523692 86-18898779075

SCAN SUPPLY CHAIN SECURITY AUDIT (ONSITE)

报告编号	EAC-2026-03-0365-CAPA-V4
审核已提交	Mar 25, 2026
合规性分数	88%
审核类型	外部审计
审计状态	审查
CAPA状态	CAPA 完成
审计到期日	3月 24, 2027

本报告仅适用于 SCAN - Supplier Compliance Audit Network

放弃: 本审计报告仅针对SCAN成员的利益和使用方向编制。未经SCAN事先明确书面许可，不得将本审计报告中包含的任何材料更改，传输，复制或分发给任何其他方。本审计报告中包含的信息涉及与SCAN无关的第三方设施。 SCAN不保证或保证本审计报告中包含的信息的准确性。审核报告不应以任何方式被SCAN视为任何形式的建议。 SCAN对本审计报告的准确性不承担任何责任。
www.scanassociation.com

地点信息

Dongguan Mi-Ho Plastic Electronic Technology Co., Ltd.

1~3 Floor, Building A, No.139 Yuquan Road, Huangdong Village, Fenggang Town, Dongguan, Guangdong, China 523692 86-18898779075

扫描ID	CN08667W9TDO
Point of Contact Name	Mr. Huang Wanshan
Point of Contact Email	stevensd@188.com, 3243379206@Qq.Com, liu2007xi@163.com

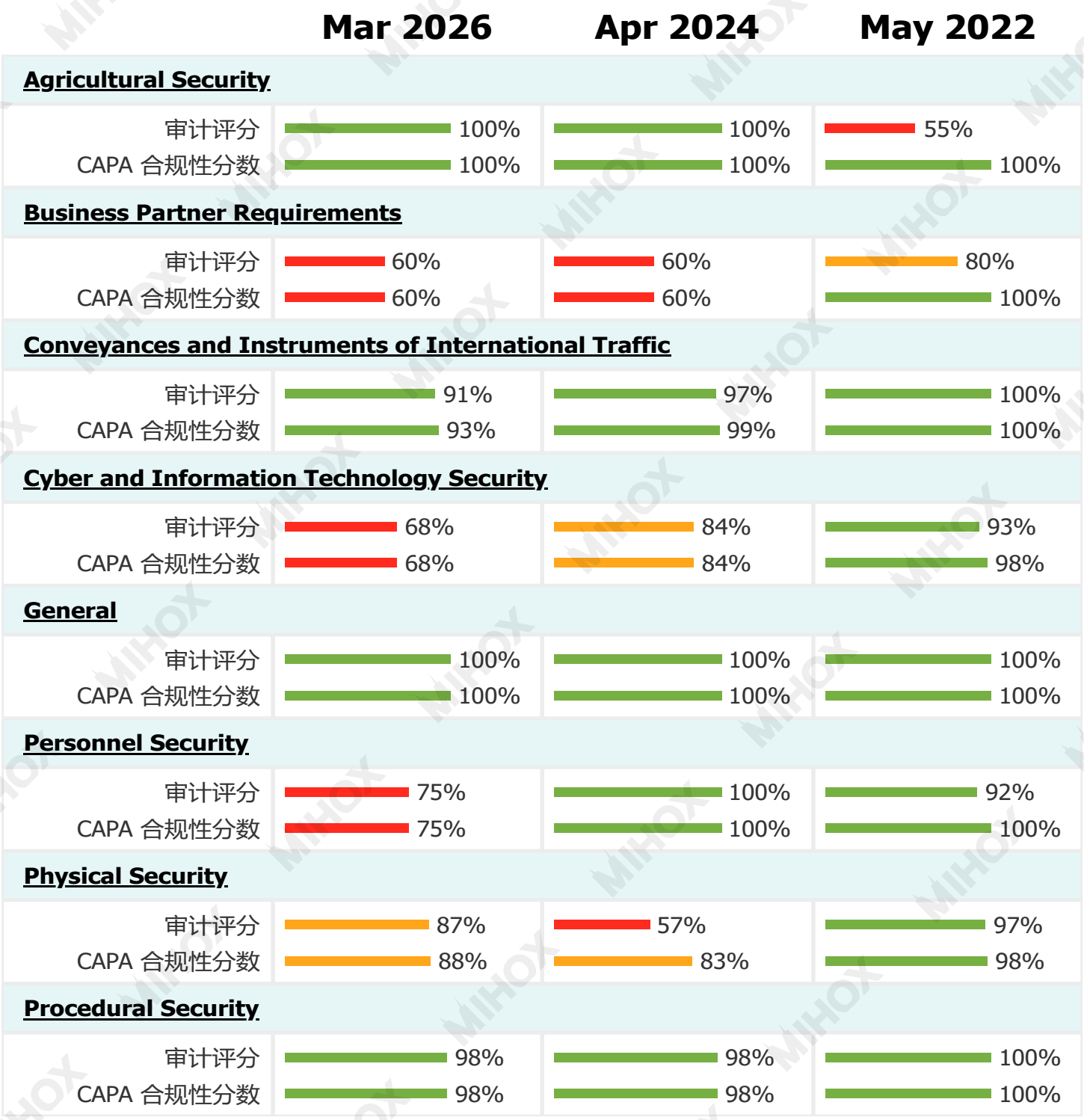
联系人姓名	电话	电子邮件
		3243379206@Qq.Com

地点	Dongguan Mi-Ho Plastic Electronic Technology Co., Ltd.
主要地点	是
关键位置	否
已分配的审核者	Bureau Veritas
安排日期	Mar 20, 2026

审计摘要

	提交日期	合规性分数
CAPA前	Mar 25, 2026	87%
CAPA后	Apr 28, 2026	88%

按类别的合规性 - 最近3次审核



Risk Assessment			
审计评分	89%	100%	100%
CAPA 合规性分数	89%	100%	100%
Seal Security			
审计评分	90%	91%	100%
CAPA 合规性分数	98%	91%	100%
Security Training & Threat Awareness			
审计评分	98%	100%	93%
CAPA 合规性分数	98%	100%	100%

CAPA 前的正确和错误回答计数

Classification Type	Total	Correct Responses		Incorrect Responses	
		Scored	Non Scored	Scored	Non Scored
全部的	**133**	**109**	**1**	**23**	**0**
Critical	34	31	0	3	0
Material	32	29	0	3	0
Must	66	49	0	17	0
None	1	0	1	0	0

业务概况信息

工厂是否参与任何政府、当地海关或世界海关组织 (WCO) 认可的工厂安全计划?	否
工厂是否持有一份政府供应链安全证书?	否
工厂是否经过该计划的审查或审计?	是
主要的业务行业	Manufacturing
产品类型/商品	Plastic toys & cup
成立年份	2013
场地面积（平方米）	6000
建筑数量	2
所有建筑是否都包含在审计范围内？ 如果没有，请说明哪些建筑未被纳入以及原因。	Yes
工厂面积（平方米）	10500
出入口数量？ （即大门、户外门）	1
营业时间	From Monday to Friday Shift 1: 8:00am - 12:00pm / 13:30pm - 17:30pm Injection section in 2 shifts: shift 1: 8:00am - 20:00pm shift 2: 20:00pm - 8:00am of the next day
员工数量	51 - 100
合同工数量	0
内部保安数量	2
合同保安数量	0
外来工数量	0
年收益	1000 万 - 5000 万
该工厂是否外包任何制造服务?	否
如果外包任何生产服务，请描述外包的服务和国家/地区位置。	N/A
该工厂向哪些国家/地区出口?	USA, Japan and Canada etc
识别开展任何工作或存储产品的附属地点。	No
该工厂是否外包任何运输服务?	是

公司名称	联系人电子邮件	联系人电子邮件	百分比的时间
Shenzhen City Hua Ya Da Logistic Co., Ltd	Mr.Liu	thyme173@163.com	100

该工厂是否与任何销售代理或供应商代表合作?	Yes
输入营业执照上显示的此工厂的地址。	1~3 Floor, Building A, No.139 Yuquan Road,Huangdong Village, Fenggang Town, Guangdong City, China
完成本次审计的审计师姓名（名字和姓氏）	Dickie Duan
审计师证书编号	297015-212059
现场工厂代表姓名（名字和姓氏）与电子邮件地址	Mr. Huang Wanshan / Factory Manager /Liu2007xi@163.com
工厂代表邮箱地址	Liu2007xi@163.com

审计回应

审核已分配	到期日	总体合规分数
Feb 25, 2026	**Apr 11, 2026**	**88%**

概述 100%

1 没有 营业执照是否与审计表上所列的该工厂名称和地址相符？ 请附上营业执照的照片。

问题指南: 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)

- (●) 是
- ( ) 否

#1 business lice... jpg

注释: *未提供评论*

2 必须 是否确定了与安全事项相关的主要联络人 (POC)?

问题指南: 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)

- (●) 是 - 提供 POC 的姓名、电话号码和电子邮件地址
- ( ) 否

注释: Mr. Huang Wanshan / Factory Manager, 18898779075, Liu2007xi@163.com

3 没有 准备本次审计时，审计师是否审查了之前的 SCAN 审计 CAPA 信息?

仅在此前未进行过带有已分配 CAPA 的 SCAN 审计时，选择“不适用”。

问题指南: Prior to conducting the SCAN Audit, review previous SCAN Audit CAPA and make note of changes implemented. Regarding previous audits and CAPAs, there is a link to a previous SCAN Audit CAPA if it is available in the Pending Activities within the system. The main POC for any of the Service Providers who have access to the system, will have access to see if there is an available SCAN Audit CAPA. It is possible that other audits were conducted. Only SCAN Audit CAPAs should be reviewed for verification. Other audits/CAPAs (not SCAN related) conducted for this facility should not be considered as part of this SCAN Audit.

- (●) 是
- ( ) 否
- ( ) N/A

注释: *未提供评论*

4 没有 在当前审计期间，是否发现所有之前的 SCAN 审计 CAPA 信息都已按照所提供的 SCAN 审计 CAPA 指示得到妥善解决/缓解?

问题指南: During the SCAN Audit, review prior SCAN Audit CAPA information to determine if the details provided were implemented at the facility as stated.

Answer "Yes" if SCAN Audit CAPA information/updates have been implemented.

Answer "No" if SCAN Audit CAPA information/updates have not been implemented. *Intention is to call out any remediation efforts that were to have been implemented prior to this current audit*

New criteria should not impact previous SCAN Audit CAPAs assigned when reviewing to see if compliant. Any new non-conformances should be addressed during the current audit being conducted.

- ( ) 是
- (●) 否 - 请标出任何被认定未妥善解决/缓解的漏洞

注释: All previous CAPAs were reviewed and verified during the current audit, some or the previous CAPA were still noted:

1.The facility's business partners did not conduct security any risk assessment of their operation.

2.The facility did not require corrective action plans from the business partner with evidence of implementation, if there were areas of non compliance found on the questionnaire.

3.No vulnerability tests were not conducted.

4. There was no written procedure to address returning equipment slated for disposal back to IT.

5. The facility had a procedure to conduct periodic audits of the seal document records, but no audit was

conducted.

6. No security alarm or other technologies used in the factory.

7. The facility's management team did not conduct random and documented reviews of CCTV footage periodically to ensure security procedures are being followed.

8. CCTV recordings were only maintained for 50 days for review.

9. Not all visitors were not required to present photo identification upon arrival, such as no such requirement for auditor on the audit day.

10. The facility did not inspect visitors' bag before entering and leaving the compound of the facility.

5 危急 最近（过去 12 个月内）是否在被审计地点完成了所附 SCAN 工厂和供应商培训在线培训模块?

问题指南: 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.

- (●) 是 - 请附上培训证书的照片
- ( ) 否



#5 training certi...jpg

注释: Mr. Huang Wanshan / Factory Manager participated in the free SCAN Factory and Supplier Training on March 20, 2026.

6 材料 在过去 24 个月内，是否在该地点完成了针对工厂雇佣实践的社会合规或负责任采购审计?

问题指南: 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)

- (●) 是 - 请提供审计日期和审计分数/评级
- ( ) 否 -- 审核报告存档已超过24个月
- ( ) 从未进行/没有存档记录

注释: Audit Date: July 18, 2025

Audit Score: No score on the report

7 材料 工厂是否有记录在案的社会合规计划?

问题指南: 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)

- (●) 是
- ( ) 否

注释: The facility had a documented social compliance program.

风险评估 89%

8 必须 工厂是否对其供应链进行风险评估并进行记录？该评估应包含政策和程序遵从性相关的安全漏洞，以及识别任何潜在的地理威胁。

问题指南: 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)

- (●) 是 - 已审阅完整的风险评估示例
- ( ) 否 - 无法提供示例/未进行风险评估

注释: *未提供评论*

9 必须 是否将工厂风险评估分享给业务合作伙伴和承包商?

问题指南: 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.

- (●) 是
- ( ) 否 - 评估结果不予共享
- ( ) 未进行风险评估

注释： *未提供评论*

10 材料 工厂风险评估是否包括承包商、季节性员工、服务提供商等特定群体具有的漏洞?

问题指南： 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)

- ○ 是
- ◉ 否 - 未包含特定漏洞
- ○ 未进行风险评估

注释： The facility risk assessment did not include vulnerabilities specific to contracted service providers such as seasonal employees, service providers etc.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA： 这是最佳实践。制定并记录一项程序，要求贵组织识别和评估安全计划内的潜在漏洞。该流程应包括对可能存在薄弱环节的领域进行系统性审查，并制定处理和缓解这些漏洞的方法。
如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程，并上传照片以作为完成的证据。否则，请注明您已考虑未来实施此流程。

CAPA 指南： One of the most significant risk areas includes factors beyond the direct control of the company or its management, with contractor-related vulnerabilities being especially critical. Consequently, the documented risk assessment must explicitly identify vulnerabilities that arise from, or are managed by, contracted service providers.

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.

- ○ 已经实施
- ◉ 已知悉 - 将考虑在未来实施

注释： 我们将组织反恐小组对括承包商、季节性员工、服务提供商等特定群体去评估其特有漏洞并制定相关处理措施及缓解方法。预计在2026-06-30内完成

验收意见： 公认

11 必须 是否定期更新工厂风险评估?

问题指南： 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)

- (●) 上次更新在过去 12 个月内
- ( ) 上次更新在 12 个月到 18 个月之间
- ( ) 上次更新在 18 个月到 24 个月之间
- ( ) 未记录有更新或上次更新已在 24 个月之前
- ( ) 未进行风险评估

注释: *未提供评论*

12 材料 工厂是否已实施货物运输管理流程？ （选择所有适用项）

仅在货物运输并非由该工厂管理或协助时，选择"不适用"。
问题指南: 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] 记录在案的货运流程可用
- [x] 货运流程包括从始发地到最终国际运输工具 (IIT) 堆场的运输时间
- [x] 货运流程包括货物可能处于静止状态的位置
- [x] 已实施的货运流程图可供审阅
- [ ] 记录在案的货运管理流程不可用
- [ ] N/A

注释: *未提供评论*

13 材料 制定工厂的危机计划。（选择所有适用项）
问题指南: 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] 有文件化的危机计划
- [x] 危机计划包括必要时向业务合作伙伴报告危机相关问题
- [ ] 危机计划包括工厂无法使用时的替代地点
- [ ] 没有文件化的危机计划

注释: *未提供评论*

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 这是最佳实践。制定并记录一项程序，概述与有关的利益相关方（包括业务合作伙伴和承包商）共享贵工厂危机管理计划的流程。虽然目前尚未强制要求，但这项主动措施未来可能成为一项要求，并将有助于确保在紧急情况下协调响应工作。

如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程，并上传照片以作为完成的证据。否则，请注明您已考虑未来实施此流程。

CAPA 指南: The documented crisis plan must include the following elements:

- A clear definition of the types of crises the facility may face.
- Detailed procedures on how the facility responds to each type of crisis.
- Communication protocols for notifying affected business partners during a crisis.
- Information about alternate locations that would be utilized if the primary facility becomes unusable due to a crisis.

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.

- ○ 已经实施
- ◉ 已知悉 - 将考虑在未来实施

注释: 我们将组织反恐小组按照相关要求去制定危机计划，概述与有关的利益相关方共享工厂危机管理计划的流程，明确可能的危机类型；如何响应的具体行动；在危机期间通知相关合作伙伴的规程；备用点的信息等等。预计在2026-06-30内完成

验收意见: 公认

14 材料 为确保稳健的供应链安全计划，工厂是否已将所有相关部门的代表纳入跨职能团队?

问题指南: 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)

- (●) 是
- ( ) 否

注释: The facility incorporated representatives from all of the relevant departments into a cross-functional team to ensure a robust supply chain security program.

商业合作伙伴要求 60%

15 没有 工厂是否签约使用承包商提供的安保、运输或制造劳务等服务?
问题指南: (CTPAT MSC 3.5)

- (●) 是
- ( ) 否

注释: *未提供评论*

16 必须 工厂是否审查并向业务合作伙伴（特别是为国际供应链活动提供支持的合作伙伴）提供安全标准的副本?
问题指南: 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.

