FACILITY SECURITY ASSESSMENT

CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM

IMPORTER/MANUFACTURING/EXPORTER SECURITY CRITERIA (2020)

Introduction:

This assessment is intended to assist clients in conducting a comprehensive assessment of their international supply chain as well as individual facilities to assess their own state of compliance. The assessment is based upon the C-TPAT security criteria including importer, manufacturing and exporter minimum security requirements. Evaluation is based upon our assessment of the physical, procedural, documentary and security management systems of the facility on the day of the on-site assessment of the facility named below in Section 3.

This report is not to be construed as a certification of the company's management system nor proof of compliance to any security standard. It is a report to show a) the degree to which the facility was found compliant with C-TPAT security requirements on the day of the assessment; b) the issues that were found to not be compliant with C-TPAT security requirements that should be improved or corrected to evidence compliance to reduce risk to the supply chain; c) the relative security risk stated as "low", "medium" or "high" that the facility is rated and d) the identification of any 'best practices' employed by the facility.

CLIENT INFORMATION			
Client Name (owner of the report)	**Omkar Corporation**		
Address	BLDG NO- D-1, Gala No-110 to 115, and BLDGNO- D-2, Gala no -110 to 112, Harihar Complex		
City, State/Province, Postal Code	Dapoda, Bhiwandi, Thane, Maharashtra -421302		
Country	India		
Client Contact Person and Title	Mr. Manoj Dnyanmothe – Director		
Contact Person Telephone	+91-9323128856	Email	sales@omkaecorproation.net

AUDIT COMPANY DETAILS/INFORMATION	
Audit Company	**Accordia Global Compliance Group**
Office / Regional Office Responsible	Delhi/India
Auditor:	Anil Tiwari, Lead Auditor

SITE ASSESSMENT FACILITY DETAILS/INFORMATION			
Facility Name	**Omkar Corporation**		
Facility Name in Local Language	**Omkar Corporation**		
Address	BLDG NO- D-1, Gala No-110 to 115, and BLDGNO- D-2, Gala no -110 to 112, Harihar Complex		
City, State/Province	Dapoda, Bhiwandi, Thane, Maharashtra	Postal Code	421302
Country	India		
Facility Contact Person and Title	Mr. Manoj Dnyanmothe – Director		
Contact Person Telephone	+91-9323128856	Email	sales@omkaecorproation.net
Facility Business License	Factory License No. 13340 Valid till 31st December 2025		
A. Products/Activities at the facility site	The factory is into manufacturing and exporting Christmas decorations, ribbons, textile items & garments. The main productions processes are carried out by this facility are procurements of Raw material (Fabric &		

	Yarn) – Embroidery or Printing - Cutting - Fusing - Stitching – Checking – Packing –Dispatch. Production Capacity – 18000 pieces per day.		
B. Site Description	Description of site and surroundings	Factory has one building in the premises which is in good condition. Total area factory was 1580 square meters. The building is located in an industrial area on 1580 Square meters of land and is surrounded by 5-meter fence. There are two entry gates with guards 24x7.	
		Level Number	Total Size (ft^2 or mt^2)
	Production Building	1	17000 Square Feet
	Shipping Area	1	1500 Square Feet
	Other Building (explain)		
C. Is there any night production work at the site?	□ Yes ☒ No		
D. Are there any on-site worker dormitory buildings?	□ Yes ☒ No If yes, explain:		
	Location of building(s)	.	
	Approximate No. of workers in dormitories		
Is warehouse customs bonded:	□ Yes ☒ No		
Is facility located in a Free Zone:	☒ Yes □ No If YES, provide details:	Facility is located in industrial zone.	

Summary of Noncompliance/Observations/Best Practices					
C-TPAT Requirement	**Record Number of Issues**				**NC Findings Only** *(note to auditor, summarize in as few words as possible NC's only)*
	Non Compliance		Observation	Best Practice	
	Must	Should			
1. Corporate Security					
2. Risk Assessment					
3. Business Partner					
4. Cybersecurity					
5. Transportation					
6. Seal Security					
7. Procedural Security					
8. Agricultural Security					
9. Physical Security					
10. Physical Access Controls	1	1			It was noted that there was a procedure manual that visitors/vendors were positively identified upon arrival at the facility, but the auditor of this audit and his car driver were not identified. It was noted during review of records and interaction with management that the facility has not screened the arrived packages and emails for contraband before being admitted.
11. Personnel Security					
12. Education, Training and Awareness					
Total NC's (A)	1	1	0	0	
Point values per issue (B)	**-2**	**-1**	**-0.5**	**+1**	

Points deduction/addition (A) x (B)	-2	-1	0	0	-3	**(C)** Total points (Σ of all columns)
Total points = 91 (D)	(91-03) / 91 x100 =		96.70		**Final Score**	
Calculation instruction:	((D-C) ÷ D) x 100 = Final Score					

RATING OF BUSINESS

Based on the results of the assessment of the business against the C-TPAT Security Criteria, the RISK TO THE SUPPLY CHAIN based on evaluation of security measures is considered to be:

	SCORE	RISK RATING
✓	**90 -100**	**MINIMAL - PASS**
	75-89	**LOW – PASS**
	65-74	**MEDIUM – CAP REQUIRED**
	Below 65	**HIGH - FAIL**

Minimal Risk = PASSING

Low Risk = PASSING

Findings may be reviewed for improvement and best practices considered for implementation

Medium Risk = CORRECTIVE ACTIONS REQUIRED FOR SCORE TO MEET 75%

Facility shall be given the opportunity to improving their score to 75% through corrective action. Corrective Action should be focused on areas of greatest risk so that security controls can be implemented to reduce or mitigate overall risk and best practices considered for implementation. Corrective Actions can be submitted for Desktop Review.

High Risk = FAILED – BELOW 65

"MUST" requirements generally not met and the company has deficient security management systems. Corrective Action Plan is not recommended but, factory shall be allowed time to make improvements and then request to be re-audited within a reasonable time period. Best practices should be considered for implementation.

Assessment Parameters

A. Assessment Date:	14th September 2024			
B: Time in and time out	Day 1 Time in:	09:00	Day 2 Time in:	N/A
	Day 1 Time out:	17:00	Day 2 Time out:	N/A
C: Number of Assessment Days Used:	1.0			
D: Assessment type:	☒ Full Initial ☐ Periodic (annual, bi-annual, etc.) ☐ Follow–up to clear CAP/NCs			
E: Was the assessment announced?	☐ Announced ☒ Semi – announced: Window detail: 4 weeks ☐ Unannounced			
F: Who signed and agreed security CAP *(Name and job title)*	Mr. Manoj Dnyanmothe – Director			
G: Previous assessment date:	N/A			
H: Previous assessment type:	☐ Full Initial ☐ Periodic (annual, bi-annual, etc) ☐ Follow–up to clear CAP/NCs			
I: Was any previous assessment reviewed during this assessment?	☐ Yes ☐ No Not Applicable			

Logistics and Transportation			
			Comments
A. Percentage of Exports to the United States are shipped by:	Ocean Shipping	95%	
	Ground/Container Trucks	0%	
	Air	5%	
	Rail	0%	

B. Companies used for export transportation:	Ocean:	Quick Transport	Containers/Month Shipped:	10	
	Ocean:	n/a	Containers/Month Shipped:	0	
	Ground/ Truck	n/a	Containers/Month Shipped:	0	
	Ground/ Truck	n/a	Containers/Month Shipped:	0	
	Ground/ Truck	n/a	Containers/Month Shipped:	0	
	Air:	Quick Transport	Containers/Month Shipped:	1	
	Other:	n/a	Containers/Month Shipped:	0	
C. Ground Transport Companies transporting containers from facility to port of export:	Name:	Quick Transport	C-TPAT Member?	Yes	
	Name:		C-TPAT Member?		
	Name:		C-TPAT Member?		

SECTION 1 – Security Criteria – Corporate Security			
		Non-Compliance Raised (✓ if NC raised)	
1 - Security Vision/Responsibility 1.1 Commitment to Security: *In promoting a culture of security, companies should demonstrate their commitment to supply chain security and the CTPAT Program through a statement of support.* *The statement should be signed by a senior company official and displayed in appropriate company locations.*	Statement of support should highlight the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband. Senior company officials who should support and sign the statement may include the president, CEO, general manager, or security director. Areas to display the statement of support include the company's website, on posters in key areas of the company (reception; packaging;	Describe the company's statement of support (security policy) and its location in the facility: Omkar Corporation has a statement of support that is found in the company's Security Policy. The policy is posted on the wall of the entrance to the office and at the employee entry and the warehouse shipping office.	

	warehouse; etc.), and/or be part of company security seminars, etc		
1.2 Responsibility within the Company: *To build a robust Supply Chain Security Program, a company should incorporate representatives from all of the relevant departments into a cross-functional team. These new security measures should be included in existing company procedures, which creates a more sustainable structure and emphasizes that supply chain security is everyone's responsibility.*	Supply Chain Security has a much broader scope than traditional security programs. It is intertwined with Security, in many departments such as Human Resources, Information Technology, and Import/Export offices. Supply Chain Security programs built on a more traditional, security department-based model may be less viable over the long run because the responsibility to carry out the security measures are concentrated among fewer employees, and, as a result, may be susceptible to the loss of key personnel.	List the person's titles that are part of the cross-functional team for assuring cargo security and compliance to CTPAT requirements: Mr. Manoj Dnyanmothe – Director	
1.3 System Review: *The supply chain security program **must** be designed with, supported by, and implemented by an appropriate written review component.* *The purpose of this review component is to document that a system is in place whereby personnel are held accountable for their responsibilities and all security procedures outlined by the security program are being carried out as designed.* *The review plan must be updated as needed based on pertinent changes in an organization's operations and level of risk.*	The goal of a review is to ensure that employees are following the company's security procedures. ▪ The review process does not have to be complex ▪ Company decides the scope of reviews and how in-depth they will be ▪ Normally, based on company's role in the supply chain, business model, level of risk ▪ Smaller companies may create a very simple review methodology ▪ Company may choose to use smaller targeted reviews directed at specific procedures (e.g. seal control, container	Does the company perform regular (at least ANNUAL) review of their supply chain security program? Check Yes or No ☒ Yes ☐ No If NO, explain:	

	inspection, manifesting, etc.) - However, it's best for the company to conduct an overall general review, periodically, to ensure that all areas of the security program are working as designed - If the company is already conducting reviews as part of larger annual management review, that process is sufficient to meet this requirement		
1.4 Competence * (ONLY CTPAT MEMBERS): *The company's point(s) of contact (POC) for CTPAT* ***must*** *be knowledgeable about CTPAT program requirements. These individuals need to provide regular updates to upper management on issues related to the program, including the progress or outcomes of any audits, security related exercises, and CTPAT validations.* * NOTE 6.4 is only answered IF the company being audited is a CTPAT Member – ignore this question if the auditee is a supplier factory that is NOT a member of CTPAT	CTPAT expects the designated POC to be a proactive individual who engages and is responsive to his or her Supply Chain Security Specialist. This competence is expected throughout the supply chain to manufacturers. Members may identify additional individuals who may help support this function by listing them as contacts in the CTPAT Portal.		

SECTION 2 – Security Criteria – Manufacturers, Brokers, Trucking Companies, Exporters, etc.			
		Non-Compliance Raised (✓ if NC raised)	
2.1 Risk Assessment (facility) *Foreign Manufacturers, Brokers, Consolidators, Trucking Companies, etc. **must** have a documented and verifiable process for determining risk in their factory and, if applicable, throughout their supply chains based on their business model (i.e. volume, country of origin, routing, C-TPAT membership, potential terrorist threat via open source information, having inadequate security, past security incidents, etc.)* *The RA **must** identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities. The member must take into account CTPAT requirements specific to the member's role in the supply chain.*	The overall risk assessment (RA) has two key parts. a) Self-assessment of the company's security practices, procedures, and policies to understand vulnerabilities b) Identification of local threat(s) based on the company's business model / role in the supply chain. A simple method is assigning the level of risk between low, medium, and high. Risk assessment best practice is to use C-TPAT 5 Step Risk Assessment methodology.	Describe the results of their RA: Omkar Corporation factory has conducted security risk assessment by using the 5 Step C-TPAT Risk Analysis methodology 2nd September 2024	
2.2 Risk Assessment (Mapping) *Since the manufacturer is part of the international portion of an importer's own risk assessment, the factory should document or map the movement of its cargo, to the extent possible, throughout its portion of the supply chain (from the point of origin to the importer's distribution center.)* *The mapping should include all business partners involved both directly and indirectly in the exportation/movement of the goods. As applicable, mapping should include documenting how cargo moves in and out of transport facilities/cargo hubs and noting if the cargo is "at rest" at one of these locations for an extended period of time. Cargo is more vulnerable when "at rest," waiting to move to the next leg of its journey.*	When developing a process to map supply chains, high risk areas are the first to be considered. When documenting the movement of cargo, the company is to consider all applicable involved parties - including those who will only be handling the import/export documents such as customs brokers and others that may not directly handle the cargo, but may have operational control such as Non Vessel Operated Common Carriers (NVOCCs) or Third Party Logistics Providers (3PLs). If any portion of the transport is subcontracted, this may also be considered because the more layers of indirect parties, the greater risk involved. The mapping exercise involves looking more in-depth at how your supply chain works.	Does the company perform mapping of their cargo? Check Yes or No ☒ Yes ☐ No	

2.3 Risk Assessment (Reviews) *Risk assessments must be reviewed annually, or more frequently as risk factors dictate.*	Circumstances that may require a risk assessment to be reviewed more frequently than once a year include: ▪ an increased threat level from a specific country ▪ periods of heightened alert ▪ following a security breach or incident ▪ changes in business partners ▪ changes in corporate structure/ownership such as mergers / acquisitions	Has the company performed a Risk Analysis within the past 12 months? Check Yes or No ☒ Yes ☐ No If no, explain:	
2.4 Crisis Management Plan *Companies should have written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption.*	A crisis may include: ▪ the disruption in movement of trade data due to a cyberattack, ▪ a fire, ▪ carrier driver being hijacked by armed individuals. Based on risk and where the company operates from, contingency plans may include: ▪ additional security notifications or support; ▪ how to recover what was destroyed or stolen ▪ returning to normal operating conditions.	Does the company have a Crisis Management Plan that addresses the steps to follow in the case of emergencies and disruption to movement of trade? Check Yes or No ☒ Yes ☐ No	

SECTION 3 – Business Partner Selection			
		Non-Compliance Raised (✓ if NC raised)	
3.1 Business Partner Screening *Foreign manufacturers must have written, risk-based process for screening new business partners and for monitoring current partners.* *A factor that companies should include in this process is checks on activity related to money laundering and terrorist funding.* *Included are written and verifiable processes for the selection of business partners including, carriers, other manufacturers, product suppliers and vendors (parts and raw material suppliers, etc.).*	The following are examples of some of the checking elements that can help determine if a company is legitimate: ▪ Verifying the company's business address and how long they have been at that address ▪ Conducting research on the internet on both the company and its owners ▪ Checking business references ▪ Requesting a credit report. Examples of business partners that need to be screened are: ▪ direct business partners such as manufacturers ▪ product suppliers ▪ pertinent vendors ▪ service providers ▪ transportation/logistics providers. ▪ vendors/service providers that are directly related to the company's supply chain and/or handle sensitive information /equipment are also included on the list to be screened ▪ includes brokers ▪ contracted IT providers. Depth of screening depends on the level of risk in the supply chain	Describe the process: Omkar Corporation in Thane, Maharashtra, India selects their raw material suppliers, Kora suppliers and other business partners by way of a documented due diligence process whereby a new supplier fills in a Due Diligence Questionnaire with information about the company's financial strength, owners background and integrity, company's business license to operate, local tax authority approval, etc. Ground transportation companies are designated buy the corporate logistics department and are limited to only using CTPAT member trucking companies or Non-CTPAT companies who submit to annual audits and provide written commitment, signed by the top management, to comply with CTPAT security requirements. The Omkar Corporation compliance head of Security reviews the Due Diligence form for any issues that may present a risk. If issues are found, the VP of Security will require further information or have an independent security assessment performed prior to approval of a new business partner.	
3.2 Screening to include CTPAT membership *The business partner screening process must take into account whether a partner is a CTPAT Member or a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States (or an approved MRA).*	Note: This requirement is applicable to IMPORTERS, however, can also apply to factories who contract with vendors/conveyances. Business partners' CTPAT certification may be found via the CTPAT Portal's Status Verification Interface system. If the business partner certification is from a foreign AEO program under an MRA with	Are business partners selected based on their CTPAT membership or other mutually recognized program (if applicable) Check as appropriate: ☒ Yes ☐ No	

Certification in either CTPAT or an approved AEO is acceptable proof for meeting program requirements for business partners. *Companies must obtain evidence of the certification and continue to monitor these business partners to ensure they maintain their certification.*	the United States, the foreign AEO certification will include the security component. MRAs include: New Zealand, Canada, Jordan, Japan, South Korea, the European Union (28 member states), Taiwan, Israel, Mexico, Singapore, the Dominican Republic, and Peru.	□ NA - No AEO or MRA is applicable in this country	
<u>3.3 Due Diligence/Security Audits</u> * <u>(ONLY CTPAT MEMBERS):</u> *When a company outsources or contracts elements of its supply chain, the company **must** exercise due diligence (via visits, questionnaires, etc.) to ensure these business partners have security measures in place that meet or exceed CTPAT's Minimum Security Criteria (MSC).* * NOTE 7.5.3 is only answered IF the company being audited is a CTPAT Member Importer – ignore this question if the auditee is a supplier factory that is NOT a member of CTPAT	Importers and exporters tend to outsource a large portion of their supply chain activities. Importers (and some exporters) are the parties in these transactions that usually have leverage over their business partners and can require that security measures are implemented throughout their supply chains, as warranted. For those business partners that are not CTPAT or accepted MRA members, the CTPAT Member will exercise due diligence to ensure (when it has the leverage to do so) that these business partners meet the program's applicable security criteria. To verify adherence to security requirements, importers conduct security assessments of their business partners.		
<u>3.4 Corrective Action – Security Assessments</u> *If weaknesses are identified during business partners' security assessments, they **must** be addressed as soon as possible, and corrections must be implemented in a timely manner. Company must confirm that deficiencies have been mitigated via documentary evidence.*	Auditor Note: CTPAT recognizes that there will be different timelines for making corrections based on what is needed for the correction. Installing physical equipment may take more time than a change to a procedure but the security problem must be addressed upon discovery. Based on the level of risk involved and the importance of the weakness found, some issues may require immediate attention. If it is a deficiency that may jeopardize the security of a container, for instance, it should be addressed as soon as possible.	As a result of past security audits performed at this facility, did the company agree to make the corrective actions to findings in the audit in a timely manner? Check Yes or No ☒ Yes □ No If NO, explain:	
<u>3.5 Social Compliance</u> *Companies should have a documented social compliance program in place that, at a minimum, addresses how the*	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.	Forced Labor is defined by ILO Convention No. 29. Does the facility have a social compliance program (e.g. SA8000,	

company ensures goods are not mined, produced or manufactured, wholly or in part, with prohibited forms of labor, i.e., forced, imprisoned, indentured, or indentured child labor.	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. There are US legal requirements that prohibit the importation of merchandise mined, produced or manufactured, wholly or in part, in any foreign country by forced or indentured child labor – including forced child labor.	SMETA, internal Code of Conduct) to which they regularly (annual) audit? If YES, explain: SEDEX	

SECTION 4 – Cypersecurity

Non-Compliance Raised (✓ if NC raised)

Cybersecurity is the key to safeguarding a company's most precious assets:

- intellectual property,
- customer information,
- financial and trade data,
- employee records

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

4.1 Cybersecurity Policies and Procedures *Companies must have comprehensive written cybersecurity policies and/or procedures to protect information technology (IT) systems. The written IT policy, at a minimum, must cover all of the individual Cybersecurity criteria.*	Members are encouraged to follow cybersecurity protocols that are based on recognized industry frameworks/ standards. The *National Institute of Standards and Technology (NIST) is one such organization that provides a Cybersecurity Framework (https://www.nist.gov/cyberframework) that offers voluntary guidance based upon existing standards, guidelines, and practices to help manage and reduce cybersecurity risks both internally and externally.	Does the company have comprehensive written cybersecurity policies and procedures in place? Check Yes or No ☒ Yes ☐ No	
4.2 Cybersecurity – Threat Protection *To defend Information Technology (IT) systems against common cybersecurity threats, a company must install sufficient software/hardware protection from malware (viruses, spyware, worms, Trojans, etc.) and internal/external intrusion (firewalls) in company's computer systems. Companies must ensure that their security software is current and receives regular security updates. Members must have policies and procedures to prevent attacks via social engineering. If a data breach occurs or another unseen event results in the loss of data and/or equipment, procedures must include the recovery (or replacement) of IT systems and/or data.*		Does the company have software/hardware protection against security breach in place? Check Yes or No ☒ Yes ☐ No If yes, state what is in place: -Facility is using firewall and anti-malware software in conjunction with employee education. - Restricted IT admin and access rights to a small handful of users is invaluable in minimizing the risk of data breaches as employees cannot	

		give away information they don't have access to. - Using protocols, such as creating temporary passwords for contractors or expediting the onboarding process for new hires, will also help to minimize scenarios in which password sharing is needed in the workplace	
4.3 Cybersecurity – IT Systems Testing *Companies using network systems must regularly test the security of their IT infrastructure. If vulnerabilities are found, corrective actions must be implemented as soon as feasible.*	The company may conduct vulnerability scans. VS identifies openings (open ports and IP addresses), operating systems, and software through which a hacker could gain access to the company's IT system. The VS does this by comparing the results of its scan against a database of known vulnerabilities and produces a correction report for the business to act upon. There are many free and commercial versions of vulnerability scanners available.	Does the company perform Vulnerability Scans of their systems? Check Yes or No ☒ Yes □ No If YES, what is the frequency: Quarterly ___________________________	
4.4 Cybersecurity – Sharing of Threat Information *Cybersecurity policies should address how a company shares information on cybersecurity threats with the government and other business partners.*	Companies are encouraged to share information on cybersecurity threats with the government and business partners within their supply chain. Companies may want to join the National Cybersecurity and Communications Integration Center (NCCIC - https://www.us-cert.gov/nccic). The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. (Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost)	Does the company have membership in NCCIC or any other information sharing group? Check Yes or No □ Yes ☒ No	
4.5 Cybersecurity – Detection Systems *A system must be in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and*		Does the company have any methods to detect unauthorized access to IT systems or any blocking mechanism for improper access to external websites/tampering? Check Yes or No	

tampering or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions.		☒ Yes □ No If YES, explain: - Facility installed hardware and software firewall in the computers to protect it from the unauthorized incoming and outgoing data.	
4.6 Cybersecurity – Periodic Review of Policies *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.*		Does the company meet to review and update cybersecurity policies and procedures at least annually? Check Yes or No ☒ Yes □ No Date of most recent review: 02/09/2024	
4.7 Cybersecurity – User Access Restriction *User access must be restricted based on job description or assigned duties. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements. Computer and network access must be removed upon employee separation.*		Does the company : 1. Restrict access based on job description or assignments: ☒ Yes □ No 2. Review access rights of persons on a regular basis (at least annually): ☒ Yes □ No 3. Ensure that system access is terminated immediately (same day) upon worker separation: ☒ Yes □ No	
4.8 Cybersecurity – Login and Passwords *Individuals with access to Information Technology (IT) systems must use individually assigned accounts.* *Access to IT systems must be protected from infiltration via the use of strong passwords,*	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	Does the company : 1. Provide persons with individually assigned login/ accounts? ☒ Yes □ No 2. Are workers with access to IT systems forced to use strong passwords or some strong way to	