- (●) 是 - 以本地语言审核和提供的安全标准
- ( ) 是 - 安全标准已审查并仅提供英文版
- ( ) 是 - 安全标准已审查，但未提供给业务合作伙伴
- ( ) 否 - 安全标准未被所有供应商伙伴审查

注释: *未提供评论*

17 必须 工厂是否有用于遴择业务合作伙伴（包括材料供应商、制造商和物流服务提供商）的记录在案的程序? （选择所有适用项）

问题指南: 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] 有文件化的筛选流程
- [x] 筛选流程每年进行一次
- [x] 筛选流程包括寻找洗钱和资助恐怖主义的证据
- [x] 筛选流程包括对财务稳定性的监督
- [x] 筛查过程核查CTPAT/AEO认证状态
- [ ] 筛选程序执行尚未发生

注释: *未提供评论*

18 必须 是否要求工厂的签约业务合作伙伴对其运营进行年度安全风险评估?

问题指南: 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-每年
- ○ 是 - 每 2 年
- ○ 是 - 仅在合同生效时

◉ 否

注释: The facility's business partners did not conduct security any risk assessment of their operation.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项程序，要求所有签约业务合作伙伴对其运营进行年度安全风险评估。该程序应概述对评估范围、频率以及如何审查或共享结果的预期要求，以确保符合贵组织的安全标准。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。
- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）

CAPA 指南: The documented procedure must include at a minimum:

- in order to work with facility, business partners must conduct a security risk assessment every year
- business partners must provide risk assessment to facility
- risk assessment must include potential impacts to operations for facility

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.

○ 已经实施

◉ 将要实施

○ 不会实施/不会履行纠正措施请求

注释: 我们将制定相关程序，其内容包含：要求业务合作伙伴每年度定期向我们提供其最新安全风险评估审查；其评估需要涵盖潜在影响；预计2026-06-30内完成

验收意见: 公认

19 必须 工厂是否要求业务合作伙伴提供一份经签署的合规声明，或填写一份强调已落实海关-商贸反恐伙伴计划 (CTPAT) 最低安全要求的调查问卷？ 声明或调查问卷是否每年更新？ （选择所有适用项）

问题指南: 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] 要求提供已签订的合规声明和/或安全调查问卷
- [x] 每年更新一次
- [ ] 否 - 无可用/无要求

注释: *未提供评论*

20 必须 若调查问卷已提供，且在调查问卷中发现不合规领域，工厂是否要求业务合作伙伴制定纠正措施计划，并提供实施行动的证明?

如果使用经签署的合规声明代替调查问卷，则选择"不适用"。

问题指南: 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)

- ( ) 是
- (•) 否
- ( ) N/A

注释: The facility did not require corrective action plans from the business partner with evidence of implementation, if there were areas of non compliance found on the questionnaire.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项程序，说明如果业务合作伙伴未能满足所需安全标准，则必须提交纠正措施计划（CAP 或 CAPA），或提供时间表，概述他们为实现合规将采取的步骤。此流程应确保及时解决不合格项，并符合贵组织的安全预期要求。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照

片。

- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）

CAPA 指南: The documented corrective action plan must include at a minimum:

- timeframe given to business partners to make corrective actions found on security questionnaire/self-audit
- criteria for issuing a corrective action plan to business partners
- criteria for evidence demonstrating implementation

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将针对商业合作伙伴在问卷调查时未遵守规定时后续要求制定相关书面程序，其内容包含：

A.商业合作伙伴必须向本公司提供相关纠正计划。

B.本公司将要求其在三个月内完成整改并提供相关改善证据。

C.向其发送本公司纠正行动计划/证据的标准。

D.若未能在规定时间内完成整改，将考虑将其移除。

备注：我们向其提供改善标准

预计在2026-06-30内完成

验收意见: 公认

网络和信息技术安全 68%

21 没有 该工厂是否联网并部署计算机网络系统?

- ◉ 是
- ○ 否

注释: *未提供评论*

22 必须 工厂是否拥有涵盖全面网络安全/信息安全计划所有必要领域的记录在案的政策和程序手册?

记录在案的 IT 政策必须至少涵盖本网络和信息技术安全审计部分中的所有个人网络安全标准。

问题指南: 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)

- (●) 所有区域均已记录在案
- ( ) 1 个区域缺失
- ( ) 2-3 个区域缺失
- ( ) 3 个以上区域缺失
- ( ) 目前尚未制定任何记录在案的政策或程序

注释: *未提供评论*

23 必须 工厂是否有记录在案的网络安全政策来保护信息技术系统，且该政策每年接受审查和更新?
问题指南: 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)

- ( ) 政策已记录在案，并在过去 12 个月内更新
- ( ) 政策已记录在案，并在过去 12-18 个月内更新
- (●) 政策已记录在案，但上次更新距今超过 18 个月
- ( ) 记录在案的政策不可用

注释: Policy was documented but last update was greater than 18 months ago, last update conducted in July 2023.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项正式的网络安全程序，概述保护所有电子设备免受黑客攻击、未经授权访问或入侵的措施。本政策必须明确预防性控制措施、监控实践和响应程序，以确保系统的完整性和安全性。
- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照

片。

- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）

CAPA 指南: Cybersecurity is an increasingly critical concern in today's operating environment. To ensure adequate protection, the documented cybersecurity procedure must include, at a minimum:

- Clearly defined steps to protect the organization's IT systems from unauthorized access, compromise, or disruption.
- A process for identifying, reporting, and resolving cybersecurity threats and vulnerabilities.
- A requirement for the policy to be reviewed and updated at least annually, or more frequently in the event of policy violations, incidents, or emerging threats.
- Inclusion of all "Must" and "Critical" class requirements outlined in this cybersecurity section to ensure alignment with audit and compliance standards.

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定相关文件，内容包含；必须执行的控制措施：

所有设备必须安装公司批准并集中管理的端点防护软件

必须启用自动操作系统和应用程序安全更新。

必须启用硬件防火墙和主机防火墙。

身份验证： 必须使用唯一的用户ID和强密码（最少12位字符，含大小写字母、数字和符号）。禁止共享凭证。

最小权限原则： 用户仅被授予其工作职责所必需的系统和数据访问权限。权限变更须经正式审批。

离职流程： 人力资源部须及时通知IT部门，立即禁用离职员工的所有访问权限。

网络必须进行分段（如将访客Wi-Fi、办公网络、服务器网络隔离）。

无线网络必须使用强加密协议（如WPA3或WPA2-Enterprise）。

关键要求：敏感数据（如客户信息、财务数据、知识产权）在存储和传输时必须进行加密。

定期对关键数据进行安全备份，备份数据需异地存储并定期测试恢复流程。

所有新员工入职时必须接受基础网络安全培训。

必须要求：全体员工须每年至少参加一次强制性的安全意识更新培训，内容涵盖钓鱼邮件识别、社交工程、安全操作规范等。所有关键系统（服务器、网络设备、防火墙、应用程序）的安全日志（如登录尝试、访问记录、配置更改）必须收集并发送至中央安全信息。日志必须保留至少90天，以满足取证和合规需求。

IT安全团队监控针对可疑活动（如多次失败登录、异常数据外传、恶意流量模式）的自动警报。

定期进行漏洞扫描和渗透测试，至少每季度一次，对发现的高危漏洞必须立即处理。及时了解新兴威胁和漏洞，并评

估其对本公司环境的影响。

任何用户一旦发现可疑活动，必须立即通过指定电话向IT报告。IT作为事件接收中心，进行初步分类后立即上报给安全响应团队。 采取措施防止事件扩大。 找出根本原因，从系统中彻底清除威胁（如清除恶意软件、修复漏洞）。在确认安全后，将受影响的系统和数据从干净备份中恢复，并恢复正常运营。

每个重大安全事件处理后，必须进行事后分析，形成事件报告。报告必须包括：

根本原因分析、纠正措施、预防措施。

本政策必须至少每年由安全负责人牵头进行一次正式审查和更新。在发生以下情况时，必须进行临时审查和更新：

发生重大的政策违规或安全事件后。引入新的技术或业务模式带来重大风险变更时。出现重大的新兴威胁时。相关法律法规发生重大变化时。预计2026-06-30内完成

验收意见： 公认

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释： 我们将制定相关文件，内容包含；指派工程部主管每月对公司的网络进行访问控制；防火墙配置；数据加密；更新和补丁管理；漏洞扫描；部署入侵检测系统等检查。若发现任何缺陷/漏洞立即根据以下几个步骤执行，访问控制设置；修改系统版本；关闭存在漏洞的服务；补丁修复；系统版本升级等；发现安全威胁、漏洞立即向安全主任报告；至少每年定期更新程序，若发生政策违规、各种事件或新兴威胁，审查和更新日期将会缩短。预计2026-06-30

重新打开评论： 计划不当。 请在评论框中提供您的计划和未来时间表，以便每年更新网络安全政策。

24 必须 工厂是否安装有防火墙和防恶意软件来识别、保护、检测、响应和恢复其网络？ （选择所有适用项）

问题指南： 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)

- ☑ 已部署防火墙
- ☑ 已安装防恶意软件
- ☐ 未部署防火墙或防恶意软件

注释： *未提供评论*

25 必须 防火墙和防恶意软件的更新频率如何？

问题指南: 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
- ( ) 视需要由现场 IT 服务人员手动安装更新
- ( ) 未执行更新
- ( ) 未部署防火墙或防恶意软件

注释: *未提供评论*

26 必须 工厂是否制定了预防社会工程学攻击的记录在案的程序?

问题指南: 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)

- ( ) 是
- (●) 否

注释: The facility did not a documented procedure to prevent attacks via social engineering.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项程序，用于防范社会工程学攻击。
- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。
- 如果将要实施，请在文本框中分提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: This documented procedure must include employee awareness training, verification protocols for identity confirmation, guidelines for handling sensitive information, and steps to recognize and report suspicious activities.

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定预防社会工程学攻击程序。内容包含：对员工反恐意识的培训、对外来人员身份确认的验证规程、对网络敏感信息处理规程，以及识别和报告可疑活动的章程。预计在2026-06-30内完成

验收意见: 公认

27 必须 如果发生数据泄露或其他不可预见事件导致数据和/或设备丢失，工厂是否制定了包含 IT 系统和/或数据恢复（或更换）的程序?

问题指南: This must be addressed in the question above that references the documented policy and procedure documentation collection.

(CTPAT MSC 4.2)

- ◉ 是
- ○ 否

注释: *未提供评论*

28 必须 是否至少每年进行一次测试场景，以识别会造成内部网络访问漏洞的开放端口和 IP 地址?

问题指南: 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)

- ○ IT 人员每年至少进行一次漏洞测试
- ◉ 不执行漏洞测试

注释: No vulnerability tests were not conducted.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项程序，至少每年执行一次测试场景，以识别所有可能造成内部网络面临未经授权的访问或漏洞风险的开放端口和 IP 地址。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。
- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: This documented procedure must outline the frequency, scope, and methods of testing—such as vulnerability assessments, penetration testing, and simulation exercises—to proactively detect and address weaknesses in the organization's security posture. The documented policy must include, at a minimum:

- A clear explanation of the types of vulnerability tests conducted.
- Identification of the personnel or third parties responsible for conducting the tests.
- The frequency at which each type of test is performed.
- Detailed steps for resolving any gaps or vulnerabilities identified through testing.

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定网络测试场景程序，内容包含：1.实施的漏洞测试类型，漏洞评估：对指定的IP地址范围进行系统性扫描，识别已知的漏洞、错误配置和不当开放的端口。；渗透测试：在漏洞评估的基础上，由安全专家模拟真实攻击者的技术手段，尝试利用发现的漏洞来验证其可利用性和实际风险。分为网络外围渗透测试和内部网络渗透测试；模拟攻击：针对性地模拟高级持续性威胁，测试整个组织的检测和响应能力。工程部主管负责测试，漏洞评估每季度一次；渗透测试至少每年一次；演练每两年一次 。测试结束后，执行方需提供详细的报告，包括漏洞描述、风险等级。信息安全团队对已修复的漏洞进行重新扫描或验证，确认问题已解决后关闭工单。预计2026-06-30内完成
验收意见: 公认

29 必须 在测试防火墙、恶意软件和其他网络漏洞时发现问题后，是否采取了纠正措施？ 请说明将如何解决这些问题。

问题指南: 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)

- ○ 是
- ○ 否
- ◉ 不执行漏洞测试

注释: No vulnerability tests were not conducted.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项网络安全程序，明确在测试防火墙、恶意软件防御和其他网络漏洞期间发现问题时，启动和管理纠正措施的流程。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程，并上传已安装的自动化系统/软件的数字照片以作为完成的证据。
- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: This documented procedure must include:

- Procedures for documenting identified problems.
- Steps for assessing the severity and impact of vulnerabilities.
- Assigned responsibilities for remediation efforts.
- Timelines and tracking mechanisms for resolving issues.
- Verification and validation processes to ensure corrective actions are effective.

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定相关程序，内容包含：记录已发现的问题将立即录入统一的系统；由安全主任牵头，联合系统管理员和网络工程师，对每个漏洞进行评估并划分等级；划分整改工作的责任；解决问题的时间表和跟踪机制，为每个优先级的漏洞设定明确的修复截止日期，并持续跟踪。紧急风险： 24-48小时内必须修复或实施缓解措施。高风险：15天内完成修复。中风险： 30-60天内完成修复。低风险： 90天内修复或接受风险；有效性确认（预防类似问题）：流程改进： 审查漏洞产生的原因。例如，如果是因补丁更新不及时，则强化补丁。预计2026-06-30内完成

验收意见: 公认

30 材料 工厂向谁报告网络安全威胁和未经批准的网络系统访问尝试？ （选择所有适用项）

问题指南: 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] 高级管理层
- [x] 内部业务合作伙伴
- [x] 外部业务合作伙伴
- [x] government agencies
- [ ] 未制定报告流程和程序

注释: *未提供评论*

31 必须 是否有自动化系统来监控和防止未经授权的访问和篡改系统和/或电子数据?

问题指南: 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)

- (●) 是
- ( ) 否

注释: *未提供评论*

32 必须 是否对任何违反 IT 系统政策和程序的违规人员采取了纪律处分?

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

- (●) 是
- ( ) 否

注释: Disciplinary action was taken against anyone identified violating IT systems policies and procedures.

33 必须 管理层是否定期审查具有网络访问权限的用户，以便限制其仅访问那些执行当前工作要求所必需的应用程序?

问题指南: 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)

- ○ 每月进行一次管理审查
- ○ 每季度进行一次管理审查
- ○ 每年进行一次管理审查
- ◉ 未进行管理审查

注释: Management did not regularly review the users who had network access in order to restrict access to only those applications required to perform current job requirements.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项网络安全程序，要求管理层和/或 IT 部门定期审查网络访问权限，以确保仅向授权用户授予访问权限，且权限范围仅限于当前工作职责所需。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。
- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: The documented procedure must include:

- Access is granted only to authorized individuals and strictly limited to applications necessary for performing current job responsibilities.
- A clearly defined process for management and/or IT to review employee application and system access.
- A review frequency of at least once per month.
- Guidelines to restrict access to only those systems and applications required to perform the employee's current job duties.
- Procedures for modifying or revoking access when an employee's role changes or upon separation from the organization.

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定相关文件，内包含；访问控制核心原则，最小权限政策明确： 公司的《信息安全管理制度》中明确规定，所有用户的访问权限授予必须遵循"最小权限原则"。即：仅向授权个人授予其履行当前工作职责所必需的最少应用程序和系统访问权限。 禁止授予任何非必要的"宽泛"或"默认"权限。审查流程：部门负责人每月定期逐一核实每位下属的权限是否与当前职位匹配。对于不匹配的权限（过多或过少），负责人在报告上标注并签字确认，返回给IT安全部门。IT安全部门在收到确认报告后的三个工作日内，完成权限的调整操作。除定期审查外，当发生以下事件时，会立即触发审查流程：员工职位变动或部门调动。员工参与新的项目（需要临时权限）。员工离职。职责变更时：人力资源部在收到职位变动通知后，会立即向IT安全部门和原部门/新部门负责人发送《权限变更通知单》。
IT安全部门将根据新职位的工作需求，先撤销其所有旧权限，再重新授予新职位所必需的权限，避免权限累积。
员工离职时：
人力资源部在确认离职日期的同时，会立即通知IT安全部门。
IT安全部门将在离职生效日当天立即禁用该用户的所有账户和访问权限，而非简单地删除，以便后续审计追溯。预计2026-06-30内完成

验收意见: 公认

34 必须 是否有记录在案的程序来取消那些被解雇或休长假的员工的网络访问权限?

问题指南: 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)

- ◉ 是，记录在案的流程包括长期休假以及离职员工访问权限的撤销
- ○ 是，记录在案的流程可用，但不包括长期休假员工访问权限的撤销，仅涉及离职员工访问权限的撤销
- ○ 在审计期间，没有用于撤销离职员工网络访问权限的记录在案的流程

注释: *未提供评论*

35 必须 工厂如何管理对计算机的访问?

问题指南: 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)

- (●) 密码和/或口令
- ( ) 生物识别技术
- ( ) 电子身份证
- ( ) 多因素身份验证 (MFA)
- ( ) 无需凭证

注释: *未提供评论*

36 必须 若采用密码或口令，是否确保其具备足够复杂度并定期更改？（选择所有适用项）

如果尚未采用密码或口令，则选择"不适用"。
问题指南: 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)

- [ ] 必须采用复杂密码
- [x] 定期更改密码
- [ ] 无需采用复杂密码或定期更改密码
- [ ] N/A

注释: Passwords was not complex for 1 out of 3 sampled computers.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项程序，通过实施严格的密码和口令管理措施，保护 IT 系统免遭入侵。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。

- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: This procedure must include guidelines to ensure that all passwords and passphrases are:

- Safeguarded against unauthorized access,

- Created using complexity requirements (e.g., minimum length, character variety), and

- Changed periodically according to a defined schedule.

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定相关程序：内容包含：防止未经授权的访问

安全存储与传输： 所有系统密码均以加密形式，禁止明文存储。在传输过程中，必须使用加密通道

访问尝试限制： 系统对所有账户实施登录失败锁定策略（例如，连续5次失败尝试后锁定账户15分钟），并记录所有异常登录行为，以抵御暴力破解。

会话管理： 设置会话超时（如15分钟无操作自动注销），防止因终端未锁屏导致的未授权访问。

密码策略通过统一的身份认证管理系统在技术上强制执行，用户在创建或修改密码时必须满足以下最低要求：

最小长度： 不少于 12个字符。

字符多样性： 必须同时包含以下四类字符中的至少三类：

大写英文字母（A-Z）

小写英文字母（a-z）

数字（0-9）

特殊符号（例如：!@#$%^&*）

密码历史检查： 新密码不得与近期使用过的（如最近24次）密码重复。

禁止使用弱密码： 系统后台设有常见弱密码字典库（如Password123!、公司名+年份），会自动拒绝此类密码设置

标准变更周期： 所有用户密码必须每90天更改一次

例外情况下的立即变更： 在发生安全事件（如怀疑密码泄露）、员工离职或职责重大变更后，相关账户密码将被要求立即重置。预计2026-06-30内完成

验收意见: 公认

37 必须 计算机终端是否按员工配置专有账户?

问题指南: 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)

- (●) 是
- ( ) 否

注释: *未提供评论*

38 必须 如果员工和/或承包商得到允许以远程访问信息技术 (IT) 系统，是否使用虚拟专用网 (VPN) 或类似软件来控制访问?

问题指南: 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)

- ( ) 允许远程访问，并使用 VPN 或类似软件
- ( ) 允许远程访问，但没有 VPN 或类似软件用于控制访问
- (●) 不允许远程访问

注释: *未提供评论*

39 必须 是否所有网络安全政策都适用于接入网络的个人设备?

问题指南: 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)

- ○ 所有安全政策均适用于个人设备，工厂不允许个人设备在未使用 VPN 或类似软件的情况下连接到网络
- ◉ 工厂不允许使用任何个人设备接入网络
- ○ 所有安全政策均适用于个人设备，但不需要使用 VPN 或类似软件
- ○ 安全政策不适用于个人设备，个人设备可接入工厂网络

注释: *未提供评论*

40 材料 IT 安保部门是否对下载软件和访问外部网站进行限制和监控?

问题指南: 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)

- ◉ 是
- ○ 否

注释: *未提供评论*

41 材料 该工厂备份数据的频率如何?

问题指南: 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)

- ○ 每日备份数据
- ○ 每周备份数据
- ◉ 每月备份数据
- ○ 未执行数据备份

注释: *未提供评论*

42 材料 数据备份是否存储在异地并加密？（选择所有适用项）

问题指南: 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)

- ☑ 数据备份存储在场外
- ☑ 数据备份已加密
- ☐ 数据未存储在场外，也未加密
- ☐ 未执行数据备份

注释: *未提供评论*

43 必须 是否制定了将计划处置的设备退回 IT 部门的记录在案的程序?

问题指南: 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)

- ○ 是
- ◉ 否

注释: There was no written procedure to address returning equipment slated for disposal back to IT.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项网络安全程序，以管理计划处置的设备退回 IT 部门的事宜。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。

- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: This documented procedure must ensure that all equipment is securely collected by the IT department to be properly sanitized of sensitive data and handled in accordance with organizational security and disposal policies.

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定相关程序，内容包含：

第1步：发起申请与审批

设备用户或所在部门通过IT服务管理系统提交“IT资产处置申请”，说明设备信息及退役原因。

第2步：安全收集与登记

申请人将计划处置的设备送至指定的IT设备回收处，禁止随意放置或丢弃。

第3步：销毁： 使用认可的硬盘粉碎机进行现场销毁。

证据留存： 对销毁过程拍照或录像。

预计2026-06-30内完成

验收意见: 公认

44 必须 是否制定了根据适当行业指南对 IT 设备进行妥善清理或销毁的流程?

问题指南: 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)

- ◉ 是

○ 否

注释: *未提供评论*

国际交通运输及工具 93%

45 没有 工厂是否用国际运输工具 (IIT) 装载?

问题指南: 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.

◉ 是

○ 否

注释: *未提供评论*

46 危急 在工厂的控制范围内或运输途中，是否以安全的方式存放 IIT（无论位于现场或场外）？（选择所有适用项）请附上各个适用区域的照片。

问题指南: 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)

☑ IIT 存放区既没有停放个人车辆，也没有存放任何其他物品

☑ IIT 存放区受到保护和/或监控（请说明）

☑ 储存、装载的 IIT 均加贴封条予以封存

#46 container lo...jpg

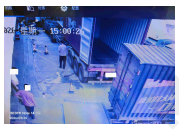
- [x] 在工厂控制期间保障 IIT 安全的记录在案的程序可用
- [ ] IIT 存放不符合最低安全要求（请说明）

注释: Container was stored at a designated secured area and mornitored by security guard and CCTV.

47 危急 您是否能够通过闭路电视录像监督正在进行的 IIT 检查或之前完成的 IIT 检查?

问题指南: 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.

- (●) 是
- ( ) 否



#47 IIT inspecti... jpg

注释: Per CCTV records review, IIT inspection was conducted by designated person.

48 危急 是否制定了记录在案的程序，用于在 IIT 装载前检查其安全完整性，且包括所有最低要求?

问题指南: 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)

- (●) 是 - 请附上第 1 页的图像
- ( ) 未制定记录在案的程序
- ( ) 记录在案的程序仅包含指南中所示的部分要求

#48 written pro... jpg

注释: *未提供评论*

49 危急 装载前对 IIT 进行的记录在案的检查是否包括所有最低要求领域? （选择所有适用项）

问题指南: 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)

- [x] 使用检查表 (请上传检查表照片附件)
- [x] IIT 尺寸
- [x] IIT 编号
- [x] 检查人员姓名
- [ ] 检查的日期和时间
- [x] IIT 的地板和顶部完好无损，无孔洞或泄漏
- [x] 内/外墙体，底盘无损坏
- [x] 包括对入侵物种（例如蛋、巢、污垢、种子）的检查
- [ ] 主管签名
- [ ] 未完成检查或未记录检查

#49 container i... jpg

注释: *未提供评论*

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

包括在得分中

CAPA: 制定并记录一项程序，以确保在装载前进行的所有国际运输工具 (IIT) 检查均涵盖所有最低要求的检查区域。

请在文本框中提供有关纠正措施的完成/实施时间和方式的摘要。另请上传一份空白检查表和一份填妥的检查表副本，以便审查。

CAPA 指南: The documented procedure must include:

- Use of a standardized inspection checklist (paper or electronic)
- Documentation of the Instruments of International Traffic (IIT)'s size and identification number
- Name of the individual conducting the inspection
- Date and time of the inspection
- Assessment of the condition of: Floor; Roof; Inside/Outside walls; Undercarriage; Presence of pest contamination (e.g., eggs, nests, dirt, seeds)
- Supervisor's signature confirming the inspection was completed accurately and thoroughly

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.

- (●) 已经实施
- ( ) 不会实施/不会履行纠正措施请求

货柜检查.pdf

注释: 我们已经根据反恐要求制定了相关检查表，内容包含了必须检查的项目如：

使用标准化检查清单（纸质版或电子版）

- 国际运输工具 (IIT) 的尺寸和识别编号文档
- 执行检查的人员姓名
- 执行检查的日期和时间
- 评估以下情况：地板；屋顶；内/外墙体；底盘；虫害污染迹象（例蛋、巢、污垢、种子）

-确认检查已准确且彻底完成的主管签名

验收意见: 公认

---

50 必须 记录在案的检查流程是否包括检查 IIT 的外部硬件，以确保其具备充分的防拆卸能力?

问题指南: 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)

- ( ) 是
- (●) 否

注释: There was no documented inspection process include inspection of the external hardware of the IIT to ensure that it was properly equipped to withstand attempts of removal.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项程序，要求所有国际运输工具 (IIT) 检查均涵盖对外部硬件的全面审查。该审查必须确保所有硬件组件均已牢固安装，并能够防范篡改或拆卸风险。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照

片。

- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: The documented procedure must include, at a minimum:

- Visual and physical inspection of locking mechanisms, hinges, and seal housings
- Verification that all hardware is intact, undamaged, and free from signs of tampering
- Documentation of inspection findings on a standardized checklist
- Designation of responsible personnel and required training
- Escalation process if defects or 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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将会制定相关检查表并留存，检查表内容包含： 对门锁装置、铰链和密封壳体进行目视检查和物理检查

- 验证所有硬件完好无损且无篡改迹象
- 在标准化检查清单上记录检查结果

预计在2026-06-30内完成

验收意见: 公认

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将会制定相关检查表并留存，检查表内容包含： 对门锁装置、铰链和密封壳体进行目视检查和物理检查

- 验证所有硬件完好无损且无篡改迹象
- 在标准化检查清单上记录检查结果

重新打开评论: 请在评论框中为您提交的纠正措施计划添加预计在不久的将来完成的日期。

51 材料 IIT 装载过程中是否拍摄了照片和/或闭路电视录像？ （选择所有适用项）

问题指南: 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] 已拍摄照片
- [x] 已录制视频
- [ ] 未拍摄视频或照片，或未覆盖所需区域

#51 photos take... jpg

注释: *未提供评论*

52 危急 发货区是否使用了适当的设备来执行 IIT 七点检查法？ （选择所有适用项）

请附上用于执行该 IIT 检查的所有设备的照片。

问题指南: 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.

- [ ] 测量工具
- [x] 起落架的镜子
- [x] 敲击测试工具
- [x] IIT 内部清洁工具
- [ ] 无可用工具/工具不符合要求
- [ ] 未进行 IIT 检查

#52 equipment ... jpg

注释: *未提供评论*

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

包括在得分中

CAPA: 制定并记录一项程序，概述国际运输工具 (IIT) 的检查规范，具体说明如何执行所需的七点检查法。在文本框中，准确描述用于执行此类检查的设备，并附上所用设备的佐证照片以作为证据。在文本框中，准确描述用于执行此类检查的设备，并附上所用设备的佐证照片以作为证据。

请在文本框中提供有关纠正措施的完成/实施时间和方式的摘要。另请上传一份空白检查表和一份填妥的检查表副本，以便审查。

CAPA 指南: The documented procedure must, at a minimum, include the following inspection equipment requirements:

- A measurement tool such as a laser distance measurer, pre-measured string, or tape measure to verify Instruments of International Traffic (IIT) dimensions
- A mirror designed for undercarriage inspections (note: cosmetic or makeup mirrors are not acceptable)
- A mallet or hammer to test wall integrity and identify hidden compartments or weak points
- A tool to sweep or clean the inside of the IIT, such as a broom, air blower hose, or shop vacuum

This procedure ensures that inspections are thorough, standardized, and supported with the proper tools to identify potential security risks effectively.

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.

- (●) 已经实施
- ( ) 不会实施/不会履行纠正措施请求

检查工具.pdf

注释: 我们已经有了下面检查工具：车底探视镜、卷尺、锤子、扫帚

验收意见: 根据评论和证据接受

53 必须 IIT 检查是否在安全区域和闭路电视监控下进行？ （选择所有适用项）

问题指南: 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 检查区域在闭路电视上可见
- [x] 在闭路电视上可看到 IIT 内部从尾部到前端的情况
- [x] inspections are conducted in a secured area
- [ ] 检查既未被闭路电视录像，也未在安全区域进行
- [ ] 未进行 IIT 检查

注释: *未提供评论*

54 必须 工厂是否保存培训记录，说明哪些员工接受过 IIT 七点检查法的培训?

问题指南: 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.

- (●) 是
- ( ) 否
- ( ) 未进行 IIT 检查

注释: *未提供评论*

55 材料 是否设有管理人员或监督人员进行后续 IIT 检查的程序?

问题指南: 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)

- ( ) 是
- (●) 否
- ( ) 未进行 IIT 检查

注释: There was no procedure where management or supervision conducts follow up IIT inspections.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 这是最佳实践。制定并记录一项程序，以便管理层或主管人员对国际运输工具 (IIT) 进行审查和/或后续检查。

如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程，并上传照片以作为完成的证据。否则，请注明您已考虑未来实施此流程。

CAPA 指南: The documented procedure must, at a minimum, include:

- Routine management or supervisor reviews of Instruments of International Traffic (IIT) inspection records and

documentation

- Periodic follow-up inspections of selected IITs to verify the accuracy and quality of initial inspections
- Documentation of review activities, including reviewer name, date, findings, and any corrective actions taken
- Criteria or triggers for follow-up inspections, such as findings from audits, nonconformities, or newly trained staff
- Defined process for addressing deficiencies, including retraining or disciplinary action if inspections are not conducted properly

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.

- ○ 已经实施
- ◉ 已知悉 - 将考虑在未来实施

注释: 我们任命了安全主任将会对后续IIT进行检查并保留记录，要求不定期对IIT进行抽查，发现不合格项后对涉及相关人员进行培训

验收意见: 公认

56 材料 所有 IIT 检查和 IIT 装载是否都受到监督?

问题指南: 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)

- ◉ 是 - 全都受到监督
- ○ 是 - 随机的部分 IIT 检查和 IIT 装载受到监督
- ○ 否

注释: *未提供评论*

57 没有 工厂是否直接为其任何客户或业务合作伙伴与运输服务提供商签约?

问题指南: 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.

- ◉ 是
- ○ 否

注释: *未提供评论*

58 材料 工厂是否有记录在案的程序来要求确认所装运货物到达目的地（IIT 堆场或货运代理位置）？

问题指南: 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)

- (●) 是
- ( ) 否

注释: *未提供评论*

59 材料 工厂要求签约运输公司使用哪些跟踪技术来监督行动轨迹以及确认货物到达?

问题指南: 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)

- ( ) 承运人控制的 GPS
- ( ) 托运人控制的 GPS
- ( ) 承运人调度人员致电核实
- ( ) 司机致电确认
- (●) 以上两个或多个选项 - 请说明
- ( ) Other - please describe
- ( ) 未使用跟踪技术

注释: GPS carrier controlled and cell phone confirmation by driver were used.

60 材料 在可能的情况下，从工厂到港口或下一个目的地的运输路线是否随机改变，以尽量减少可预测性?

问题指南: 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.

- (●) 是
- ( ) 否
- ( ) 仅提供一条路线

注释: *未提供评论*

61 材料 工厂是否向运输服务司机提供记录在案的指示，详细说明了仅允许必要的停靠？（即仅在政府机构检查点或重新加油等情况下停靠。）

仅在该工厂只通过集货商或承运人装运小包裹时，选择"不适用"。

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) N/A

注释: *未提供评论*

62 危急 工厂是否针对物料的到达和离开移动而记录了司机信息？（选择所有适用项）

问题指南: 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] 司机日志已妥善保存(请附上正在使用的日志照片)
- [x] 牵引车编号/IIT编号
- [x] 要求提供司机的带照片身份证件
- [x] 承运人名称
- [x] 日期
- [x] 抵达时间
- [x] 起运时间
- [x] IIT 起运时的封条验证信息
- [ ] 没有司机日志可供查看

#62 container log.jpg

注释: *未提供评论*

63 材料 工厂是否要求承运人提前通知计划提货的预计到达时间，包括司机姓名和卡车车牌号?

问题指南: 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)

- (●) 是
- ( ) 否

注释: *未提供评论*

64 没有 工厂是否发运拼箱货物 (LCL)?

- (●) 是
- ( ) 否

注释: *未提供评论*

65 危急 是否制定了记录在案的 LCL 安全程序，该程序要求在每次停靠后使用防篡改封条、挂锁或高安全性封条对 LCL IIT 进行封装?

问题指南: A documented policy must describe how the facility secures shipments leaving the facility including temporary seals on less than container (LCL) shipments. Seals applied to the Instruments of International Traffic (IIT) must be a tamper evident seal, a padlock or a high security seal. Example: A simple one time use seal (with a unique seal #) is acceptable.

- (●) 是 (请上传程序文件中对应章节的照片)
- ( ) 否



#65 LCL securit... jpg

注释: *未提供评论*

66 没有 工厂是否进行空运?

- ( ) 是
- (●) 否

注释: *未提供评论*

68 没有 工厂是否用顶开、侧开、通风（牲畜）、软面集装箱发运货物?

- ( ) 是
- (●) 否

注释: *未提供评论*

70 危急 在装载 IIT 之后，是否立即采用符合 ISO 17712:2013 标准的高安全性封条来封装国际货物?