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.*	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	protect passwords and use them to gain access to systems?: ☒ Yes ☐ No 3. Does the system ensure/ require workers to change passwords regularly (30, 60, 90 days)?: ☒ Yes ☐ No What is the frequency? 30 Days	
4.9 Cybersecurity – Remote Access *Companies 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.* *Companies must also have procedures designed to prevent remote access from unauthorized users.*	VPNs are not the only choice to protect remote access to a network. Multi-factor authentication (MFA) is another method. An example of a multi-factor authentication would be a token with a dynamic security code that the employee must type in to access the network.	Does the company : 1. Allow users to remotely connect to company networks? ☒ Yes ☐ No If YES, what technologies used to ensure remote access protection Facility is using Network Access Control technic to ensure remote access protection. 2. If YES, does the company have documented procedures to prevent remote access from unauthorized users? ☒ Yes ☐ No	
4.10 Cybersecurity – Personal Devices *If companies 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.	Does the company allow personal devices to be used and connected to the company's networks?: ☐ Yes ☒ No If YES, do they require devices to be tested receive regular security updates? ☐ Yes ☐ No	

4.11 Cybersecurity – Software Licensure *Cybersecurity policies and procedures should include measures to prevent the use of counterfeit or improperly licensed technological products.*	Software is intellectual property (IP) owned by the entity that created it. Without permission of the manufacturer or publisher, it is illegal to install software, no matter how it is acquired. Permission usually takes the form of a license from the publisher, which comes with authorized copies of software. Unlicensed software is: ▪ More likely to fail as a result of an inability to update. ▪ More prone to contain malware, ▪ Does not come with warranties or support ▪ Forces companies on its own to deal with failures. ▪ Brings legal consequences for unlicensed software ▪ Civil penalties ▪ Criminal prosecution. Companies 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 that authentic products are bought and to protect against counterfeiting.	Does the company purchase only licensed software?: ☒ Yes ☐ No If YES, explain the process to obtain legal/legitimate software: Facility has a policy to obtain legal/legitimate software from the authorized publisher/website only which has license key as well. ___________________________ ____________________________	
4.12 Cybersecurity – Data Backup *Data should be backed up once a week or as appropriate. All sensitive and confidential data should be stored in an encrypted format.*		Does the company conduct a full backup of network systems and PC workstation data?: ☒ Yes ☐ No If YES, what is the frequency: ☐ Daily ☐ Weekly ☐ Bi-Weekly ☒ Monthly ☐ Other:________________	
4.13 Cybersecurity – Inventory *All media, hardware, or other IT equipment that contains sensitive*	Some types of computer media are hard drives, removable drives, CD-ROM or CD-R discs, DVDs, or USB drives. The National Institute for Systems and Technology (NIST) has developed the	Does the company maintain an inventory of all media, hardware and other IT equipment that deals with the import/export process?	

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.*	government's data media destruction standards. Companies may want to consult NIST standards for sanitization and destruction of IT equipment and media. Media Sanitization: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization	☒ Yes ☐ No When the company destroys equipment, do they properly sanitize in accordance with NIST guidelines? ☒ Yes ☐ No	

SECTION 5 - TRANSPORTATION SECURITY

Conveyance and Instruments of International Traffic Security – Smuggling schemes often involve the modification of conveyances and Instruments of International Traffic (IIT), or the hiding of contraband inside IIT.
This criteria category covers security measures designed to prevent, detect, and/or deter the altering of IIT structures or surreptitious entry into them, which could allow the introduction of unauthorized material or persons.
At the point of stuffing/loading, procedures need to be in place to inspect IIT and properly seal them. Cargo in transit or "at rest" is under less control, and is therefore more vulnerable to infiltration, which is why seal controls and methods to track cargo/conveyances in transit are key security criteria.
Breaches in supply chains occur most often during the transportation process; therefore, Members must be vigilant that these key cargo criteria be upheld throughout their supply chains.

Non-Compliance Raised (✓ if NC raised)

5.1 Conveyance Storage *Conveyances and Instruments of International Traffic (IIT) must be stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure of an Instrument of International Traffic or (as applicable) allow the seal/doors to be compromised.*	The secure storage of conveyances and Instruments of International Traffic (both empty and full) is important to guard against unauthorized access.	Does the company store containers, loaders or other loading devices securely when not in use? ☒ Yes ☐ No Provide details: Yes facility has a documented procedure to store container and loaders security when not in use. They identified the empty containers as ''at rest'' to guard against unauthorized access. ______________________________ ______________________________	
5.2 Inspection – Security and Agriculture *The CTPAT inspection process must have written procedures for both security and agricultural inspections.*	With the prevalence of smuggling schemes that involve the modification of conveyances or Instruments of International Traffic, it is imperative that Members conduct inspections of conveyances and Instruments of International Traffic to look for visible pests and serious structural deficiencies. Likewise, the prevention of pest contamination via conveyances and IIT is of paramount concern, so an agricultural component has been added to the security inspection process.	Check all that are used by company: ☒ Ocean Containers ☐ Flatbeds ☐ Unit load devices (ULDs), ☐ Lift vans, ☐ Cargo vans, ☐ Shipping tanks, ☐ Bins, ☐ Skids, ☐ Pallets, ☐ Caul Boards, ☐ Cores for textile fabrics, ☐ Other specialized containers For any checked, indicate those that are not inspected by the company: No, Facility has maintained the inspection	

		checklist and policies procedure and doing inspection when required. ___________________________ ___________________________	
5.3.1 Container Inspection (except Canada & Mexico) *7/8 point inspection must be conducted on all empty containers and unit load devices (ULS) / 8 point inspection must be conducted on all empty refrigerated containers and ULDs (only for shipments via ocean, air, and land borders (as applicable) by rail or intermodal freight)* *1. Front wall;* *2. Left side;* *3. Right side;* *4. Floor;* *5. Ceiling/Roof;* *6. Inside/outside doors, including the reliability of the locking mechanisms of the doors;* *7. Outside/Undercarriage; and* *8. Fan housing on refrigerated containers.*	Security and agricultural inspections must be 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. Expectations for overseas supply chains are to inspect all instruments of IIT at the point of stuffing/packing. However, if an ocean/air based supply chain is higher risk, it may warrant including more extensive inspection procedures to include conveyances and/or inspections at marine port terminals or air logistics facilities. Usually, there are higher levels of risk involved in shipments with land border crossings, which is why both the conveyance and IIT undergo multiple inspections.	Does the company perform 7 point inspections/ 8 point inspections on refrigerated containers? (Verify through review of 5 recent inspection reports) ☒ Yes ☐ No Indicate non-compliances: ___________________________ ___________________________	
5.3.2 Container Inspection (Canada & Mexico land crossing ONLY) *Additional inspection requirements for land border crossings via highway carriers:* *Inspections of conveyances and IIT must be conducted at conveyance/IIT storage yards. Where feasible, inspections must be conducted upon entering and departing the storage yards and at the point of loading/stuffing.*	Security and agricultural inspections must be 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. Expectations for overseas supply chains are to inspect all instruments of IIT at the point of stuffing/packing.	(Canada and Mexico ONLY) Does the company perform 17 point inspections on Tractors and Trailers? (Verify through review of 5 recent inspection reports) ☐ Yes ☐ No Indicate non-compliances: __________________________ __________________________	

Inspections must include 17-point inspections: ***Tractors:*** *1. Bumper/tires/rims;* *2. Doors, tool compartments and locking mechanisms;* *3. Battery box;* *4. Air breather;* *5. Fuel tanks;* *6. Interior cab compartments/sleeper; and* *7. Faring/roof* ***Trailers:*** *1. Fifth wheel area - check natural compartment/skid plate;* *2. Exterior - front/sides;* *3. Rear - bumper/doors;* *4. Front wall;* *5. Left side;* *6. Right side;* *7. Floor;* *8. Ceiling/roof;* *9. Inside/outside doors and locking mechanisms;* *10.Outside/Undercarriage.*			
5.4 External Container Hardware *Conveyances and Instruments of International Traffic (as appropriate) must be equipped with external hardware that can reasonably withstand attempts to remove it. The door, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism must be fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device.*	Companies are suggested to consider using containers/trailers with tamper resistant hinges. Companies 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.	Does the company use conveyances and IIT equipped with hardware that can reasonably withstand attempts to remove? ☒ Yes ☐ No If no, indicate non-compliances: ___________________________ ___________________________	
5.5 Conveyance and IIT inspection by checklist	This is a recommendation, not a requirement.	Does the company use an inspection checklist for all conveyances and IIT? ☒ Yes ☐ No If yes, is this document signed by supervisor? Yes	

The inspection of all conveyances and empty Instruments of International Traffic should be recorded on a checklist. *The following elements should be documented on the checklist:* *• Container/ Trailer/ Instruments of International Traffic number;* *• Date of inspection;* *• Time of inspection;* *• Name of employee conducting the inspection;* *• Specific areas of the Instruments of International Traffic that were inspected.* *If the inspections are supervised, the supervisor should also sign the checklist.* *The completed container/Instruments of International Traffic inspection sheet should be part of the shipping documentation packet.* *The consignee should receive the complete shipping documentation packet prior to receiving the merchandise.*		☒ Yes ☐ No If yes, is this document included with the shipping documentation and provided to consignee prior to receipt of the cargo? ☒ Yes ☐ No	
5.6 Location of Security Inspections of Conveyances *All security inspections should be performed in an area of controlled access and, if available, monitored via a CCTV system.*	This is a recommendation, not a requirement.	Does the company perform inspection of conveyances in a controlled access area? ☒ Yes ☐ No Is the area where the inspections are performed under CCTV monitoring? ☒ Yes ☐ No	
5.7 Visible Pest Contamination *If visible pest contamination is found during the*	Keeping records on the types of contaminants found, where they were found (conveyance location), and how the pest contamination was eliminated, are helpful actions that may assist companies in preventing future pest contamination.	Is there evidence of pest contamination during inspection? ☒ Yes ☐ No	

conveyance/Instruments of International Traffic inspection, washing/vacuuming ***must*** *be carried out to remove such contamination. Documentation must be retained for one year to demonstrate compliance with these inspection requirements.*		If yes, provide description of evidence: Facility has maintained the documentation of pest contamination of with pictorial evidence. Documents verified during the audit and found satisfactory.	
5.8 Risk-based Random Conveyance Search *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.* • *conducted at random without warning,* • *shall not become predictable.* • *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.*	Supervisory searches of conveyances may be conducted to counter internal conspiracies. As a best practice, supervisors can hide an item (like a toy or colored box) in the conveyance to determine if the field test screener/conveyance operator finds it. Supervisory personnel could be a security manager, held accountable to senior management for security, or other designated management personnel.	Does the company perform secondary and random searches of conveyances in addition to regular inspections by traffic personnel? ☒ Yes ☐ No If yes, briefly explain the process/procedure: Facility has a procedure to random search of conveyances by management personnel after the transportation staff have conducted.	
5.9 Conveyance Tracking – origin to final destination *CTPAT Members should work with their transportation providers to track conveyances from origin to final destination point.* *Specific requirements for tracking, reporting, and sharing of data should be incorporated within terms of service agreements with service providers.*	This is a recommendation, not a requirement.	Does the company track conveyances from point of origin to destination? ☒ Yes ☐ No If yes, briefly explain: All containers are locked and sealed. If the shipment is being sent on trucks then it is locked. Facility tracks the location of trucks/cargo with high frequently over the phone.	