仅在该工厂只通过集货商或承运人装运小包裹时，选择"不适用"。

问题指南: 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)

- (●) 是(请上传使用中的符合ISO相关标准的封条照片)
- ( ) 否
- ( ) N/A

#70 security sea... jpg

注释： *未提供评论*

71 危急 工厂是否有记录在案的和可验证的程序来确保安全封条在控制之中？ （选择所有适用项）

仅在封条由第三方（如集货商或承运人）提供时，选择"不适用"。

问题指南： 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] 政策已记录在案（请附上适用程序部分的照片）
- [x] 封条妥善存放
- [x] 列出了有权取用存放的封条的特定员工
- [ ] 记录在案的政策不可用
- [ ] N/A

#71seal control ... jpg

注释： *未提供评论*

72 必须 工厂是否有记录在案的流程，以便在发生安全威胁或运输违规时，及时通知供应链中的任何业务合作伙伴和相关执法机构?

问题指南： 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)

- (●) 是
- ( ) 否

注释： *未提供评论*

73 材料 在跨境运输或货物转运之前，是否存在记录在案的程序，以检查 IIT 交通运输工具是否有篡改迹象（包括实地检查和 VVTT）？

仅在该工厂只通过集货商或承运人装运小包裹时，选择"不适用"。

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) N/A

注释: *未提供评论*

农业安全 100%

74 必须 该工厂是否制定了预防可见虫害污染的记录在案的程序，包括遵守木质包装材料 (WPM) 法规?

仅当该工厂在其生产或运输过程中不使用任何木材或木质包装材料时，选择"不适用"。

问题指南: 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)

- ( ) 是
- ( ) 否

- (●) N/A

注释: No wood or wood products utilized in the manufacturing or shipping process.

75 必须 该工厂是否制定了记录在案的流程，用于在装载前清除 IIT 外部和内部的虫害污染及其他杂物？ 记录在案的流程必须规定为期一年的保留政策。

仅在该工厂只通过集货商或承运人装运小包裹时，选择"不适用"。

问题指南: 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)

- (●) 是 - 请附上流程中该部分的照片 #76 prevent visi...jpg
- ( ) 无记录在案的流程和/或保留政策不完善
- ( ) N/A

注释: *未提供评论*

76 材料 工厂是否在装载前清除 IIT 外部和内部的虫害污染及其他杂物?

仅在该工厂只通过集货商或承运人装运小包裹时，选择"不适用"。

问题指南: 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.

- (●) 是 - 请说明如何进行验证
- ( ) 否
- ( ) 脏污 IIT 被拒收
- ( ) N/A

注释: Before loading, the facility arranged designated person to conduct pest contamination and other debris inspection, if pest contamination and other debris ideintified from IIT exterior and interior prior to loading, the

facility would remove it immediately.

77 材料 工厂是否有记录在案的程序，用于检查和审查虫害入侵证据（如诱饵诱捕器）、定期灭杀以及从运输和存储工厂中清除杂物?

问题指南: 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)

- (●) 是 - 并已实施（请告知如何进行验证）
- ( ) 是
- ( ) 否

注释: The facility had 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. For example, the facility set baited traps at finished goods warehouses, conducted pest contamination on each container before loading.

78 必须 对于国际货物而言，木质包装材料是否经过热处理或熏蒸，以杀死虫害并降低在 IIT 装箱处引入虫害的可能性？ （选择所有适用项）

仅在该工厂没有将木质包装材料用于国际货物时，选择"不适用"。

问题指南: 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)

- [ ] 工厂仅使用经过热处理或其他处理的包装材料
- [ ] 生产流程中使用的所有木材的来源都记录在案，并提供给收货人
- [ ] 工厂无法详细说明在使用前对木材包装材料所做的处理
- [x] N/A

注释: No wood packaging material used for international shipments.

79 必须 对于国际货物而言，装运过程中使用的木质托盘是否经过热处理或熏蒸，以杀死虫害并降低在装运工厂引入虫害的可能性？ 托盘是否存放在工厂内，以限制其接触种子、污垢和其他污染物？ （选择所有适用项）

仅当该工厂没有将木质托盘用于国际货物时，选择"不适用"。

问题指南: 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)

- [ ] 托盘经过热处理或熏蒸
- [ ] 托盘上加盖有热处理印章，或为交付的每个托盘颁发植物检疫检验证书
- [ ] 托盘存储在建筑物内
- [ ] 记录在案的流程可用
- [ ] pallets are observed stored outside and on the ground
- [ ] 托盘未经热处理或熏蒸
- [x] N/A

注释: No wood pallets used for international shipments.

封条安全 98%

80 必须 工厂是否有详细记录在案的高安全性封条程序，其中规定了封条在工厂和运输过程中的发放和控制程序？ （选择所有适用项）

仅在该工厂只使用由第三方提供商提供的封条，通过集货商或承运人装运小包裹时，选择"不适用"。

问题指南: 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] 控制对封条的访问
- [x] 库存、分发和跟踪（封条日志）
- [x] 控制运输中的封条
- [x] 运输途中封条破损
- [x] 封条差异
- [ ] 每年审查一次程序
- [ ] 文档不可用
- [ ] 发现实施中的漏洞（请提供备注）
- [ ] N/A

注释: Procedures were not reviewed annually.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项高安全性封条程序，概述如何在工厂内和运输过程中发放、加装和管控封条。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。

- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: The documented procedure must, at a minimum, include:

- Responsibilities: Clearly define the roles and responsibilities of personnel involved in managing, issuing, applying, and verifying seals.

- Seal Inventory Control: Procedures for securing, tracking, and recording all seals in inventory, including issuance logs.

- Application Protocol: Steps for applying seals to Instruments of International Traffic (IIT), including when and where seals must be affixed and by whom.

- Verification: Requirement to record and verify seal numbers on shipping documentation (e.g., Bills of Lading).

- Monitoring During Transit: Instructions for drivers/carriers on maintaining seal integrity, including actions required if a seal is broken or compromised.

- Documentation and Retention: Maintaining records of seal usage, verification, and reporting discrepancies, with specified retention periods.

- Security Measures: Procedures to prevent unauthorized access to seal storage and ensure seal authenticity (e.g., using ISO 17712:2013-compliant bolt seals).

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.

- (●) 已经实施
- ( ) 将要实施
- ( ) 不会实施/不会履行纠正措施请求

封条管理程序.pdf

注释: 我们由安全主任牵头IT部门，对该程序从流程到复核阶段进行了讨论看程序内容是否与实际行动是否相符合，查找漏洞优化流程。我们在2026-04-27日完成了最近的年度审查

验收意见: 公认

- (●) 已经实施
- ( ) 将要实施
- ( ) 不会实施/不会履行纠正措施请求

封条管理程序.pdf

注释: 我们已经在2026-04-01制定了相关程序。

重新打开评论: 已记录的详细高安全密封程序应每年进行审查，请在评论框中详细描述您的实施情况，并提供最近一次年度审查日期。

81 危急 安全封条是否存储在安全位置?

仅在该工厂只使用由第三方提供商提供的封条，通过集货商或承运人装运小包裹时，选择"不适用"。

问题指南: 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)

- (●) 是 (请上传封条存放位置的照片)
- ( ) 否
- ( ) N/A

#81 seal storage... jpg

注释: *未提供评论*

82 危急 工厂是否有记录在案的测试报告或封条供应商提供的声明，以验证所使用的封条是否符合（或超过）最新的 ISO 17712 标准?

仅在该工厂只使用由第三方提供商提供的封条，通过集货商或承运人装运小包裹时，选择"不适用"。

问题指南: 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)

- (●) 是 (请上传封条测试报告的照片)
- ( ) 否
- ( ) N/A

#82 seal test rep...jpg

注释: *未提供评论*

83 必须 是否制定了记录在案的程序，要求管理层人员对封条库存、封条日志、装运单据和交通运输工具进行定期审计，以验证是否遵循了封条控制措施。所有步骤必须记录在案。（选择所有适用项）

仅在该工厂只使用由第三方提供商提供的封条，通过集货商或承运人装运小包裹时，选择"不适用"。
问题指南: 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)

- [x] 记录在案的程序可用
- [ ] 执行并记录审计
- [x] 无记录在案的政策或实操
- [ ] N/A

注释: The facility had a procedure to conduct periodic audits of the seal document records, but no audit was conducted.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25** 包括在得分中

CAPA: 制定并记录一项程序，要求管理层人员对封条库存、封条日志、装运单据和交通运输工具进行定期审计，以确保封条控制程序得到妥善实施和遵循。
- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。
- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: The documented procedure must include, at a minimum:
- Audit Frequency & Responsibility
- Audits must include a thorough review of the following: Seal inventory – Verify count, condition, and compliance

with ISO 17712; Seal log – Ensure all entries are accurate and complete (seal numbers, issue/return dates, personnel involved); Shipping documents – Confirm seal numbers recorded match those applied to conveyances; Conveyances – Spot check trucks/trailers to verify seals in use are compliant and match documentation.

- Each audit must be recorded and retained, including: Date of audit; Name and title of the auditor; Findings or observations; Any identified nonconformities or issues; Corrective actions taken and follow-up verification (if applicable)
- Outline a process for addressing any discrepancies found during the audit.
- Audit logs and associated documentation must be retained in accordance with internal retention policies and be available for internal and external review.

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.

- (●) 已经实施
- ( ) 将要实施
- ( ) 不会实施/不会履行纠正措施请求

封条管理程序.pdf

注释: 封条库存：核对数量、状况及是否符合 ISO 17712经检查符合要求；封条日志 ： 确保所有条目准确完整（封条编号、发放/退回日期、相关人员）经检查符合要求；装运单据：确认记录的封条编号与交通运输工具上实际使用的封条编号一致；交通运输工具 - 抽查卡车/拖车，以验证使用的封条是否合规且与文档记录相符。经检查符合要求

审核日期：2026-04-28，审核人：黄万山-安全主任

未发现不符合项

验收意见: 公认

- (●) 已经实施
- ( ) 将要实施
- ( ) 不会实施/不会履行纠正措施请求

封条管理程序.pdf

注释: 我们已经在2026-04-01制定了相关程序。

重新打开评论: 相关程序已经制定，但尚未进行审计。 请参考 CAPA 指南，在评论框中描述您最新的封条库存、封条日志、运输单据和运输工具的审核记录，以便审核。

84 危急 描述工厂的封条施用流程。（选择所有适用项）

仅在该工厂只使用由第三方提供商提供的封条，通过集货商或承运人装运小包裹时，选择“不适用”。

问题指南: 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] 封条施用程序中包含 VVTT 流程
- [x] 二次测试和验证由主管或保安在出厂时进行检查
- [x] 封条编号在装运单据上以电子方式记录
- [x] 在闭路电视录像上记录测试程序
- [x] 将封条编号告知或以其他方式发送给收货人
- [x] 在离开原产地港口之前，若更改封条编号，会告知工厂
- [x] 流程已记录在案
- [ ] 未制定封条施用流程
- [ ] N/A

注释: *未提供评论*

程序安全 98%

85 危急 毗邻发货区和收货区的区域是否封闭或受到监控?

问题指南: 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.

- (●) 是 (请上传该区域被包围,并且/或者有其它监督设置的照片)
- ( ) 否



#85 shipping &... jpg

注释: *未提供评论*

86 危急 是否制定了记录在案的程序，用于报告工厂内对 IIT 和/或产品存放区的未经授权访问，以及要通知哪些人员?

问题指南: 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)

- (●) 是 (请上传程序文件中对应章节的照片)
- ( ) 否

#86 procedure i... jpg

注释: *未提供评论*

87 危急 是否制定了记录在案的程序，用于监控和限制访问工厂的关键运营区域（如仓库拣选、最终打包或包装、发货和收货）?

问题指南: 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.

- (●) 是 (请上传程序文件中对应章节的照片)
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞



#87 limit access... jpg

注释: *未提供评论*

88 危急 是否制定了记录在案的程序，要求商品/货物装运单据中使用的所有信息必须清晰、完整和准确?

问题指南: Facilities must have a documented process for ensuring shipping documents are legible, complete, and accurate.
(CTPAT MSC 7.6)

- (●) 是 (请上传程序文件中对应章节的照片)
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞

#88 shipping do... jpg

注释: *未提供评论*

89 危急 是否制定了记录在案的程序，用于在 IIT 装载过程中或货物离开工厂后，调查和解决箱数不足、超载或任何单据问题?

问题指南: 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)

- (●) 是 (请上传程序文件中对应章节的照片)
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞

#89 shortage, o... jpg

注释: *未提供评论*

90 危急 是否制定了记录在案的程序，确保标记、清点、称重并在装运单据上准确申报国际货物?

如果此工厂不涉及国际货物业务，则选择"不适用"。

问题指南: 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.

- (●) 是 (请上传程序文件中对应章节的照片)
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞
- ( ) N/A

#90 internation... jpg

注释: *未提供评论*

91 危急 是否制定了限制访问发货和收货单据的记录在案的程序?

问题指南: 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.

- (●) 是 (请上传程序文件中对应章节的照片)
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞



#91 written pro... jpg

注释: *未提供评论*

92 材料 是否使用预先打印的纸质文件/表格来准备商业文件并妥善保管?

问题指南: Best practice dictates if paper documents are used, facility must describe steps taken to secure them in a documented procedure.
(CTPAT MSC 7.7)

- (●) 预先打印的文档/表格受到保护
- ( ) 预先打印的文档/表格未受到保护
- ( ) 预先打印的文档/表格不予使用

注释: *未提供评论*

93 材料 在准备出口单据时，共享网络打印机的密码是否受保护?

仅在未使用共享网络打印机时选择 NA。

问题指南: This is a best practice and is encouraged that the access to shared network printers should be controlled via individually assigned passwords.

- ( ) 是
- ( ) 否
- (●) N/A

注释: There were no shared network printers being utilized.

94 危急 是否制定了记录在案的程序，要求商业单据包在发货时一并寄送? 请说明具体流程。

问题指南: 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.

- (●) 是
- ( ) 否

- ○ 是 - 但发现实施中的漏洞

注释: Document packets were sent with shipment at departure once information was verified as correct.

95 危急 是否制定了记录在案的程序，用于在涉嫌或发现非法运输活动或任何异常情况时，通知当地执法部门和客户?

问题指南: 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)

- ◉ 是 (请上传程序文件中对应章节的照片)
- ○ 否



#95 notify whe... jpg

注释: *未提供评论*

96 危急 是否采用了记录在案的门禁控制程序和设备，以确保只有获授权的员工才能进入工厂?

问题指南: 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.

- ◉ 是（请附上适用文档部分和设备的照片）
- ○ 否
- ○ 是 - 但发现实施中的漏洞

#96 authorized ... jpg

注释: *未提供评论*

97 危急 是否制定了记录在案的程序，用于将安全问题（如盗窃未遂、欺诈或内部阴谋）告知业务合作伙伴?

问题指南: 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.

- (●) 是 (请上传程序文件中对应章节的照片)
- ( ) 否



#97 procedure t... jpg

注释: *未提供评论*

98 材料 是否制定了记录在案的程序，用于要求发运部门在起运前核对装载货物与采购订单是否相符?

问题指南: 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.

- (●) 是
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞

注释: *未提供评论*

99 危急 是否制定了记录在案的程序，用于控制门禁装置（如身份识别卡、门锁钥匙、门禁卡和安全警报码）的发放、撤销和更换?

问题指南: 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.

- (●) 是 (请上传程序文件中对应章节的照片)
- ( ) 否

#99 written pro... jpg

注释: *未提供评论*

100 没有 现场是否有专门的安保人员/保安?

- (●) 是
- ( ) 否

注释: *未提供评论*

101 必须 是否制定了记录在案的岗位说明，用于概述安保人员或身兼两职（包括安保职能）人员的角色和职责?

问题指南: 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.

- (●) 是
- ( ) 否

注释: *未提供评论*

102 必须 该工厂是否要求安保人员或承包商在非工作时段在工厂中"巡逻"，并且是否用闭路电视监控、电子记录或纸质检查清单对"巡逻"进行记录?

问题指南: 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.

- ( ) 要求巡逻；并以电子方式或通过闭路电视记录
- (●) 要求巡逻；仅以纸质方式记录
- ( ) 要求巡逻；未进行文档记录
- ( ) 不要求巡逻，也未予以记录

注释: *未提供评论*

103 必须 管理层是否根据安保人员/保安的工作指示和政策进行验证?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞

注释: *未提供评论*

104 必须 是否制定了记录在案的程序，用于确保提单 (BOL)、货运代理收据 (FCR) 和舱单准确反映了提供给承运人的信息?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞

注释: *未提供评论*

105 必须 是否制定了记录在案的程序，用于在发现安全相关事件（例如，恐怖主义、毒品、偷渡、盗窃）时立即启动内部调查并予以记录?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞

注释: *未提供评论*

物理安全 88%

106 危急 是否有一个与发货和收货区分开的员工和访客车辆指定停放区?

问题指南: 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)

- (●) 是（请附上适用区域的照片）
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞



#106 shipping a... jpg

注释: *未提供评论*

107 材料 是否有适当的控制措施将国内货物与将要发往国外的国际货物分开?

问题指南: 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)

- (●) 是
- ( ) 否

注释: *未提供评论*

108 材料 是否制定有要求定期检查工厂围墙沿线,或其他围栏、建筑物和结构的预防性维护程序? （选择所有适用项）

问题指南: 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] 政策已记录在案
- [x] 定期检查已记录在案
- [x] 预防维护日志已留存
- [ ] 未设任何程序

注释: *未提供评论*

109 危急 是否有任何屏障限制车辆和人员进出工厂？ 请附上适用区域的照片。

问题指南: 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)

- (●) 物理屏障
- ( ) 环境屏障
- ( ) 物理和环境屏障结合
- ( ) 无屏障

#109 physical b... jpg

注释: There were barriers installed to limit the ingress and egress to the facility by vehicles and personnel.

110 危急 大门在未使用时是否处于上锁和监控状态?

仅在工厂没有大门时，选择"不适用"。

问题指南: Gates must be locked when not in use. CCTV should also monitor gates at all times.
(CTPAT MSC 9.4)

- (●) 是 - 大门在未使用时处于上锁/锁闭状态，并由闭路电视监控（请附上适用区域的照片）
- ( ) 是 - 大门在未使用时处于上锁/锁闭状态（请附上适用区域的照片）
- ( ) 否
- ( ) N/A

#110 factory gate.jpg

注释: *未提供评论*

111 必须 工厂入口、出口、货物装卸和存储区域、围栏沿线和停车区是否有足够的照明来检测黑暗环境下的物体移动?

问题指南: 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)

- (●) 是
- ( ) 否

注释: *未提供评论*

112 必须 工厂将下列哪些安全技术作为其系统和控制措施的一部分？（选择所有适用项）

问题指南: 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] 闭路电视
- [x] access control
- [ ] security alarm
- [ ] 使用其它技术手段
- [ ] 未使用安全技术

注释: No security alarm or other technologies used in the factory.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项程序，要求在工厂安装和使用安全技术。
- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。
- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: 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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将会配齐下列所有的控制措施：门禁、安全警报、CCTV、安保、可上锁的大门。

预计在2026-06-30内完成

验收意见: 公认

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将会配齐下列所有的控制措施：门禁、安全警报、CCTV、安保、可上锁的大门。

重新打开评论: 请在评论框中为您提交的纠正措施计划添加预计在不久的将来完成的日期。

113 必须 您是否有管理安全技术使用的记录在案的程序?

问题指南: 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)

- ◉ 是
- ○ 无记录在案的程序
- ○ 未使用安全技术

注释: *未提供评论*

114 材料 安保设备是否由获许可/认证的承包商安装?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 未使用安全技术

注释: *未提供评论*

115 材料 您的安保系统有维保合同吗?

问题指南: 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.

- (●) 是，有有效合约
- ( ) 没有有效合约
- ( ) 未使用安全技术

注释: *未提供评论*

116 必须 关键的安保基础设施所处区域是否受保护,且工厂仅授权因工作之需而进出的人员予以访问?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 未使用安全技术

注释: *未提供评论*

117 材料 停电时，该工厂是否有备用电力系统，以确保电子安全系统的不间断运行?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 未使用安全技术

注释: *未提供评论*

118 危急 是否有用于监控工厂和场所，包括入口、出口、货物存储、运输、包装和其他装卸区域的闭路电视系统？（选择所有适用项）

问题指南: 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)



#118 CCTV cont... jpg

- [x] 所有入口/出口
- [x] 货物存储/运输区域
- [x] 装卸货区域
- [x] 包装区域
- [x] 外围围墙
- [x] 如果检测到未经授权的访问，闭路电视监控将触发警报
- [ ] 没有闭路电视

注释: *未提供评论*

119 材料 您的闭路电视系统是否有指示何时系统离线或未作录制的故障警报?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 没有闭路电视

注释: *未提供评论*

120 危急 闭路电视系统是否全天候24小时连续每周七天不间断运行?

问题指南: 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)

- (●) 是（请附上适用区域的照片）
- ( ) 否
- ( ) 没有闭路电视



#120 CCTV reco... jpg

注释： *未提供评论*

121 必须 工厂闭路电视系统是否采用最高质量的图片设置进行录制?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 没有闭路电视

注释： *未提供评论*

122 必须 工厂管理团队是否定期对闭路电视录像进行随机的有记录审查，以确保安全程序得到遵守?

问题指南: 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, time, 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)

- ( ) 是
- (●) 否
- ( ) 没有闭路电视

注释: The facility's management team did not conduct random and documented reviews of CCTV footage periodically to ensure security procedures are being followed.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项物理安全程序，要求管理层对闭路电视录像进行随机且记录在案的审查，以确保遵守安全规程并识别任何违规行为。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。

- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: This is over and above the reviews that should be performed by the security team. The documented procedure must include, at a minimum:

- Regular, random reviews of footage in critical facility areas
- A log documenting date of review, reviewer, footage reviewed, and findings
- Retention of review records for at least 12 months
- A follow-up process for any irregularities found

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定相关程序，指派专人对监控进行审查，每周不定时查看监控影像是否正常、要求记录情况并至少保留记录一年，若发现不合规现象立即上报安全主任。预计2026-06-30内完成

验收意见: 公认

123 危急 闭路电视的记录会留存多少天?

问题指南: 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)



#123 insufficien... jpg

- ○ 90 天或更久
- ◉ 45 - 89 天
- ○ 小于 45 天
- ○ 未保留记录
- ○ 没有闭路电视

注释: CCTV recordings were only maintained for 50 days for review.

124 必须 员工在工厂期间是否随时展示身份识别卡?

问题指南: 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.

- ○ 是
- ◉ 携带身份证件但未出示
- ○ 否

注释: *未提供评论*

125 危急 是否制定了记录在案的程序，要求访客在到达时出示带照片的身份证件，并让保安或其他授权员工将其信息记录在日志中? （选择所有适用项）

问题指南: 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)

- ☑ 记录在案的程序可用
- ☐ 查看带有照片的身份证明
- ☑ 使用访客登记簿
- ☐ 未制定记录在案的流程



#125 visitor log.jpg

注释: Not all visitors were not required to present photo identification upon arrival, such as no such requirement for auditor on the audit day.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25** 包括在得分中

CAPA: 制定并记录一项程序，要求所有访客在进入工厂时出示身份证明并登记。

在文本框中说明您何时以及如何完成纠正措施或实施流程。请上传访客登记簿的电子图片以供审查。

CAPA 指南: The documented procedure must include, at a minimum:

- An authorized employee or security personnel must require visitors to present photo identification upon arrival
- Verification of the visitor's identity and record their details must be entered into the visitor log
- The visitor log must include at a minimum: arrival time, date, visitor name, reason for visit, visitor badge number, departure time.

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.

- (●) 已经实施
- ( ) 不会实施/不会履行纠正措施请求

访客登记.pdf

注释: 我们将实地为安保人员实时演示一次流程，访客到达、礼貌询问、要求访客出示带身份证明的证件、填写访客登记表、复核身份信息、在备注栏填写访客是否出示带照片的身份证明。我们会随机询问访客在进入前是否向安保人员出示了带照片的身份证明，访客离开后对该访客的出入记录进行核查。在2026-4-28完成。

验收意见: 公认

- (●) 已经实施
- ( ) 不会实施/不会履行纠正措施请求

访客登记.pdf

注释: 我们制定了相关程序，要求安保人员对外来访客进入登记时必须完整填写抵达时间、日期、访客姓名、来访原因、访客识别卡编号、离开时间。并且要求访客出示相关身份证明以供核实

重新打开评论: 该程序已经到位，但并非所有访客在抵达时都不需要出示带照片的身份证明。 请在评论框中详细描述您如何解决该问题，如何监控该过程以确保其能够正确实施，并提供实施日期。

126 必须 是否制定了记录在案的程序，用于在访客进入和离开工厂的制造、生产或发货区之前，检查其包袋?

问题指南: Upon arrival and exit of facility all visitor bags should be checked by guards, management, or other authorized personnel.

- ( ) 是
- ( ) 否
- (●) 是 - 但发现实施中的漏洞

注释: Though the facility had a procedure in place to inspect visitors' bag before entering and leaving the compound of the facility, no such inspection conducted.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项物理安全程序，要求对进出贵工厂的所有访客的随身行李及包裹进行检查。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。

- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: The documented procedure must include, at a minimum:

- Specify inspection methods, responsible staff, and how to handle refusals
- Maintaining logs of inspections with visitor details and outcomes
- Define prohibited items and escalation steps
- Ensure regular staff training and periodic audits to maintain compliance

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定相关程序，访客抵达时，安保人员需立即告知公司包袋检查政策，在访客完成登记后，进入受限制区域之前，在访客结束访问，离开受限制区域之时都需要检查。检查方法：要求访客自行打开所有携带的包袋，进行目视检查。检查应迅速、专业且尊重访客隐私，原则上不直接用手触碰访客私人物品。易燃易爆物，毒品或公司明确规定的其他违禁物品不允许携带。发现违禁品时的处理流程：建议访客将物品寄存于保安室，离厂时取回。任何拒收或冲突情况，安保人员须立即通过对讲机或电话向安全主任报告。将事件详情（时间、访客姓名、公司、物品描述、处理结果）完整记录于《访客检查异常事件记录表》所有检查日志及相关异常事件记录需至少保存 24个月，以备审计和核查。每年对相关人员至少进行一次培训。预计2026-06-30内完成

验收意见: 公认

---

127 危急 是否制定了记录在案的程序，要求向访客发放带有编号的访客识别卡，并让其在工厂逗留期间全程佩戴出示?

问题指南: 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)

- ◉ 是（请附上适用项目的照片）
- ○ 否
- ○ 是 - 但发现实施中的漏洞



#127 visitor bad...jpg

注释: *未提供评论*

---

128 危急 是否有记录在案的政策，要求访客在工厂逗留期间始终有人陪同?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞

注释: *未提供评论*

129 材料 是否制定了记录在案的程序，用于在分发前检查所收到的邮件和包裹?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞

注释: *未提供评论*

130 材料 危险品或价值昂贵的物品存储在工厂时是否会隔离存储?

仅在工厂没有价值昂贵的物品和危险材料物品时选择 NA。

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) N/A

注释: *未提供评论*

人员安全 75%

131 必须 工厂是否制定了记录在案的程序，用于核实求职申请中提供的信息，如地址、以往工作经历、教育程度、个人和职业推荐人以及任何适用的证书（根据当地法律适用）？

问题指南: 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)

- ( ) 政策已记录在案
- (●) 是 - 但发现实施中的漏洞
- ( ) 未设任何程序

注释: The facility had 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, but no verification conducted for previous employment history, education.

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项人员安全程序，其中应包含验证和记录求职申请中所填信息的具体方法，以确保在录用前求职者信息的准确性和完整性。

- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。

- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: The documented procedure must include, at a minimum:

- Verification of identity and address using government-issued photo identification

- Employment history validation, including dates of prior employment, job titles, and reasons for leaving
- Education and certification checks, where applicable to the position
- Reference checks with previous employers or listed references

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定有关验证和记录求职申请中提供的详细信息的方法的书面程序。其主要包含：在求职者填写入职登记表时，要求完整填写个人信息、住址、工作经历、教育信息等。
并在各方面符合公司要求时提前一天进行信息核实，核查信息应按照但不限于下列方法执行：学信网查询其教育经历是否真实；电话与其亲属/前公司领导、同事核实基本信息；前往公安机关请求查询其是否存在作奸犯科、信用不良等信息。预计在2026-06-30内完成。
验收意见: 公认

132 必须 该工厂是否制定了记录在案的政策，要求正式和临时工作的求职者提交书面就业申请并提供身份证明?

问题指南: 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)

- ◉ 是 - 需要提供和收集书面申请和政府签发的身份证件
- ○ 否 - 无需提供或收集书面申请和政府签发的身份证件（部分流程不可接受）

注释: *未提供评论*

133 必须 在当地法律允许的情形下，是否存在记录在案的程序，用于对在人事、运输或计算机系统等工厂敏感领域工作的求职者和员工进行背景调查？ 此要求也适用于合同工。

仅在当地法律禁止开展背景调查时，选择"不适用"。

问题指南: 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)

- (●) 是，已制定记录在案的程序
- ( ) 没有书面程序文件
- ( ) 是 - 但发现实施中的漏洞
- ( ) N/A

注释: *未提供评论*

134 没有 做了什么类型的调查？（请勾选所有适用选项）

- [x] 犯罪背景调查
- [ ] 信用调查
- [ ] 其他

注释: *未提供评论*

135 必须 工厂是否制定了《员工行为准则》，该准则要求员工和承包商签署确认书，并概述了预期要求、可接受的行为以及处罚或纪律处分程序?

问题指南: 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)

- (●) 是
- ( ) 否
- ( ) 是 - 但发现实施中的漏洞

注释: *未提供评论*

安全培训和威胁意识 98%

136 必须 是否为所有新员工提供安全威胁意识培训，并为在职员工提供年度巩固课程？ （选择所有适用项）

问题指南: 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] 制定有培训计划
- [x] 留存培训记录，以确保所需人员参加培训
- [ ] 管理人员随机审阅文档
- [x] 每年为所有员工提供培训
- [x] 为新员工提供培训
- [ ] 没有进行威胁意识培训

注释: *未提供评论*

CAPA 已分配 **2026/03/26** | 到期日 **2026/05/25**

CAPA: 制定并记录一项安全威胁意识培训计划，要求必须对新员工进行培训，并为在职员工提供年度培训。
- 如果已经实施，请在文本框中说明您何时以及如何完成纠正措施或实施流程。请附上带标题和文档说明的流程的照片。
- 如果将要实施，请在文本框中提供您的纠正措施计划以及完成和实施该流程的时间表（未来日期）。

CAPA 指南: The documented program must include, at a minimum:
- Mandatory security threat awareness training for all new employees prior to assignment in any facility role.
- Annual refresher training for all existing employees, regardless of tenure or role.
- Training topics to include: Types of security threats (e.g., theft, tampering, social engineering, cyber intrusion); Warning signs and indicators of suspicious behavior or activity; Reporting procedures and channels for security concerns; Roles and responsibilities during a security incident
- Attendance records with employee name, date, and training format

- Annual random review of employee documentation to ensure compliance
- Annual review of training content to incorporate new threats, lessons learned, and policy changes

You can review the section "Security Training and Threat Awareness" in the "SCAN Factory and Supplier Training" for some references and details when establishing this program.

The training link is: https://scrisksolutions.zendesk.com/hc/en-us/articles/34831843732115-SCAN-Factory-and-Supplier-Training-Registration-Guide

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.

- ○ 已经实施
- ◉ 将要实施
- ○ 不会实施/不会履行纠正措施请求

注释: 我们将制定培训计划，对所有新入职的员工工作前进行安全威胁意识培训，老员工每年进行一次巩固培训。培训内容包含安全威胁的类型、可疑行为或活动的警告信号和指标；安全问题的报告程序和渠道；安全事件期间的角色和责任等。定期根据新兴威胁、经验教训和政策变更等更新培训内容，培训记录每年度进行一次审查。预计2026-06-30完成

验收意见: 公认

137 必须 培训课程结束时是否包含对理解掌握情况进行的评估？（选择所有适用项）

问题指南: 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)

- ☑ 执行了评估
- ☑ 如果未达到合格分数，则需要再培训
- ☐ 未执行评估

注释: *未提供评论*

138 必须 工厂是否为执行安全和农业检查的员工提供培训？（选择所有适用项）

问题指南: 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] 培训材料列出了具体要求
- [x] 培训包括所有必要主题
- [x] 培训日志列出了在该区域中工作的员工
- [x] 每年为担任此工作职能的新员工提供培训
- [x] 每年为担任此工作职能的现有员工提供培训
- [ ] 对于该特定标准没有培训日志
- [ ] 对于该特定标准没有培训材料



#138 security a... jpg

注释: *未提供评论*

139 必须 培训是否包括工厂限制区域的安全标准，如最终包装、发货和收货？ (选择所有适用项)

问题指南: 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] 培训材料列出了具体要求
- [x] 培训日志列出了在该区域中工作的员工
- [x] 每年为担任此工作职能的现有员工提供培训
- [x] 每年为担任此工作职能的新员工提供培训
- [ ] 对于该特定标准没有培训日志

#139 security cr... jpg

- [ ] 对于该特定标准没有培训材料

注释: *未提供评论*

140 必须 威胁意识培训是否告知了员工举报可疑活动或安全事件的程序?

问题指南: 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)

- (●) 是
- ( ) 否

注释: *未提供评论*

141 必须 威胁意识培训是否为发货和收货员工提供了关于门禁控制、IIT 检查以及安全封装控制程序的额外指示? (选择所有适用项)

问题指南: 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] 培训包括发货和收货控制
- [x] 培训包括如何进行 IIT 检查
- [x] 培训包括 IIT 封条实践
- [x] 培训包括如何管控封条
- [ ] 未对发货和收货人进行特定的额外培训

注释: *未提供评论*

142 必须 培训计划是否包括威胁意识、违禁品、人口走私和恐怖主义?

问题指南: 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.

- [x] 是
- [ ] 否

注释: *未提供评论*

143 必须 当员工报告安全事件或提出改进建议时，工厂是否有认可员工的程序?

问题指南: 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.

- [x] 是
- [ ] 否

注释: *未提供评论*

144 必须 培训是否包括识别有害生物污染?