<u>5.10 GPS access by Shippers</u> *Shippers should have access to their carrier's GPS fleet monitoring system, so they may track the movement of their shipments.*	This is a recommendation, not a requirement.	Does the company have access to the carrier GPS system? ☐ Yes ☒ No If yes, briefly explain: ______________________________ ______________________________	
<u>5.11 NO STOP policy for land border crossing in proximity to US (Canada/ Mexico ONLY)</u> *For land border shipments that are in proximity to the United States border, a "no-stop" policy should be implemented with regard to unscheduled stops.*	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	Does the company or conveyance company have a NO STOP policy in place for cargo passing through land border crossings? ☐ Yes ☐ No N/A If yes, briefly explain: ______________________________ ______________________________	
<u>5.12 "Last Chance" Tampering Verification (Canada/ Mexico ONLY)</u> *In areas of high risk, and immediately prior to arrival at the border crossing, CTPAT Members should incorporate a "last chance" verification process for U.S. bound shipments for checking conveyances/Instruments of International Traffic for signs of tampering to include visual inspections of conveyances and the VVTT seal verification process. Properly trained individuals should conduct the inspections.*	This is a recommendation, not a requirement.	Does the company or conveyance company have a Last Chance Verification process in place for cargo passing through land border crossings? ☐ Yes ☐ No If yes, briefly explain: Not Applicable ______________________________	

V – View seal and container 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.*			
5.13 Threat Alerts *If a credible (or detected) threat to the security of a shipment or conveyance is discovered, the Member must alert (as soon as feasibly possible) any business partners in the supply chain that may be affected and any law enforcement agencies, as appropriate.*	There should be a documented procedure within the company's security manual to state the process for communicating alerts to other business partners in the supply chain.	Does the company have a documented procedure to report alerts to other business partners in the company's supply chain? ☒ Yes ☐ No If yes, briefly explain: The facility has a documented procedure within the company's security manual to state the process for communicating alerts to other business partners in the supply chain. ______________________________	

SECTION 6 - SEALS

Seal Security – The sealing of trailers and containers, to include continuous seal integrity, continues to be a crucial element of a secure supply chain. Seal security includes having a comprehensive written seal policy that addresses all aspects of seal security; using the correct seals per CTPAT requirements; properly placing a seal on an IIT, and verifying that the seal has been affixed properly.

Non-Compliance Raised (✓ if NC raised)

6.1 Seal Procedures *CTPAT Members must have detailed, written high-security seal procedures* *• Describe how seals are issued and controlled at the facility and during transit.* *• Procedures must provide the steps to take if a seal is altered, tampered with, or has the incorrect seal number, including documentation of the event, communication protocols to partners, and investigation of the incident.* *• The findings from the investigation must be documented, and any corrective actions must be implemented as quickly as possible.* *• The written procedures must be maintained at the local operating level so that they are easily accessible.* *• Procedures must be reviewed at least once a year and updated as necessary.* *• Written seal controls must include the following elements:* ***Controlling Access to Seals**:*	The secure storage of conveyances and Instruments of International Traffic (both empty and full) is important to guard against unauthorized access.	Does the company have a documented Seal Procedure meeting the following requirements? 1. Procedure describes how seals are issues and controlled while in storage and during transit: ☒ Yes ☐ No 2. Procedure has steps to take if a seal is altered, tampered with, incorrect number as well as how to document and communicate of incidents : ☒ Yes ☐ No 3. Does the procedure include a requirement to document findings and take quick corrective actions for any findings from investigations? ☒ Yes ☐ No 4. Does the company have local documented seal procedures (not at regional or corporate level) for ease of accessibility?: ☒ Yes ☐ No 4. Does the company review and update, at least annually, the documented seal procedures? ☒ Yes ☐ No	

• Management of seals is restricted to authorized personnel. *• Secure storage.* ***Inventory, Distribution, & Tracking (Seal Log):*** *• Recording the receipt of new seals.* *• Issuance of seals recorded in log.* *• Track seals via the log. • Only trained, authorized personnel may affix seals to Instruments of International Traffic (IIT).* ***Controlling Seals in Transit**:* *• When picking up sealed IIT (or after stopping) verify the seal is intact with no signs of tampering.* *• Confirm the seal number matches what is noted on the shipping documents.* ***Seals Broken in Transit:** • If a load is examined by Customs, record the replacement seal number.* *• The driver must immediately notify dispatch when a seal is broken, indicate who broke the seal, and provide the new seal number.* *• The carrier must immediately notify the shipper, broker, and importer of the seal change and the replacement seal number.* *• The shipper must note the replacement seal number in the seal log.* ***Seal Discrepancies:*** *• Retain altered or tampered seals to aid in investigations.* *• Investigate the discrepancy; follow-up with corrective measures (if warranted). • As*		5. Does the company's seal procedures include all of the following (check all that apply)?: ☒ Access to seals restricted ☒ Seals are stored securely ☒ Seals received are recorded ☒ Seals issued are recorded ☒ Seals are tracked via log ☒ Seals are affixed on IIT only by trained persons ☒ Seals are verified as intact when IIT is collected for transit ☒ Seal numbers are confirmed against manifest documents For seals broken in transit, is there a procedure to ensure that (check all that apply): ☒ Replacement Seal numbers are recorded on the shipping documents ☒ Drivers are required to notify their dispatcher when a seal is broken and actions taken ☒ Replacement Seal information is reported to shipper, broker and importer that a seal was broken and a replacement was used ☒ Replacement Seal numbers are recorded on the seal log of the exporter For Seal Discrepancies, are there documented procedures to ensure that (check all that apply):	

applicable, report compromised seals to CBP and the appropriate foreign government to aid in the investigation.		☒ Seals are kept that are altered or tampered with to help in investigations ☒ Companies investigate discrepancies and do follow-up and take corrective actions ☒ Companies include procedures to report compromised seals to Customs and Border Protection and the appropriate foreign government to help in investigations	
6.2 Sealing Containers IITs • *All CTPAT shipments that can be sealed* ***must*** *be secured immediately after loading/stuffing/packing by the responsible party (i.e. the shipper or packer acting on the shipper's behalf)* • ***Must*** *use A high-security seal that meets or exceeds the most current ISO 17712 standard for high-security seals. Qualifying cable and bolt seals are both acceptable.* • *All seals used* ***must*** *be securely and properly affixed to IITs for cargo to/from the United States.*	The high-security seal used must be placed on the secure cam position, if available, instead of the right door handle. The seal must be placed at the bottom of the center most vertical bar of the right container door. The seal could be placed on the center most left-hand locking handle on the right container door if the secure cam position is not available. If a bolt seal is being used, it is recommended that the bolt seal be placed with the barrel portion or insert facing upward with the barrel portion above the hasp.	☒ Sealing was observed during the audit ☒ Seal was affixed to the secure cam position ☒ Seal was affixed to bottom of center most vertical bar (right side) or left locking handle of the right container door	
6.5 Seals meet ISO17712 *Companies* ***must*** *be able to document that the high-security seals they use meet or exceed the most current ISO 17712 standard.*	Acceptable evidence of compliance is a copy of a laboratory testing certificate that demonstrates compliance with the ISO high-security seal standard. Companies are expected to be aware of the tamper indicative features of the seals they purchase.	Seals used meet or exceed ISO17712 requirements for high security seals ☒ Yes ☐ No	
6.6 Seals are purchased by company *If the company buys and keeps an inventory of seals:*	Some companies rely on the shipper to provide the seal. If the shipper is a CTPAT member, they will likely have ISO17712 compliant seals.	Does the company purchase and maintain an inventory of seals? ☒ Yes ☐ No If NO, proceed to next question.	

• company management or a security supervisor **must** *conduct a seal audit that includes periodic inventory of stored seals* *•* **must** *reconcile against seal inventory logs and shipping documents.* *•audits* **must** *be documented.* *• in the seal audit process, dock supervisors and/or warehouse managers* **must** *periodically verify seal numbers used on conveyances IIT.*	9.6 is only required if the company being audited buys and maintains an inventory of seals.	If YES, are seals compliant with ISO17712 Standard (review certificate for compliance) ☒ Yes ☐ No	
6.7 CTPAT Seal Verification Process *CTPAT's seal verification process* **must** *be followed to ensure all high-security seals (bolt/cable) have been affixed properly to Instruments of International Traffic, and are operating as designed.* *The procedure is known as the VVTT process:* *V – View seal and container 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.*	When applying cable seals, they need to envelop the rectangular hardware base of the vertical bars in order to eliminate any upward or downward movement of the seal. Once the seal is applied, make sure that all slack has been removed from both sides of the cable. The VVTT process for cable seals needs to ensure the cables are taut (tight). 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.	Auditor instruction: Observe the sealing process to confirm that the seal has been applied properly and that the company performed the VVTT protocol. The company applies a high-security seal and performs VVTT process to ensure the seal is operating as designed. ☒ Yes ☐ No	

SECTION 7 - PROCEDURAL SECURITY

Procedural Security encompasses many aspects of the import-export process, documentation, and cargo storage and handling requirements. Other vital procedural criteria pertain to reporting incidents and notification to pertinent law enforcement. Additionally, CTPAT often requires that procedures be written because it helps maintain a uniform process over time. Nevertheless, the amount of detail needed for these written procedures will depend upon various elements such as a company's business model or what is covered by the procedure.

CTPAT recognizes that technology used in supply chains continues to evolve. The terminology used throughout the criteria references written procedures, documents, and forms, but this does not mean these have to be paper based. Electronic documents, signatures, and other digital technologies are acceptable to meet these measures.

The Program is not designed to be a "one size fits all" model; each company must decide (based on its risk assessment) how to implement and maintain procedures. However, it is more effective to incorporate security processes within existing procedures rather than create a separate manual for security protocols. This creates a more sustainable structure and helps emphasize that supply chain security is everyone's responsibility.

		Non-Compliance Raised (✓ if NC raised)	
<u>7.1 Conveyance Overnight Staging</u> *When cargo is staged overnight, or for an extended period of time, measures **must** be taken to secure the cargo from unauthorized access.*	The secure storage of conveyances and Instruments of International Traffic (both empty and full) is important to guard against unauthorized access.	Does the company stage loaded containers, loaders or other loading devices overnight? □ Yes ☒ No If YES, provide details about security measures to keep cargo safe from unauthorized access:	
<u>7.2 Inspection for Pest Contamination</u> *Cargo staging areas, and the immediate surrounding areas, **must** be inspected on a regular basis to ensure these areas remain free of visible pest contamination.*	Preventative measures such as the use of baits, traps, or other barriers can be used as necessary. Removal of weeds or reduction of overgrown vegetation may help in the elimination of pest habitat within staging areas.	Company performs regular inspection inside and outside where cargo is staged and loaded ☒ Yes □ No Evidence of pest contamination is evident. ☒ Yes □ No If YES, provide details: ___________________________ Facility has maintained record of pest contamination with pictorial evidence.__________________________	