问题指南: 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.

- [x] 是
- [ ] 否

注释: *未提供评论*

145 必须 是否有一个概述网络安全风险的记录在案的培训?

问题指南: 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)

- [x] 是
- [ ] 否

注释: *未提供评论*

146 必须 是否有记录在案的培训材料，用于规定管理和操作安全技术系统的人员需接受与其特定领域相关的运营和维护培训?

问题指南: 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)

- (●) 是
- ( ) 否

注释: *未提供评论*

其他

N/A

147 没有 描述厂房正面，包括任何标示牌。请附上图片。

没有可用的选择

#147 factory na... jpg

注释: The factory name was displayed at the facility gate.

148 没有 描述门卫室和工厂入口。请附上图片。

没有可用的选择



#148 security g... jpg

注释: There was only one entrance gate, and access to the facility was controlled by security guards.

149 没有 描述该地点的建筑及结构。确认哪些建筑包含在审计范围内，以及哪些建筑没有包含在审计范围内。请附上该场地的概览图，并清楚标记所到访的建筑。

没有可用的选择



#149 factory lay... jpg

注释: All buildings within the facility were constructed with concrete structures. The buildings were well maintained and solid enough to prevent unlawful entry.

150 没有 描述发货和收货区。请附上图片。

没有可用的选择



#150 shipping a... jpg

注释: The shipping and receiving areas were located separately and access-controlled.

151 没有 描述如何保护工厂周边免受未经授权的访问？ 请附上图片

没有可用的选择

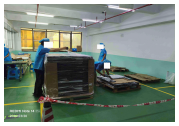


#151 factory fe... jpg

注释: Access to the facility was controlled through a guarded gate.

152 没有 描述最终包装区域。请附上图片。

没有可用的选择



#152 packing w... jpg

注释: The final packaging area was designated as a restricted area, with access limited to authorized personnel. An authorized personnel list was posted, and the area was monitored by CCTV.

153 没有 请描述任何国际运输工具 (IIT) 的储存和车辆停放区，并附上图片。

没有可用的选择



#153 private pa... jpg

注释: The container storage area and vehicle parking area were separated from other operational zones.

154 没有 工厂代表和审计师是否签署了首次会议书？ 请附上有签名的副本。

- (●) 是 - 请附上已签署的首次/结束会议书
- ( ) 否

#154 opening &... pdf

注释: *未提供评论*

附件文件 - 照片

General - 问题 # 1

#1 business license.jpg

General - 问题 # 5



#5 training certificate.jpg

Conveyances and Instruments of International Traffic - 问题 # 46

#46 container loading area.jpg

Conveyances and Instruments of International Traffic - 问题 # 47



#47 IIT inspection conducted.jpg

Conveyances and Instruments of International Traffic - 问题 # 48

#48 written procedure to inspect the security integrity of IIT.jpg

---

Conveyances and Instruments of International Traffic - 问题 # 49

#49 container inspection record.jpg

Conveyances and Instruments of International Traffic - 问题 # 51

#51 photos taken during the container loading process.jpg

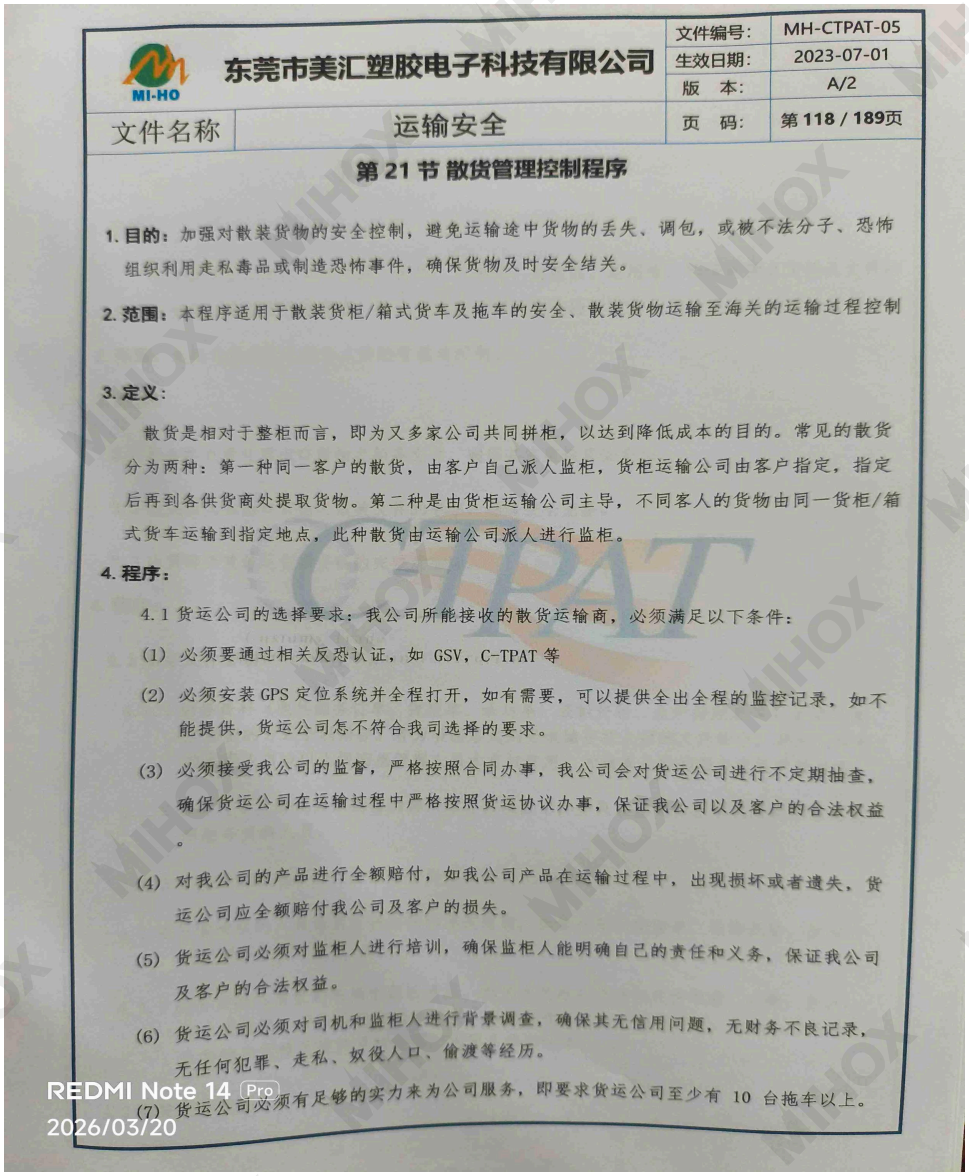
Conveyances and Instruments of International Traffic - 问题 # 52

#52 equipment used to conduct 7-point inspection.jpg

Conveyances and Instruments of International Traffic - 问题 # 62

#62 container log.jpg

Conveyances and Instruments of International Traffic - 问题 # 65



东莞市美汇塑胶电子科技有限公司

文件编号：	MH-CTPAT-05
生效日期：	2023-07-01
版　本：	A/2
页　码：	第 118 / 189页

文件名称：运输安全

第 21 节 散货管理控制程序

1. **目的**：加强对散装货物的安全控制，避免运输途中货物的丢失、调包，或被不法分子、恐怖组织利用走私毒品或制造恐怖事件，确保货物及时安全结关。

2. **范围**：本程序适用于散装货柜/箱式货车及拖车的安全、散装货物运输至海关的运输过程控制

3. **定义**：

散货是相对于整柜而言，即为又多家公司共同拼柜，以达到降低成本的目的。常见的散货分为两种：第一种同一客户的散货，由客户自己派人监柜，货柜运输公司由客户指定，指定后再到各供货商处提取货物。第二种是由货柜运输公司主导，不同客人的货物由同一货柜/箱式货车运输到指定地点，此种散货由运输公司派人进行监柜。