7.3 Supervised loading *The loading/stuffing of cargo into containers/IIT should be supervised by a security officer/manager or other designated personnel.*		Company requires loading of IIT under supervision by manager, security guard or other designated personnel? ☒ Yes ☐ No If YES, person name and/or title: **Mr. Manoj Dnyanmothe – Director**	
7.4 Digital Photograph at Loading/Stuffing *As documented evidence of the properly installed seal, digital photographs should be taken at the point of stuffing. To the extent feasible, these images should be electronically forwarded to the destination for verification purposes.*	Photographic evidence may include pictures taken at the point of stuffing to document evidence of the cargo markings, the loading process, the location where the seal was placed, and properly installed seal.	Company takes digital photos of all container/IIT units at time of sealing? ☒ Yes ☐ No	
7.5 Document Processing *Procedures **must** be in place to ensure that all information used in the clearing of merchandise/cargo is legible; complete; accurate; protected against the exchange, loss, or introduction of erroneous information; and reported on time.*		Are procedures in place to ensure that all information used in the clearing of merchandise/ cargo, is legible, complete, accurate, and protected against the exchange, loss or introduction of erroneous information? ☒ Yes ☐ No	
7.6 Document Processing (if electronic documents are used by the company, skip to next question) *If paper documents are used, forms and other import/export related documentation should be secured to prevent unauthorized use.*	Measures, such as using a locked filing cabinet, can be taken to secure the storage of unused forms, including manifests, to prevent unauthorized use of such documentation.	Does company provide secure storage of paper forms (e.g. manifests, commercial invoices, etc.)? ☒ Yes ☐ No	
7.7 Accuracy of Shipping Documents *• The shipper or its agent **must** ensure that bill of ladings (BOLs) and/or manifests accurately*	When picking up sealed Instruments of International Traffic, carriers may rely on the information provided in the shipper's shipping instructions. Requiring the seal number to be electronically printed on the bill of lading (BOL) or other export documents helps	Do all three accurately reflect the requirements for accuracy (all documents for a shipment are correct and all agree – seal number, description, quantities, etc) ☒ Yes ☐ No	

reflect the information provided to the carrier • *carriers **must** exercise due diligence to ensure these documents are accurate.* • *BOLs and manifests **must** be filed with U.S. Customs and Border Protection (CBP) in a timely manner.* • *BOL information filed with CBP **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.*	guard against changing the seal and altering the pertinent document(s) to match the new seal number. However, for certain supply chains, goods may be examined in transit, by a foreign Customs authority, or by CBP. Once the seal is broken by the government, there needs to be a process to record the new seal number applied to the IIT after examination. In some cases, this may be handwritten.	If NO, describe: ______________________________ ______________________________	
7.8 Documented Incidence Reporting Procedure *For MANUFACTURERS: Companies **must** have written procedures for:* • *reporting an incident, which includes a description of the facility's internal escalation process.* • *A notification protocol **must** be in place to report any suspicious activities or security incidents (such as drug seizures, discovery of stowaways, etc.) that take place anywhere around the world and which affects the security of the supply chain.* •*For IMPORTERS ONLY: As applicable, the Member must report any global incidents to its Supply Chain Security Specialist, the closest port of entry, any pertinent law enforcement agencies, and business partners that may be part of the affected supply chain.* • *Notifications to CBP must be made as soon as feasibly possible and in advance of any conveyance or IIT crossing the border.* • *Notification procedures must include the accurate contact information that lists the*	Examples of incidents warranting notification to U.S. Customs and Border Protection include (but are not limited to) the following: • Discovery of tampering with a container/IIT or high-security seal; • Discovery of a hidden compartment in a conveyance or IIT; • An unaccounted new seal has been applied to an IIT; • Smuggling of contraband, including people; stowaways; • Unauthorized entry into conveyances, locomotives, vessels, or aircraft carriers; • Extortion, payments for protection, threats, and/or intimidation; • Unauthorized use of a business entity identifier (i.e., Importer of Record (IOR) number, Standard Carrier Alpha (SCAC) code, etc.).	Does company have a written procedure for: ☒ reporting incidents internally ☒ has an internal escalation procedure. ☒ has a notification protocol to notify ☐ No procedure exists	

name(s) and phone number(s) of personnel requiring notification, as well as for law enforcement agencies. Procedures must be periodically reviewed to ensure contact information is accurate.			
7.9 Challenging Unauthorized Persons *Procedures **must** be in place to identify, challenge, and address unauthorized/ unidentified persons.* *Personnel **must** know the protocol to challenge an unknown/unauthorized person, how to respond to the situation, and be familiar with the procedure for removing an unauthorized individual from the premises.*		Are documented procedures in place to identify, challenge and address unauthorized or unidentified persons? ☒ Yes ☐ No Through interview with personnel, do they know the protocol to challenge persons who are unknown or unauthorized to be in the facility and what is necessary for removing that individual from the premises. ☒ Yes ☐ No	
7.10 Anonymous Reporting Mechanism *Companies should set up a mechanism for workers to report security related issues anonymously.* *When an allegation is received, it should be investigated, and if applicable, corrective actions should be taken.*	Internal problems such as theft, fraud, and internal conspiracies may be reported more readily if the reporting party knows the concern may be reported anonymously. Companies can set up a hotline program or similar mechanism that allows people to remain anonymous if they fear reprisal for their actions. It is recommended that any report be kept as evidence to document that each reported item was investigated and that corrective actions were taken.	Is there an anonymous reporting system or mechanism that workers can use to report issues related to security issues? ☒ Yes ☐ No If YES, describe: Facility has a mechanism for workers to report security related issues anonymously. Facility has displayed the details regarding this in the notice board. ______________________	
7.11 Significant Discrepancies – Investigations *All shortages, overages, and other significant discrepancies or anomalies in cargo shipments **must** be investigated and resolved, as appropriate.*	There must be a method for companies to investigate issues where discrepancies exist between manifest documentation and actual cargo received and that investigation method is in place to find the answers.	Is there a system or process in place to investigate significant discrepancies in cargo shipments between point of export and point of destination? ☒ Yes ☐ No If YES, describe: Facility has a system in place to investigate issues where discrepancies exist. Facility maintained	

		register regarding is there any discrepancies happened. ____________________________	
7.12 Reconciliation of Cargo *Arriving cargo should be reconciled against information on the cargo manifest. Departing cargo should be verified against purchase or delivery orders.*	Some importers will use electronic systems to scan cargo at destination. The scan will be used to provide details of the cargo received versus the manifests and purchase orders. In some cases, importers will use manual processes to confirm cargo received against manifests.	Is there a system or process in place to reconcile cargo received against the manifest documents? ☒ Yes ☐ No If YES, describe: Facility is using electronic systems to scan cargo at destination. The scan will be used to provide details of the cargo received versus the manifests and purchase orders.	
7.13 Notification of Seal Numbers to Consignees *Seal numbers assigned to specific shipments should be transmitted to the consignee prior to departure.*	The consignee is the **receiver** of the shipment and is usually the owner of the goods. The consignee is listed on a Bill of Lading as the responsible party to receive the cargo. This question is to know if the manufacturer shipping the cargo notifies the consignee in advance of the cargo being shipped	Does the company notify the consignee of the seal numbers prior to the departure of the cargo? ☒ Yes ☐ No	
7.14 Recording Seal Numbers on Shipping Documents *Seal numbers should be electronically printed on the bill of lading or other shipping documents.*	Manifests and other shipping documents (Bill of Lading, Commercial Invoice, etc.) should have the Seal Number electronically printed on the documents.	Does the company print seal numbers onto shipping documents in an electronically printed way? ☒ Yes ☐ No	
7.15 Internal Investigation of Security Incidents • *Companies* ***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*	Companies must have a process or procedure to conduct internal investigations of any security incident, including acts of terrorism, discovery of narcotics or stowaways, absconders (run-aways/fugitives)	Does the company have a documented Internal Investigation procedure to timely conduct investigations of any security-related issues as required by the standard? ☒ Yes ☐ No	

government law enforcement agency. *• The internal company investigation **must** be documented, completed as soon as feasibly possible, and made available to CBP/CTPAT and any other law enforcement agency, as appropriate, upon request.*			

SECTION 8 - AGRICULTURAL SECURITY

Agriculture is the largest industry and employment sector in the U.S. It is also an industry threatened by the introduction of foreign animal and plant contaminants such as soil, manure, seeds, and plant and animal material which may harbor invasive and destructive pests and diseases. Eliminating contaminants in all conveyances and in all types of cargo may decrease CBP cargo holds, delays, and commodity returns or treatments. Ensuring compliance with CTPAT's agricultural requirements will also help protect a key industry in the U.S. and the overall global food supply.

Key Definition: Pest contamination – The International Maritime Organization defines pest contamination as visible forms of animals, insects or other invertebrates (alive or dead, in any lifecycle stage, including egg casings or rafts), or any organic material of animal origin (including blood, bones, hair, flesh, secretions, excretions); viable or non-viable plants or plant products (including fruit, seeds, leaves, twigs, roots, bark); or other organic material, including fungi; or soil, or water; where such products are not the manifested cargo within instruments of international traffic (i.e. containers, unit load devices, etc.)

Non-Compliance Raised (✓ if NC raised)

8.1 Procedures to prevent visible pest contamination *• Companies **must**, in accordance with their business model, have written procedures designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations.* *• Visible pest prevention measures **must** be adhered to throughout the supply chain* *• Measures regarding WPM **must** meet the International Plant Protection Convention's*	WPM is defined as wood or wood products (excluding paper products) used in supporting, protecting, or carrying a commodity. WPM includes items such as pallets, crates, boxes, reels, and dunnage. Frequently, these items are made of raw wood that may not have undergone sufficient processing or treatment to remove or kill pests, and therefore remain a pathway for the introduction and spread of pests. Dunnage (containers and packaging used for cargo) has been shown to present a high risk of introduction and spread of pests.	Does the company have written procedures designed to prevent visible pest contamination and to comply with WPM regulations? ☒ Yes ☐ No Does the company have visible pest prevention measures (e.g. bait traps) in place? ☒ Yes ☐ No	

(IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15).	The IPPC is a multilateral treaty overseen by the United Nation's Food and Agriculture Organization that aims to secure coordinated, effective action to prevent and to control the introduction and spread of pests and contaminants. ISPM 15 includes internationally accepted measures that may be applied to WPM to reduce significantly the risk of introduction and spread of most pests that may be associated with WPM. ISPM 15 affects all wood packaging material requiring that they be debarked and then heat treated or fumigated with methyl bromide and stamped or branded with the IPPC mark of compliance. This mark of compliance is known as the "wheat stamp". Products exempt from the ISPM 15 are made from alternative materials, like paper, metal, plastic or wood panel products (i.e. oriented strand board, hardboard, and plywood). 	If the company exports food and agricultural products, does the company's measures meet the IPPC Standards for ISPM 15? ☐ Yes ☐ No ☒ N/A, no food/agriculture is exported	

SECTION 9 - PHYSICAL SECURITY
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. One of the cornerstones of CTPAT is flexibility, and security programs should be customized to fit each company's circumstances. The need for physical security can vary greatly based on the Member's role in the supply chain, its business model, and level of risk. The physical security criteria provides a number of deterrents/obstacles that will help prevent unwarranted access to cargo, sensitive equipment, and/or information, and Members should employ these security measures throughout their supply chains
Non-Compliance Raised (✓ if NC raised)

9.1 Physical Barriers to prevent unauthorized access	Physical barriers can be fences but also can be dividing walls, natural / architectural barriers	Does the company have physical barriers that prevent unauthorized access to cargo handling, storage areas and trailer yards and office?	

• all cargo handling facilities • storage facilities • trailer yards • offices **must** have physical barriers and/or deterrents that prevent unauthorized access.		☒ Yes ☐ No If NO, Explain: ____________________________ ____________________________	
9.2 Physical Security - Fencing *Perimeter fencing must enclose the areas around cargo handling and storage facilities.* *If a facility handles cargo, interior fencing should be used to secure cargo and cargo handling areas.* *Based on risk, additional interior fencing should segregate various types of cargo such as domestic, international, high value, and/or hazardous materials.* *Fencing should be regularly inspected for integrity and damage by designated personnel. If damage is found in the fencing, repairs should be made as soon as possible.*		Does the company have fencing that encloses EXTERNAL cargo handling, storage areas? ☒ Yes ☐ No Does the company have INTERIOR fencing that encloses areas to separate domestic, international, high-value and hazardous materials? ☒ Yes ☐ No If NO, provide details: ___________________________ If fences are in place, (review inspection reports) determine if they are inspected regularly (weekly) for integrity and damage and reported to management for repairing? ☐ Yes , fences are inspected and reports are made ☒ No, fences are not inspected **It was noted during review of documentation and interaction with staff member that facility has not inspected fencing for integrity and damage.** ☐ NA, fences are not in place	✓