4. **程序**：

4.1 货运公司的选择要求：我公司所能接收的散货运输商，必须满足以下条件：

(1) 必须要通过相关反恐认证，如 GSV，C-TPAT 等

(2) 必须安装 GPS 定位系统并全程打开，如有需要，可以提供全出全程的监控记录，如不能提供，货运公司怎不符合我司选择的要求。

(3) 必须接受我公司的监督，严格按照合同办事，我公司会对货运公司进行不定期抽查，确保货运公司在运输过程中严格按照货运协议办事，保证我公司以及客户的合法权益。

(4) 对我公司的产品进行全额赔付，如我公司产品在运输过程中，出现损坏或者遗失，货运公司应全额赔付我公司及客户的损失。

(5) 货运公司必须对监柜人进行培训，确保监柜人能明确自己的责任和义务，保证我公司及客户的合法权益。

(6) 货运公司必须对司机和监柜人进行背景调查，确保其无信用问题，无财务不良记录，无任何犯罪、走私、奴役人口、偷渡等经历。

(7) 货运公司必须有足够的实力来为公司服务，即要求货运公司至少有 10 台拖车以上。

REDMI Note 14 Pro
2026/03/20

#65 LCL security procedure.jpg

Conveyances and Instruments of International Traffic - 问题 # 70

#70 security seal used.jpg

Conveyances and Instruments of International Traffic - 问题 # 71

#71seal control procedure.jpg

Agricultural Security - 问题 # 75

#76 prevent visible pest contamination.jpg

Seal Security - 问题 # 81

#81 seal storage area.jpg

Seal Security - 问题 # 82

#82 seal test report.jpg

Procedural Security - 问题 # 85

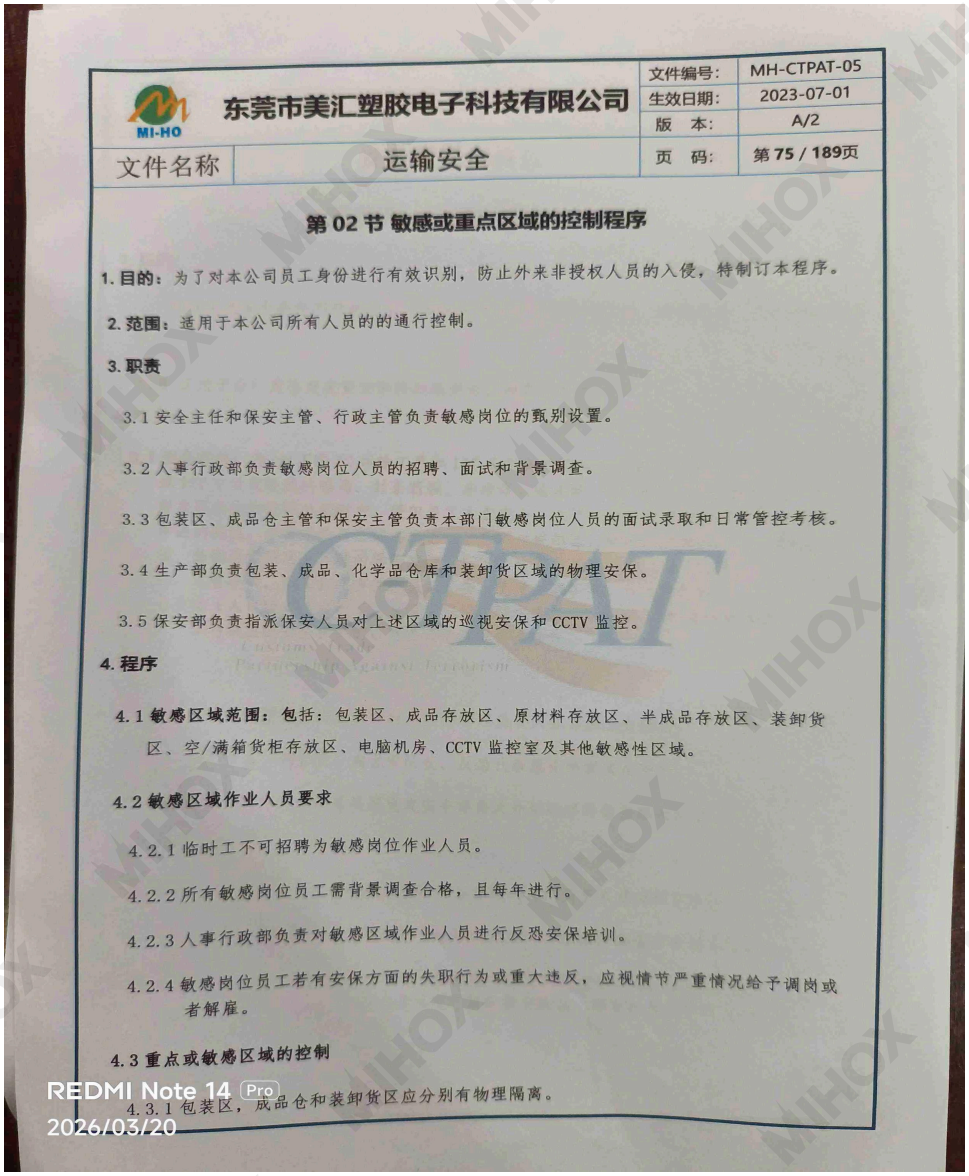


#85 shipping & receiving areas monitored by CCTV.jpg

Procedural Security - 问题 # 86

#86 procedure in place to report unauthorized access to sensitive areas.jpg

Procedural Security - 问题 # 87



东莞市美汇塑胶电子科技有限公司

文件编号:	MH-CTPAT-05
生效日期:	2023-07-01
版 本:	A/2
文件名称	运输安全
页 码:	第 75 / 189页

第 02 节 敏感或重点区域的控制程序

1. **目的：** 为了对本公司员工身份进行有效识别，防止外来非授权人员的入侵，特制订本程序。

2. **范围：** 适用于本公司所有人员的的通行控制。

3. **职责**

3.1 安全主任和保安主管、行政主管负责敏感岗位的甄别设置。

3.2 人事行政部负责敏感岗位人员的招聘、面试和背景调查。

3.3 包装区、成品仓主管和保安主管负责本部门敏感岗位人员的面试录取和日常管控考核。

3.4 生产部负责包装、成品、化学品仓库和装卸货区域的物理安保。

3.5 保安部负责指派保安人员对上述区域的巡视安保和 CCTV 监控。

4. **程序**

4.1 **敏感区域范围：** 包括：包装区、成品存放区、原材料存放区、半成品存放区、装卸货区、空/满箱货柜存放区、电脑机房、CCTV 监控室及其他敏感性区域。

4.2 **敏感区域作业人员要求**

4.2.1 临时工不可招聘为敏感岗位作业人员。

4.2.2 所有敏感岗位员工需背景调查合格，且每年进行。

4.2.3 人事行政部负责对敏感区域作业人员进行反恐安保培训。

4.2.4 敏感岗位员工若有安保方面的失职行为或重大违反，应视情节严重情况给予调岗或者解雇。

4.3 **重点或敏感区域的控制**

4.3.1 包装区，成品仓和装卸货区应分别有物理隔离。

REDMI Note 14 Pro
2026/03/20

#87 limit access control procedure.jpg

Procedural Security - 问题 # 88

#88 shipping document control procedure.jpg

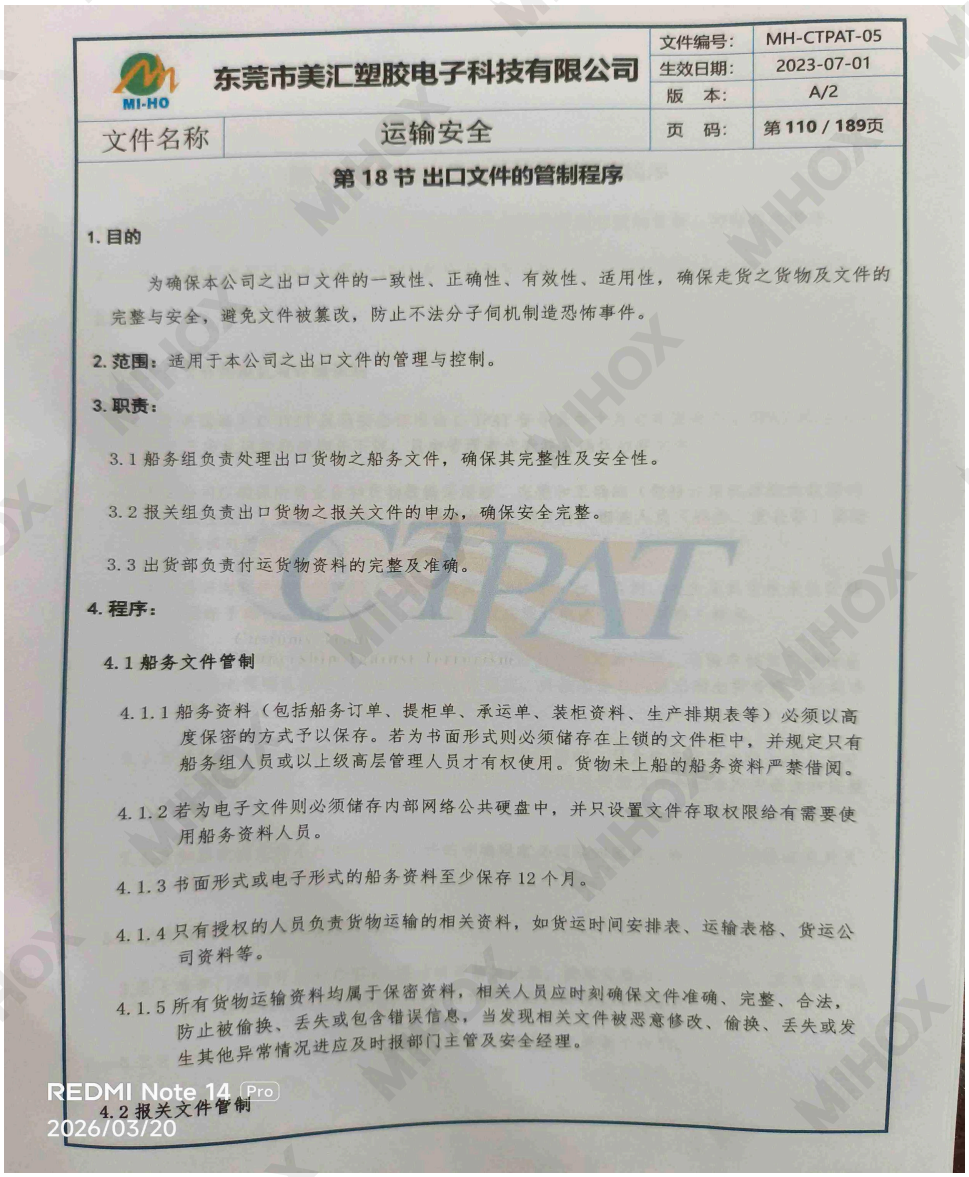
Procedural Security - 问题 # 89

#89 shortage, overage control procedure.jpg

Procedural Security - 问题 # 90

#90 international shipments marked, counted, weighed procedure.jpg

Procedural Security - 问题 # 91



MI-HO 东莞市美汇塑胶电子科技有限公司

文件编号:	MH-CTPAT-05
生效日期:	2023-07-01
版　本:	A/2
页　码:	第 110 / 189页

文件名称 运输安全

第 18 节 出口文件的管制程序

1. 目的

为确保本公司之出口文件的一致性、正确性、有效性、适用性，确保走货之货物及文件的完整与安全，避免文件被篡改，防止不法分子伺机制造恐怖事件。

2. 范围：适用于本公司之出口文件的管理与控制。

3. 职责：

3.1 船务组负责处理出口货物之船务文件，确保其完整性及安全性。

3.2 报关组负责出口货物之报关文件的申办，确保安全完整。

3.3 出货部负责付运货物资料的完整及准确。

4. 程序：

4.1 船务文件管制

4.1.1 船务资料（包括船务订单、提柜单、承运单、装柜资料、生产排期表等）必须以高度保密的方式予以保存。若为书面形式则必须储存在上锁的文件柜中，并规定只有船务组人员或以上级高层管理人员才有权使用。货物未上船的船务资料严禁借阅。

4.1.2 若为电子文件则必须储存内部网络公共硬盘中，并只设置文件存取权限给有需要使用船务资料人员。

4.1.3 书面形式或电子形式的船务资料至少保存 12 个月。

4.1.4 只有授权的人员负责货物运输的相关资料，如货运时间安排表、运输表格、货运公司资料等。

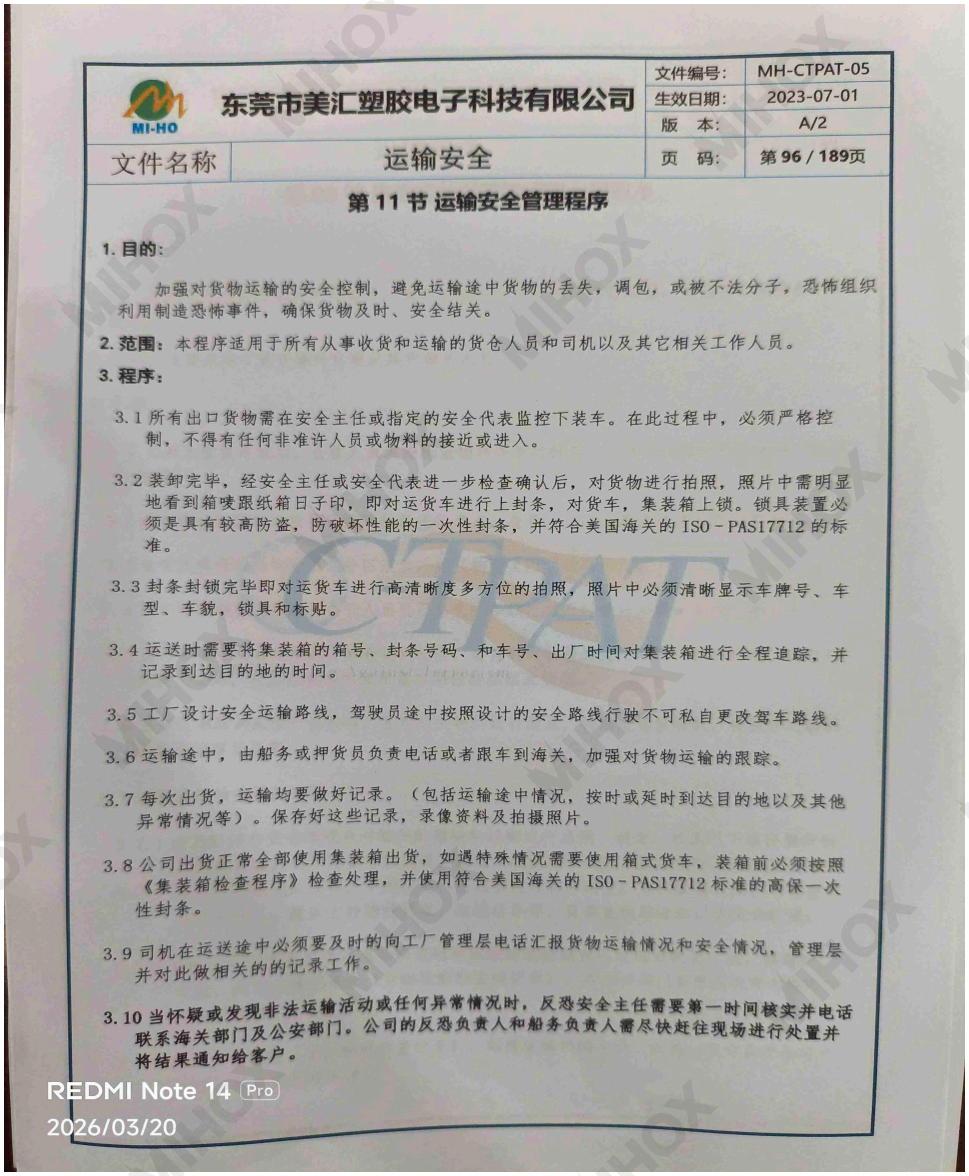
4.1.5 所有货物运输资料均属于保密资料，相关人员应时刻确保文件准确、完整、合法，防止被偷换、丢失或包含错误信息，当发现相关文件被恶意修改、偷换、丢失或发生其他异常情况进应及时报部门主管及安全经理。

4.2 报关文件管制

C-TPAT
REDMI Note 14 Pro
2026/03/20

#91 written procedure in place that restricts access to shipping and receiving documentation.jpg

Procedural Security - 问题 # 95



东莞市美汇塑胶电子科技有限公司	文件编号:	MH-CTPAT-05
	生效日期:	2023-07-01
	版 本:	A/2
文件名称 运输安全	页 码:	第 96 / 189页

第 11 节 运输安全管理程序

1. 目的:

加强对货物运输的安全控制，避免运输途中货物的丢失，调包，或被不法分子，恐怖组织利用制造恐怖事件，确保货物及时、安全结关。

2. 范围: 本程序适用于所有从事收货和运输的货仓人员和司机以及其它相关工作人员。

3. 程序:

3.1 所有出口货物需在安全主任或指定的安全代表监控下装车。在此过程中，必须严格控制，不得有任何非准许人员或物料的接近或进入。

3.2 装卸完毕，经安全主任或安全代表进一步检查确认后，对货物进行拍照，照片中需明显地看到箱唛跟纸箱日子印，即对运货车进行上封条，对货车，集装箱上锁。锁具装置必须是具有较高防盗，防破坏性能的一次性封条，并符合美国海关的 ISO－PAS17712 的标准。

3.3 封条封锁完毕即对运货车进行高清晰度多方位的拍照，照片中必须清晰显示车牌号、车型、车貌，锁具和标贴。

3.4 运送时需要将集装箱的箱号、封条号码、和车号、出厂时间对集装箱进行全程追踪，并记录到达目的地的时间。

3.5 工厂设计安全运输路线，驾驶员途中按照设计的安全路线行驶不可私自更改驾车路线。

3.6 运输途中，由船务或押货员负责电话或者跟车到海关，加强对货物运输的跟踪。

3.7 每次出货，运输均要做好记录。（包括运输途中情况，按时或延时到达目的地以及其他异常情况等）。保存好这些记录，录像资料及拍摄照片。

3.8 公司出货正常全部使用集装箱出货，如遇特殊情况需要使用箱式货车，装箱前必须按照《集装箱检查程序》检查处理，并使用符合美国海关的 ISO－PAS17712 标准的高保一次性封条。

3.9 司机在运送途中必须要及时的向工厂管理层电话汇报货物运输情况和安全情况，管理层并对此做相关的的记录工作。

3.10 当怀疑或发现非法运输活动或任何异常情况时，反恐安全主任需要第一时间核实并电话联系海关部门及公安部门。公司的反恐负责人和船务负责人需尽快赶往现场进行处置并将结果通知给客户。

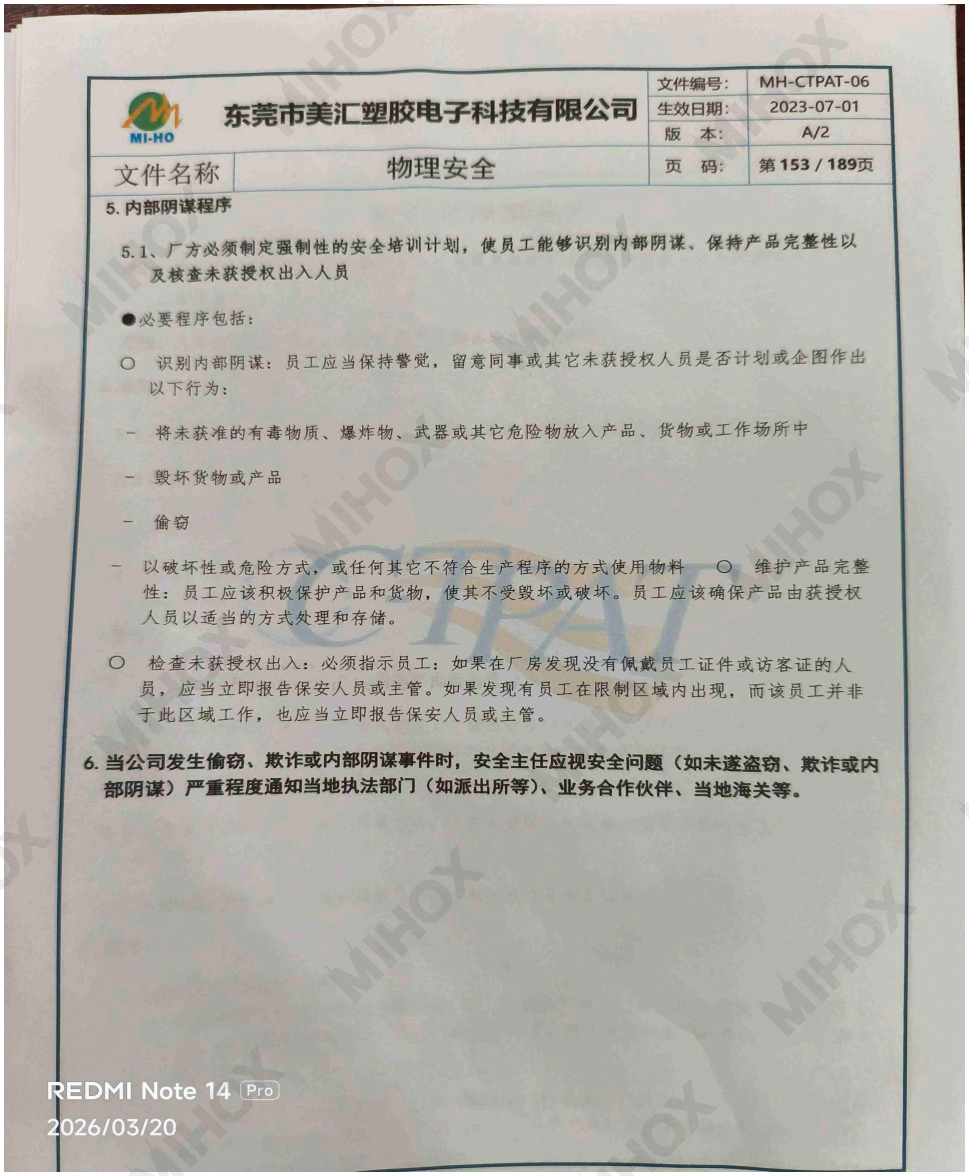
REDMI Note 14 Pro
2026/03/20

#95 notify when illegal shipping activity or any abnormality is suspected or detected.jpg

Procedural Security - 问题 # 96

#96 authorized employees access procedure.jpg

Procedural Security - 问题 # 97



东莞市美汇塑胶电子科技有限公司	文件编号:	MH-CTPAT-06
	生效日期:	2023-07-01
	版 本:	A/2
文件名称 物理安全	页 码:	第 153 / 189页

5. 内部阴谋程序

5.1、厂方必须制定强制性的安全培训计划，使员工能够识别内部阴谋、保持产品完整性以及核查未获授权出入人员

●必要程序包括：

○ 识别内部阴谋：员工应当保持警觉，留意同事或其它未获授权人员是否计划或企图作出以下行为：

- 将未获准的有毒物质、爆炸物、武器或其它危险物放入产品、货物或工作场所中
- 毁坏货物或产品
- 偷窃
- 以破坏性或危险方式，或任何其它不符合生产程序的方式使用物料

○ 维护产品完整性：员工应该积极保护产品和货物，使其不受毁坏或破坏。员工应该确保产品由获授权人员以适当的方式处理和存储。

○ 检查未获授权出入：必须指示员工：如果在厂房发现没有佩戴员工证件或访客证的人员，应当立即报告保安人员或主管。如果发现有员工在限制区域内出现，而该员工并非于此区域工作，也应当立即报告保安人员或主管。

6. 当公司发生偷窃、欺诈或内部阴谋事件时，安全主任应视安全问题（如未遂盗窃、欺诈或内部阴谋）严重程度通知当地执法部门（如派出所等）、业务合作伙伴、当地海关等。

REDMI Note 14 Pro
2026/03/20

#97 procedure to notify Business Partners of security issues such as attempted theft, fraud or internal conspiracies.jpg