9.3 Physical Security – Gates and Gate Houses *Gates where vehicles and/or personnel enter or exit (as well as other points of egress)* ***must*** *be manned or monitored. Individuals and vehicles may be subject to search in accordance with local and labor laws.*	It is recommended that the number of gates be kept to the minimum necessary for proper access and safety. Other points of egress would be entrances to facilities that are not gated. The number of gates should be kept to the minimum necessary for proper access and safety.	Does the facility have guards/personnel stationed or have CCTV monitoring at entry gates through which vehicles and/or personnel enter or exit? ☒ Yes ☐ No	
		How many gates in place for Vehicles: 01 Personnel: 01	
9.4 Physical Security – Parking *Private passenger vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas, and conveyances.*	Facilities should locate parking areas outside of fenced and/or operational areas - or at least at substantial distances from cargo handling and storage areas.	Does the facility limit parking of vehicles near or in cargo handling areas and where IITs and containers are kept? ☒ Yes ☐ No	
9.5 – Lighting *Adequate lighting* ***must*** *be provided inside and outside the facility including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas.*	Automatic timers or light sensors that automatically turn on appropriate security lights are useful additions to lighting apparatus.	Is lighting (internal and external) adequate to record high quality CCTV coverage as well as lit areas for entrances and exits, cargo handling and storage areas, fence lines and parking areas? ☒ Yes ☐ No If NO, explain why:	
9.6 Electronic Security Technology Security technology should be utilized to monitor premises and prevent unauthorized access to sensitive areas.	Electronic security technology used to secure/monitor sensitive areas and access points includes: burglary alarm systems (perimeter and interior) –these are also known as Intrusion Detection Systems (IDS); access control devices; and video surveillance systems (VSS) - including Closed Circuit Television Cameras (CCTVs). A CCTV/VSS system could include components such as Analog Cameras (coax-based), Internet Protocol-based (IP) cameras (network-based), recording devices, and video management software.	Does the facility use Electronic Security Technology, including alarms, access control devices and video surveillance? ☒ Yes ☐ No If YES, provide details: Facility is using alarms, access control devices and Video Surveillance technology	

	Secure/sensitive areas, which would benefit from video surveillance, may include: cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yard and storage areas for Instruments of International Traffic (IIT), areas where IIT are inspected, and seal storage areas.		
9.7 Security Technology – Procedures *Companies who rely on security technology for physical security **must** have written policies and procedures governing:* *• use,* *• maintenance,* *• protection of this technology.* *At a minimum, these policies and procedures **must** assure:* *• That access to the locations where the technology is controlled or managed is limited to authorized personnel;* *• procedures that have been implemented to test/inspect the technology on a regular basis;* *• inspections include verifications that all of the equipment is working properly and that the equipment is positioned properly* *• That the results of the inspections and performance testing is documented;* *• if corrective actions are necessary, they are to be implemented as soon as possible and the corrective actions are documented;* *• the documented results of these inspections be maintained for a sufficient time for audit purposes.*	Security technology needs to be tested on a regular basis to ensure it is working properly. There are general guidelines to follow: • Test security systems after any service work and during and after major repairs, modifications, or additions to a building or facility. A system's component may have been compromised, either intentionally or unintentionally. • Test security systems after any major changes to phone or internet services. Anything that might affect the system's ability to communicate with the monitoring center should be double-checked. • Make sure video settings such as motion activated recording; motion detection alerts; images per second (IPS), and quality level, have been set up properly. • Make sure camera lenses (or domes that protect the cameras) are clean and lenses are focused. Visibility should not be limited by obstacles or bright lights. • Test to make sure security cameras are positioned correctly and remain in the proper position (cameras may have been deliberately or accidentally moved).	Does the facility have written procedures for use, testing and maintenance of Security Technology equipment (select all that apply)? ☒ Procedures provide for restricted access to the equipment ☒ Procedures provide for regular Inspection and testing of equipment ☒ Procedures provide for verification that the equipment is working properly and all are positioned properly ☒ Procedures provide for results of inspections and testing is documented ☒ Procedures provide for the results of inspections are retained for a sufficient time for audit purposed	

9.8 Third Party Central Monitoring IF THE COMPANY DOES NOT USE A 3RD PARTY MONITORING SERVICE, MOVE TO THE NEXT QUESTION *If a third party central monitoring station (off-site) is used, the company **must** have written procedures stating critical systems functionality and authentication protocols such as security code changes, adding removing authorized personnel, password revisions, and systems access or denials.* *Security technology policies and procedures **must** be reviewed and updated annually, or more frequently, as risk or circumstances dictate equipment is working properly, and if applicable, that the equipment is positioned correctly;*		Does the 3rd party have written procedures for use, testing and maintenance of Security Technology equipment (select all that apply)? □ Procedures provide for restricted access to the equipment □ Procedures provide for regular Inspection and testing of equipment □ Procedures provide for verification that the equipment is working properly and all are positioned properly □ Procedures provide for results of inspections and testing is documented □ Procedures provide for the results of inspections are retained for a sufficient time for audit purposed N/A – Facility is not using 3rd Party Monitoring services	
9.9 Third Party Security Technology Vendor Selection *Companies should use licensed/certified resources when considering the design and installation of security technology.*	Security technology is complex and evolves rapidly. Purchasing the wrong security technology can result in ineffective systems/equipment Seeking qualified guidance will help a company select the right technology options for their needs and budget.	If a company uses third party vendors to install Security Technology equipment, explain how they select the service provider: ___________________________ Facility checks the trade license, Profile, and their expertise in this field. Facility is using the licensed and certified resources while considering the design and software technology.___________________________	
9.10 Security Technology Access Control *All security technology infrastructure **must** be physically secured from unauthorized access.*	Security technology infrastructure includes computers, security software, electronic control panels, video surveillance or closed circuit television cameras, power and hard drive components for cameras, as well as recordings.	Explain how Security Technology equipment (CCTV, monitoring, alarm systems, etc) is protected from unauthorized access: Facility restricting the unauthorized entries by posting the security guards in all the sensitive areas. Confidential password	

		is allocated for each computer, and additionally facility has installed censors with the doors to restrict unauthorized entries.	
9.11 Security Technology power backup *Security technology systems should be configured with an alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power.*	A criminal trying to breach your security may attempt to disable the power to your security technology in order to circumnavigate it. Thus, it is important to have an alternative source of power for your security technology. An alternative power source may be an auxiliary power generation source or backup batteries. Backup power generators may also be used for other critical systems such as lighting.	Does the company utilize batter backup for all components of the Security Technology system (CCTV recording devices, alarms, etc.) ☒ Yes ☐ No If NO, explain why:	
9.12 CCTV and Alarms If camera systems are deployed, cameras should: • *monitor a facility's premises and sensitive areas to deter unauthorized access.* • *Alarms should be used to alert a company to unauthorized access into sensitive areas.* • *Cameras should be programmed to record at the highest picture quality setting reasonably available, and be set to record on a 24/7 basis* • *cameras should have an alarm/notification feature, which would signal a "failure to operate/record" condition.*	Sensitive areas, as appropriate, may include cargo handling and storage areas, shipping/receiving areas where import documents are kept, IT servers, yards and storage areas for Instruments of International Traffic (IIT), areas where IIT are inspected, and seal storage areas. Positioning cameras correctly is important to enable the cameras to record as much as possible of the physical "chain of custody" within the facility's control. Based on risk, key areas or processes may include cargo handling and storage; shipping/receiving; the cargo loading process; the sealing process; conveyance arrival/exit; IT servers; container inspections (security and agricultural); seal storage; and any other areas that pertain to securing international shipments. A failure of video surveillance systems could be the result of someone disabling the system in order to breach a supply chain without leaving video evidence of the crime. The failure to operate feature can result in an electronic notification sent to predesignated person(s) notifying them that the device requires immediate attention.	Does the company's CCTV and Alarms meet the following (check all that apply): ☒ Monitor premises & sensitive areas ☒ Alarms alert to unauthorized access into sensitive areas ☒ CCTV is programmed to record at highest quality setting and for 24/7 basis ☒ CCTV has alarm to indicate a "failure to operate" condition	
9.13 CCTV	If camera footage is only reviewed for cause (as part of an investigation	Does the company's CCTV meets the following (check all that apply):	

*If camera systems are deployed, cameras **must*** *• be positioned to cover key areas of facilities that pertain to the import/export process* *• periodic, random reviews of the camera footage **must** be conducted (by management, security, or other designated personnel) to verify that cargo security procedures are being properly followed in accordance with the law.* *• Results of the reviews **must** be summarized in writing to include any corrective actions taken.* *• The results **must** be maintained for a sufficient time for audit purposes.*	following a security breach etc.), the full benefit of having cameras is not being realized. Cameras are not only investigative tools. If used proactively, they may help prevent a security breach from occurring in the first place. Focus the random review of the footage on the physical chain of custody to ensure the shipment remained secure and all security protocols were followed. Some examples of processes that may be reviewed are the following: • Cargo handling activities; • Container inspections; • The loading process; • Sealing process; • Conveyance arrival/exit; and • Cargo departure, **Purpose of the review:** The review is intended to evaluate overall adherence and effectiveness of established security processes, identify gaps or perceived weaknesses, and prescribe corrective actions in support of improvement to security processes. Based on risk (previous incidents or an anonymous report on an employee failing to follow security protocols at the loading dock, etc.), the Member may target a review periodically. **Items to include in the written summary**: • The date of the review; • Date of the footage that was reviewed; • Which camera/area was the recording from; • Brief description of any findings; and • If warranted, corrective actions.	☒ CCTV covers key areas of import/export process ☒ Periodic random reviews by management to verify that cargo security procedures are properly followed ☒ Results of Periodic random reviews by management are documented and corrective action is taken ☒ Results of Periodic random reviews by management are retained for a sufficient time for audit purposes	

SECTION 10 - PHYSICAL ACCESS CONTROL

Physical Access Controls – 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.

Non-Compliance Raised (✓ if NC raised)

10.1 Procedures for ID badges and access control devises *CTPAT Members **must** have written procedures governing* *• how identification badges and access devices are granted, changed, and removed.* *• Where applicable, a personnel identification system **must** be in place for positive identification and access control purposes.* *• Access to sensitive areas **must** be restricted based on job description or assigned duties.* *• Removal of access devices **must** take place when the employees separate from the company.*	Access devices include employee identification badges, visitor and vendor temporary badges, biometric identification systems, proximity key cards, codes, and keys. When employees are separated from a company, the use of exit checklists help ensure that all access devices have been returned and/or deactivated. For smaller companies, where personnel know each other, no identification system is required. Generally, for a company with more than 50 employees, an identification system is required.	Do the written procedures govern the following (check all that apply)? ☒ ID Badges and Access Control Devices are granted, changed, and removed. ☒ ID system in place for positive ID for persons seeking access to the premises. ☒ Access to sensitive areas is restricted to a business need" basis. ☒ Removal of access devices occurs immediately when an employee separates from the company	
10.2 Visitors, vendors contractor Access *Visitors, vendors, and service providers **must:*** *• present photo identification upon arrival,* *• a log **must** be maintained that records the details of the visit.* *• All visitors should be escorted.* *• all visitors and service providers should be issued temporary identification.* *• If temporary identification is used, it **must** be visibly displayed at all times during the visit.*		Do observations and the written procedures govern the following (check all that apply)? ☐ Visitors, Vendors, Service Providers present ID at arrival **It was noted that there was procedure manual that visitors/vendors were positively identified upon arrival at the facility, but the auditor of this audit and his car driver were not identified.**	✓

The registration log *must* *include the following:* *• Date of the visit;* *• Visitor's name;* *• Verification of photo identification (type verified such as license or national ID card).* *Frequent, well known visitors such as regular vendors may forego the photo ID, but* ***must*** *still be logged in and out of the facility;* *• Time of arrival;* *• Company point of contact;* *• Time of departure.*		☒ Visitor Log is maintained with details of the visit ☒ Visitors should be escorted (not must) ☒ Visitors & service providers should be issued temporary IDs ☒ Temp ID is visibly displayed at all times ☒ Visitor Log includes Date of visit, Name of visitor, verification of visitor ID ☒ Frequent/known visitors are logged in and out to include time of arrival/departure, company contact	🟧
10.3 Drivers – Positive Identification *• 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 highway carrier company that employs the driver picking up the load.*	Drivers delivering or receiving cargo must be positively identified before cargo is received or released.	Do observations and review of post orders confirm the following (check all that apply)? ☒ Drivers are positively identified before cargo is accepted or released ☒ Drivers are required to show positive official/government proof of identification to the company employee (security guard, shipping supervisor, warehouse manager, etc.)	
10.4 Register/Log for Cargo pickup *• A cargo pickup log* ***must*** *be kept to register drivers and record the details of their*	A visitor log may be acceptable as a cargo log as long as the extra information in 13.4 is recorded in it.	Do observations and review of pickup / register log meet he following (check all that apply)?	

conveyances when picking up cargo. *• When drivers arrive to pick up cargo at a facility, a facility employee* ***must*** *register them in the cargo pickup log.* *• Upon departure, drivers* ***must*** *be logged out.* *• The cargo log* ***must*** *be kept secured, and drivers must not be allowed access to it.* *The cargo pickup log should have the following items recorded:* *• Driver's name;* *• Date and time of arrival;* *• Employer;* *• Truck number;* *• Trailer number;* *• Time of departure;* *• The seal number affixed to the shipment at the time of departure.*		☒ Pickup log is in place and used to register drivers and information about the conveyances. ☒ Company employee (e.g. supervisor, guard, lead person, etc.) is performing registration of drivers ☒ Logs show that drivers and cargo are logged out at the time of departure ☒ The log is kept in a secure area where access is restricted and drivers are not allowed to have access	
13.4 Carrier Advance Notification of Pickup Time *Prior to arrival, the carrier should notify the facility of the estimated time of arrival for* *• the scheduled pick up,* *• the name of the driver* *• truck number.* *Where operationally feasible, CTPAT Members should allow deliveries and pickups by appointment only.*	This information will help shippers and carriers to avoid fictitious/false 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. 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.	Does the company receive advanced notice from the Carrier of expected arrival of drivers including (check all that apply): ☒ Scheduled pickup time. ☒ Name of the driver(s) ☒ Truck ID number ☒ Company keeps updated list of drivers with photos and driver license numbers.	
10.5 Screening of arriving packages and mail *Arriving packages and mail should be periodically screened*	Examples of such contraband include, but are not limited to, explosives, illegal drugs, and currency.	Does the company screen mail and packages (e.g. receiving personnel, receptionist, security guard inspection) for presence of contraband?	🟧

for contraband before being admitted.		☐ Yes ☒ No **It was noted during review of records and interaction with management that facility has not screened the arrived packages and emails for contraband before being admitted.**	✓
10.6 Security Guard Work Instructions (post orders) If security guards are used, work instructions for security guards **must** be contained in written policies and procedures. Management **must** periodically verify compliance and appropriateness with these procedures through audits and policy reviews.	Though guards may be employed at any facility, they are often employed at manufacturing sites, seaports, distribution centers, and storage yards for Instruments of International Traffic, consolidator, and forwarders operating sites. Normally, guards will have "post orders" that are written procedures and policies that they must follow to ensure adequate security measures are in place.	Are Security Guards in place in the facility? ☒ Yes ☐ No If YES: Do the guards have well understood written policies and procedures to follow to perform their duties? ☒ Yes ☐ No Through review of audit reports and records of policy review, how often does management perform internal audits and policy reviews to ensure appropriateness (check one)? ☐ Monthly ☐ Bi-Monthly ☒ Quarterly ☐ Semi-Annually ☐ Annually	

SECTION 11 - PERSONNEL SECURITY

Personnel Security –

A company’s human resource force is one of its most critical assets, but it may also be one of its weakest security links. The criteria in this category focus on issues such as employee screening and pre-employment verifications. Many security breaches are caused by internal conspiracies, which is where one or more employees collude to circumvent security procedures aimed at allowing an infiltration of the supply chain. Therefore, Companies must exercise due diligence to verify that employees filling sensitive positions are reliable and trustworthy. Sensitive positions include staff working directly with cargo or its documentation, as well as personnel involved in controlling access to sensitive areas or equipment. Such positions include, but are not limited to, shipping, receiving, mailroom personnel, drivers, dispatch, security guards, any individuals involved in load assignments, tracking of conveyances, and/or seal controls..

Non-Compliance Raised (✓ if NC raised)

11.1 Pre-Hiring Procedures *Written processes **must** be in place to screen prospective employees and to periodically check current employees.* *Application information, such as employment history and references, **must** be verified prior to employment, to the extent possible and allowed under the law.*	CTPAT is aware that labor and privacy laws in certain countries may not allow all of the application information to be verified. However, due diligence is expected to verify application information when permitted.	Does the company conduct pre-hiring and current checks on employees (check all that apply)? ☒ Written procedure is in place to screen job applicants ☒ Written procedures include ability to screen existing workers ☒ Company performs check of employment history and checks references of job applicants	
11.2 Pre-Hiring Procedures – Background Investigations *In accordance with applicable legal limitations, and the availability of criminal record databases, employee background screenings should be conducted.* *Based on the sensitivity of the position, employee background investigations should include temporary workforce and contractors.*	Employee background screening should include verification of the employee’s identity and criminal history, encompassing city, state, provincial, and country databases. CTPAT Members and their business partners should factor in the results of background checks, as permitted by local statutes, in making hiring decisions. Background checks are not limited to verification of identity and criminal records. In areas of greater risk, it may warrant more in-depth investigations.	Does the company conduct pre-hiring background investigations in accordance with legal limitations (check all that apply)? ☒ Company performs background investigations of all new workers. ☒ Company performs background investigations of all existing workers for cause ☐ Background investigations are not allowed under local law.	

Once employed, periodic reinvestigations should be performed based on cause, and/or the sensitivity of the employee's position.			
11.3 Employee Code of Conduct – Acceptable Behavior *Companies* ***must*** *have an Employee Code of Conduct that includes expectations and defines acceptable behaviors.* *Penalties and disciplinary procedures* ***must*** *be included in the Code of Conduct.* *Employees/contractors* ***must*** *acknowledge that they have read and understood the Code of Conduct by signing it, and this acknowledgement must be kept in the employee's file for documentation.*	A Code of Conduct helps protect a company and informs employees of expectations. Its purpose is to develop and maintain a standard of conduct that is acceptable to the company. It helps companies develop a professional image and establish a strong ethical culture. Even a small company needs to have a Code of Conduct; however, it does not need to be elaborate in design or contain complex information.	Does the company have a code of conduct that: (check all that apply)? ☒ Includes expectations and defines acceptable behavior of employees and contractors. ☒ Includes penalties and disciplinary procedures for unacceptable behavior for employees and contractors. ☒ Employees and contractors sign acknowledgements of their understanding of the Code of Conduct and are kept in the workers' files	

SECTION 12 - EDUCATION, TRAINING AND AWARENESS

Education, Training and Awareness –
CTPAT's security criteria are designed to form the basis of a layered security system. If one layer of security is overcome, another layer should prevent a security breach, or alert a company to a breach. Implementing and maintaining a layered security program needs the active participation and support of several departments and various personnel.
One of the key aspects to maintaining a security program is training. Educating employees on what the threats are and how their role is important in protecting the company's supply chain is a significant aspect to the success and endurance of a supply chain security program. Moreover, when employees understand why security procedures are in place, they are much more likely to adhere to them.

Non-Compliance Raised (✓ if NC raised)

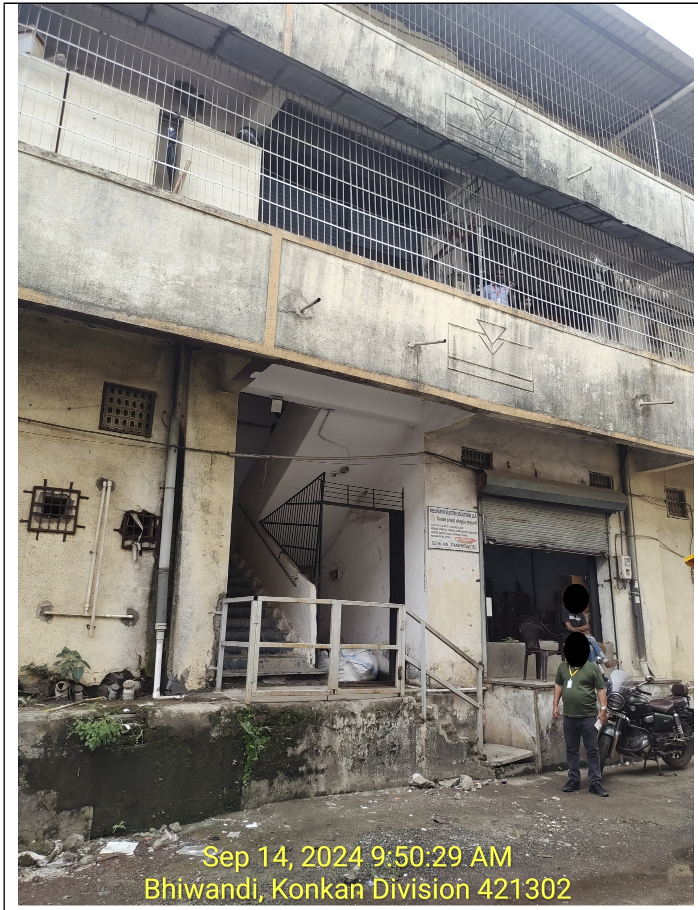
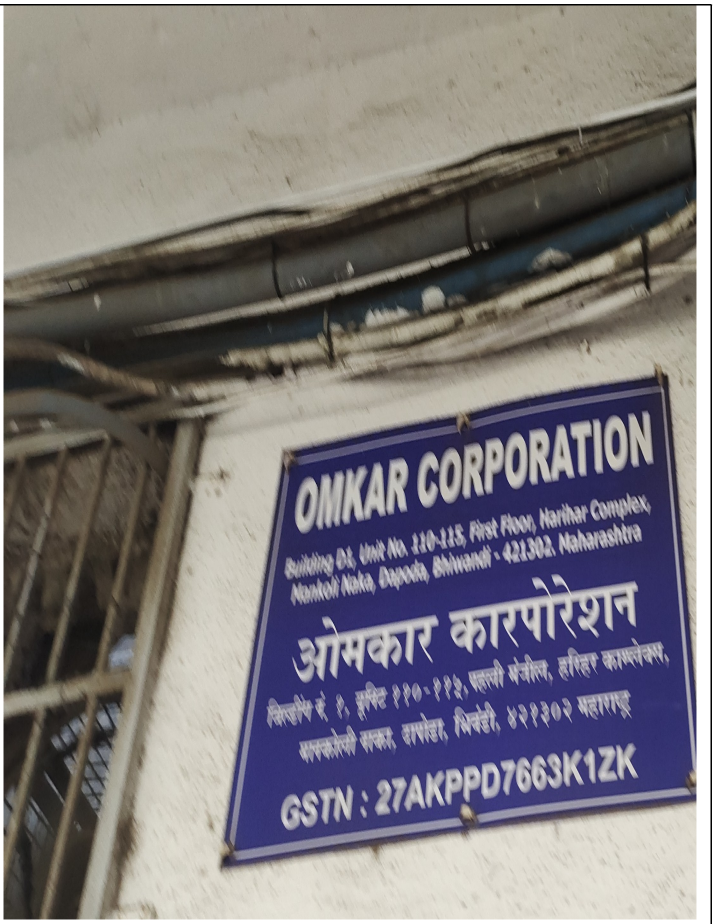
12.1 Security Training and Awareness Program *Companies **must** establish and maintain a security training and awareness program that includes awareness of security vulnerabilities of:* *• facilities,* *• conveyances,* *• cargo* *at each point in the supply chain, which could be exploited by terrorists or contraband smugglers.* *The training program **must** be comprehensive and cover all of CTPAT's security requirements and be provided to newly hired workers as well as on a regular basis for all workers.* *Personnel in sensitive positions **must** receive additional specialized training geared toward the responsibilities that the position holds.*	One of the key aspects of a security program is training. Employees who understand why security measures are in place are more likely to adhere to them. Security training must be provided to employees, as required, based on their functions and position on a regular basis, and newly hired employees must receive this training as part of their orientation/job skills training. Members must retain evidence of training such as training logs, sign-in sheets (roster), or electronic training records. Training records should include the date of the training, names of attendees, and the topics of the training.	Does the company conduct awareness training (check all that apply)? ☒ A documented (PowerPoint, video, classroom lecture, etc.) awareness training is in place covering ALL CTPAT security requirements. ☒ Newly hired workers are provided with awareness training in CTPAT at the time of hire. ☒ Company conducts regular (at least annually) awareness training with all workers.	