Procedural Security - 问题 # 99

#99 written procedure of key control.jpg

Physical Security - 问题 # 106



#106 shipping and receiving area.jpg

Physical Security - 问题 # 109

#109 physical barriers.jpg

Physical Security - 问题 # 110

#110 factory gate.jpg

Physical Security - 问题 # 118



#118 CCTV control room and monitors.jpg

Physical Security - 问题 # 120



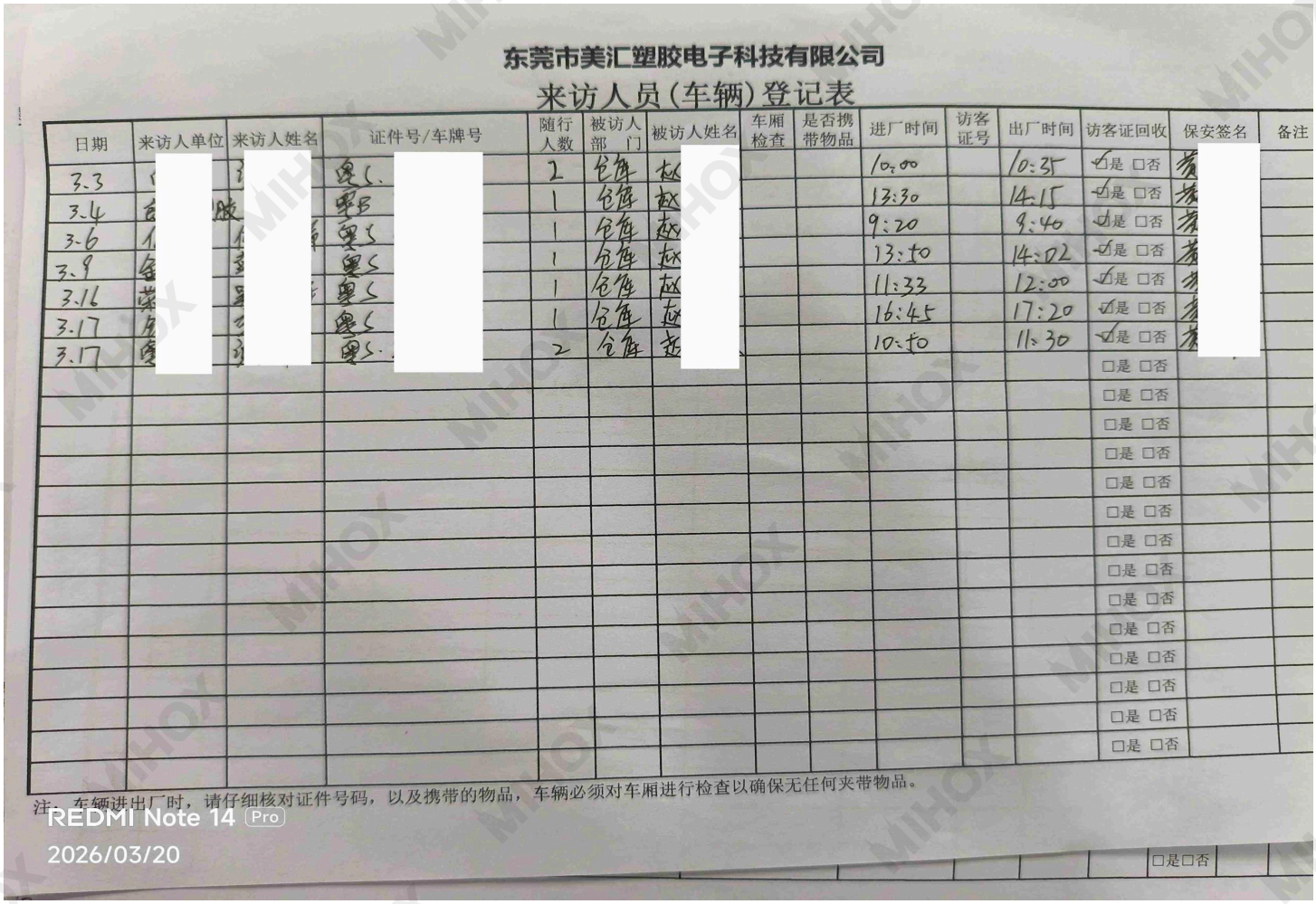
#120 CCTV records.jpg

Physical Security - 问题 # 123



#123 insufficient CCTV records kept.jpg

Physical Security - 问题 # 125



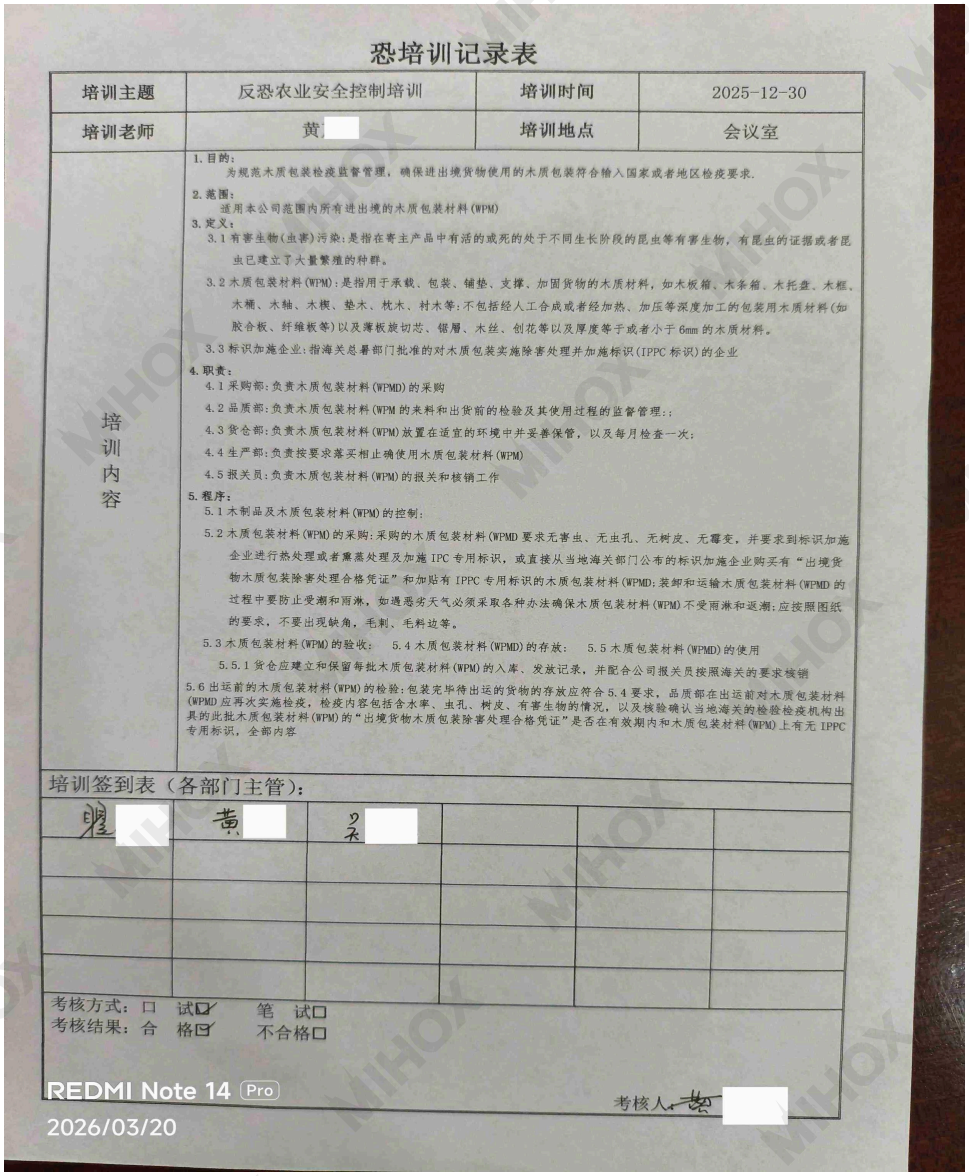
#125 visitor log.jpg

Physical Security - 问题 # 127



#127 visitor badges.jpg

Security Training & Threat Awareness - 问题 # 138



恐培训记录表

培训主题	反恐农业安全控制培训	培训时间	2025-12-30
培训老师	黄	培训地点	会议室

培训内容

1. 目的：
为规范木质包装检疫监督管理，确保进出境货物使用的木质包装符合输入国家或者地区检疫要求.

2. 范围：
适用本公司范围内所有进出境的木质包装材料(WPM)

3. 定义：
3.1 有害生物(虫害)污染:是指在寄主产品中有活的或死的处于不同生长阶段的昆虫等有害生物，有昆虫的证据或者昆虫已建立了大量繁殖的种群。
3.2 木质包装材料(WPM):是指用于承载、包装、铺垫、支撑、加固货物的木质材料，如木板箱、木条箱、木托盘、木框、木桶、木轴、木楔、垫木、枕木、衬木等;不包括经人工合成或者经加热、加压等深度加工的包装用木质材料(如胶合板、纤维板等)以及薄板旋切芯、锯屑、木丝、刨花等以及厚度等于或者小于 6mm 的木质材料。
3.3 标识加施企业:指海关总署部门批准的对木质包装实施除害处理并加施标识(IPPC 标识)的企业

4. 职责：
4.1 采购部:负责木质包装材料(WPMD)的采购
4.2 品质部:负责木质包装材料(WPM 的来料和出货前的检验及其使用过程的监督管理:;
4.3 货仓部:负责木质包装材料(WPM)放置在适宜的环境中并妥善保管，以及每月检查一次;
4.4 生产部:负责按要求落实相止确使用木质包装材料(WPM)
4.5 报关员:负责木质包装材料(WPM)的报关和核销工作

5. 程序：
5.1 木制品及木质包装材料(WPM)的控制:
5.2 木质包装材料(WPM)的采购:采购的木质包装材料(WPMD 要求无害虫、无虫孔、无树皮、无霉变。并要求到标识加施企业进行热处理或者熏蒸处理及加施 IPC 专用标识，或直接从当地海关部门公布的标识加施企业购买有“出境货物木质包装除害处理合格凭证”和加贴有 IPPC 专用标识的木质包装材料(WPMD;装卸和运输木质包装材料(WPMD 的过程中要防止受潮和雨淋，如遇恶劣天气必须采取各种办法确保木质包装材料(WPM)不受雨淋和返潮;应按照图纸的要求，不要出现缺角，毛刺、毛料边等。
5.3 木质包装材料(WPM)的验收; 5.4 木质包装材料(WPMD)的存放; 5.5 木质包装材料(WPMD)的使用
5.5.1 货仓应建立和保留每批木质包装材料(WPM)的入库、发放记录，并配合公司报关员按照海关的要求核销
5.6 出运前的木质包装材料(WPM)的检验:包装完毕待出运的货物的存放应符合 5.4 要求，品质部在出运前对木质包装材料(WPMD 应再次实施检疫，检疫内容包括含水率、虫孔、树皮、有害生物的情况，以及核验确认当地海关的检验检疫机构出具的此批木质包装材料(WPM)的“出境货物木质包装除害处理合格凭证”是否在有效期内和木质包装材料(WPM)上有无 IPPC 专用标识，全部内容

培训签到表（各部门主管）：

腾	黄	关			

考核方式：口 试☑ 笔 试口
考核结果：合 格☑ 不合格口

考核人：

REDMI Note 14 Pro
2026/03/20

#138 security and agricultural inspection training.jpg

Security Training & Threat Awareness - 问题 # 139

#139 security criteria for restricted areas training.jpg

Misc - 问题 # 147

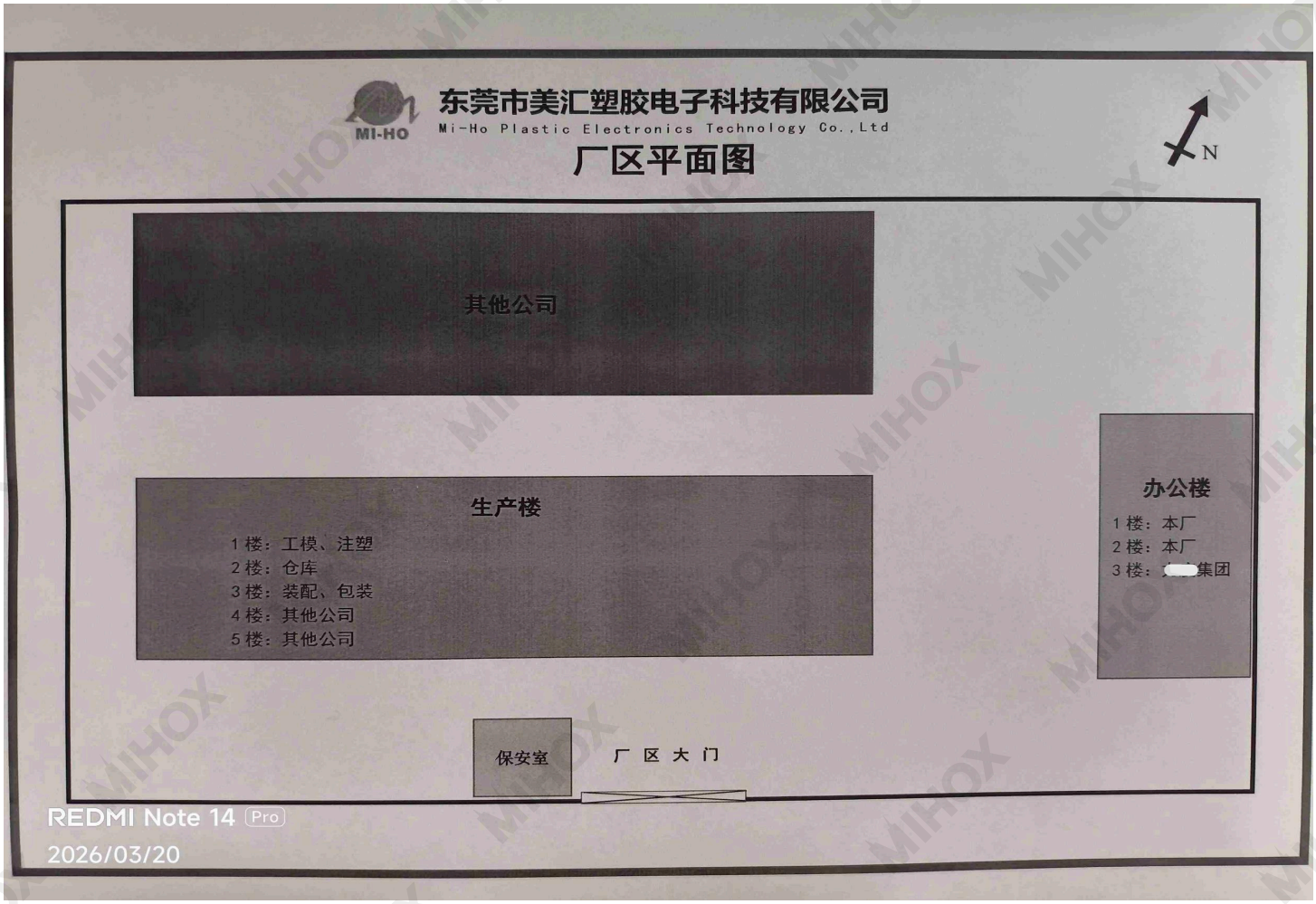
#147 factory name.jpg

Misc - 问题 # 148



#148 security guard on duty.jpg

Misc - 问题 # 149



#149 factory layout.jpg

Misc - 问题 # 150



#150 shipping and receiving area.jpg

Misc - 问题 # 151



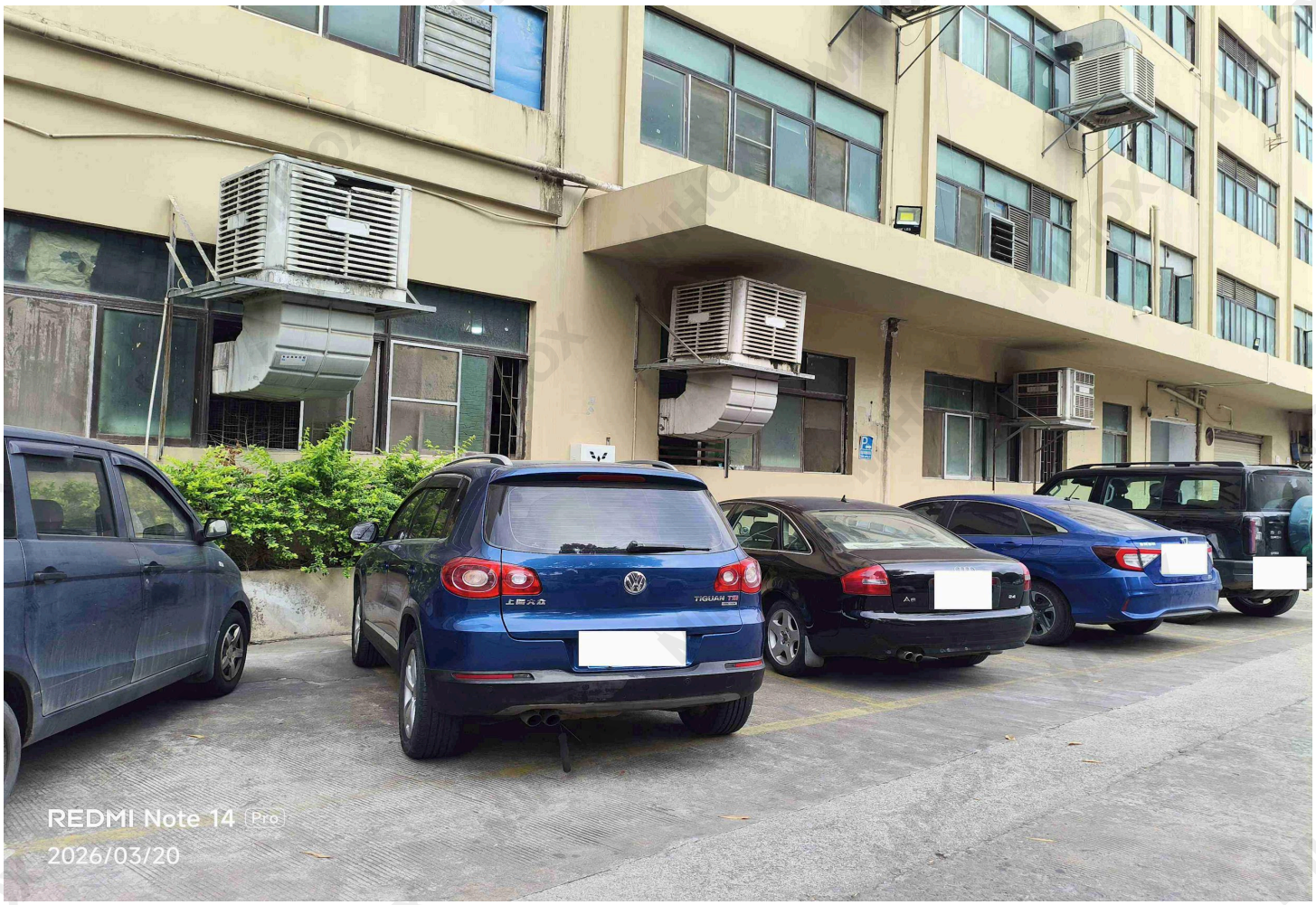
#151 factory fence.jpg

Misc - 问题 # 152



#152 packing workshop.jpg

Misc - 问题 # 153



#153 private parking area.jpg