12.2 Security Training for drivers and inspectors *Drivers and other personnel that conduct security and agricultural inspections of empty conveyances and Instruments of International Traffic (IIT)* **must** *be trained to inspect their conveyances/IIT for both security and agricultural purposes.* *Refresher training* **must** *be conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures.* *Inspection training* **must** *include the following:* *• Signs of hidden compartments* *• Concealed contraband in naturally occurring compartments* *• Signs of pest contamination.*		Does the company conduct specific training for inspection of empty containers (IIT) (check all that apply)? ☒ A documented (PowerPoint, video, classroom lecture, etc.) awareness training program exists for BOTH security and Agricultural (if appropriate) purposes for inspection personnel. ☒ Company conducts regular (at least annually) awareness training with all workers. ☒ Training includes: • Signs of hidden compartments • Concealed contraband in naturally occurring compartments • Signs of pest contamination	
12.3 Measuring Effectiveness of Training *Companies should have measures in place to verify that the training provided met all training objectives.*	Understanding the training and being able to use that training in one's position (for sensitive employees) is important. Exams or quizzes, a simulation exercise/drill, or regular audits of procedures etc. are some of the measures that the company may implement to determine the effectiveness of the training.	Company measures effectiveness of training workers by way of (check all that apply): □ exams, quizzes, □ simulation exercise or drills ☒ regular audits of procedures	
12.4 Training – Cybersecurity Policies & Procedures *As applicable, based on their functions and/or positions, personnel* **must** *be trained on the company's cybersecurity policies and procedures.* *This training* **must** *include the need for employees to protect passwords/passphrases and computer access.*	Quality training programs are important to lessen vulnerability to cyberattacks. A robust (strong) cybersecurity training program is usually one that is delivered to applicable personnel in a formal setting rather than simply through emails or memos.	Does the company conduct specific training for appropriate persons relative to: (check all that apply)? ☒ A Cybersecurity Policies and Procedures training program related is in place and delivered to workers in a formal setting ☒ Cybersecurity Training covers the need for employees to protect passwords/passphrases and computer access.	

12.5 Training – Operators and managers of security technology systems *Personnel responsible to operating and manage security technology systems* ***must*** *receive operations and maintenance training in their specific areas.*	Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable.	Does the company conduct specific training for appropriate persons relative to: (check all that apply)? ☒ A Cybersecurity Policies and Procedures training program related is in place and delivered to workers in a formal setting	
12.6 Training – Reporting Security Incidents *Personnel* ***must*** *be trained on how to report security incidents and suspicious activities.*		Does the company training include the procedures for how personnel must report security incidents and suspicious activities? ☒ Yes ☐ No	

Factory Name	OMKAR CORPORATION	Date	14th September 2024
Audit Type	CTPAT Audit (2020 MSC)	Page	1

Compliance Photos:

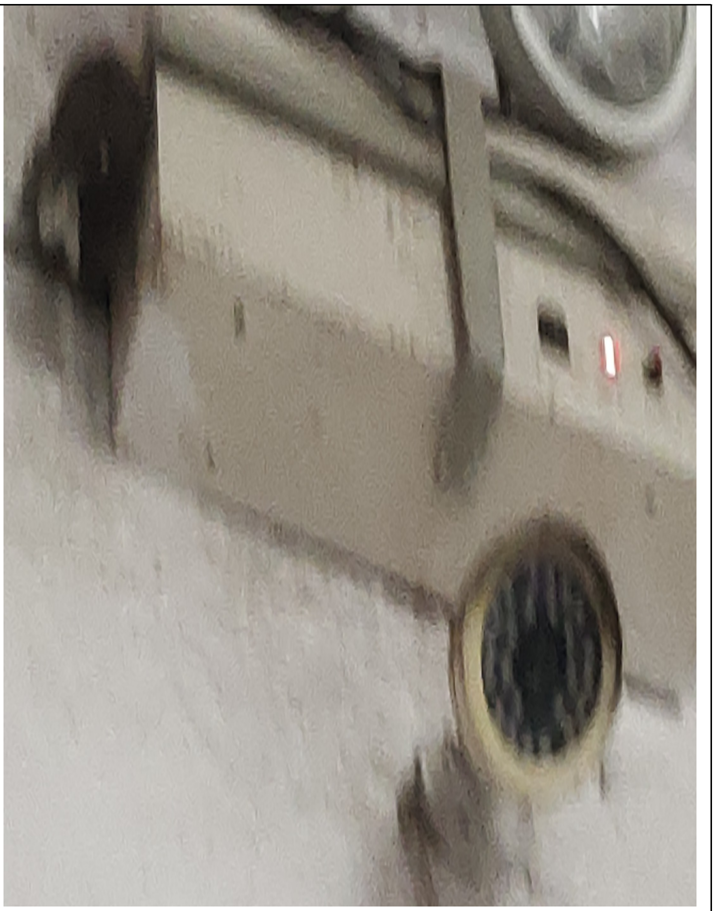
	 OMKAR CORPORATION Building 01, Unit No. 110-115, First Floor, Harihar Complex, Mankoli Naka, Dapoda, Bhiwandi - 421302, Maharashtra ओमकार कारपोरेशन GSTN : 27AKPPD7663K1ZK
Building Exterior View	**Facility name board**

Factory Name	OMKAR CORPORATION	Date	14th September 2024
Audit Type	CTPAT Audit (2020 MSC)	Page	2

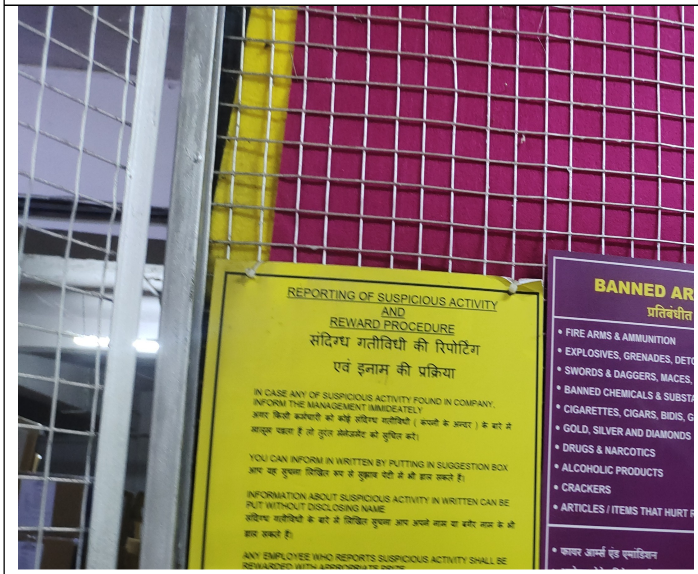
सावधान
पान.तम्बाखु व गुटखा वर्जित है
NO SMOKING
धुम्रपान करना व गुटखा खाना सकत मना है
Sep 14, 2024 9:51:54 AM
Bhiwandi, Konkan Division 421302

[redacted] [redacted] [redacted]

Security post /Gate House area



CCTV position in/out of gate and CTPAT areas



REPORTING OF SUSPICIOUS ACTIVITY AND REWARD PROCEDURE

संदिग्ध गतीविधी की रिपोर्टिंग एवं इनाम की प्रक्रिया

IN CASE ANY OF SUSPICIOUS ACTIVITY FOUND IN COMPANY, INFORM THE MANAGEMENT IMMIDEATELY
अगर किसी कर्मचारी को कोई संदिग्ध गतीविधी (कंपनी के अन्दर) के बारे में मालूम पड़ता है तो तुरंत मेनेजमेंट को सुचित करें।

YOU CAN INFORM IN WRITTEN BY PUTTING IN SUGGESTION BOX
आप यह सुचना लिखित रूप से सुझाव पेटी में भी डाल सकते हैं।

INFORMATION ABOUT SUSPICIOUS ACTIVITY IN WRITTEN CAN BE PUT WITHOUT DISCLOSING NAME
संदिग्ध गतीविधी के बारे में लिखित सुचना आप अपने नाम या बगैर नाम के भी डाल सकते हैं।

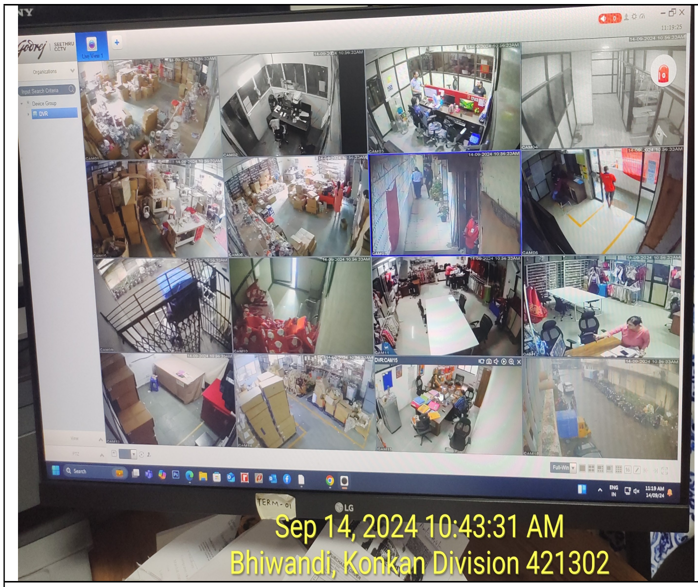
ANY EMPLOYEE WHO REPORTS SUSPICIOUS ACTIVITY SHALL BE REWARDED WITH APPROPRIATE PRIZE

BANNED AR
प्रतिबंधीत

- FIRE ARMS & AMMUNITION
- EXPLOSIVES, GRENADES, DETO
- SWORDS & DAGGERS, MACES,
- BANNED CHEMICALS & SUBSTA
- CIGARETTES, CIGARS, BIDIS, G
- GOLD, SILVER AND DIAMONDS
- DRUGS & NARCOTICS
- ALCOHOLIC PRODUCTS
- CRACKERS
- ARTICLES / ITEMS THAT HURT R
- फायर आर्म्स एंड एम्मोडिशन

Banned article policies

Biometric machine



Server Room

Loading unloading area

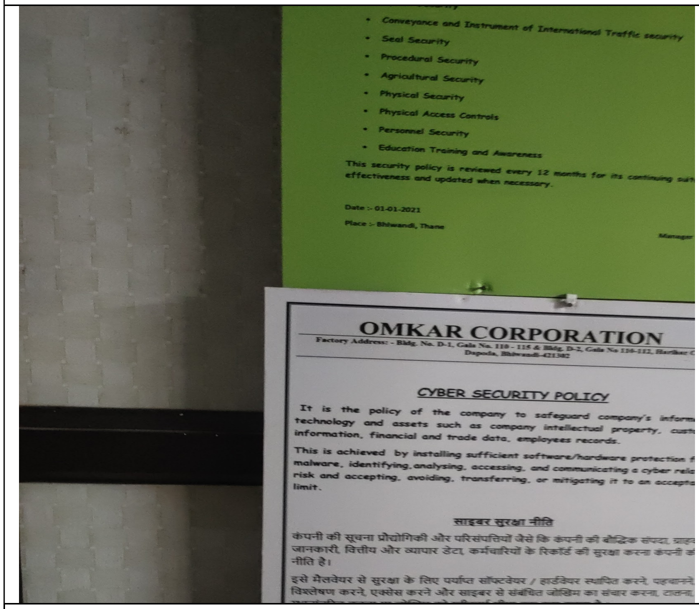
7/8 Point Inspection

Finished Goods Packing Area

NO PERSONAL BELONGINGS ALLOWED IN THE AREA
इस क्षेत्र में कोई निजी सामान की अनुमति नहीं हैं
Omkar Corporation
Authorised Persons Packing Area

Access control (stores, packing, loading-unloading)

17712 ISO Standard Seal



- Conveyance and Instrument of International Traffic security
- Seal Security
- Procedural Security
- Agricultural Security
- Physical Security
- Physical Access Controls
- Personnel Security
- Education Training and Awareness

This security policy is reviewed every 12 months for its continuing suit effectiveness and updated when necessary.

Date :- 01-01-2021

Place :- Bhiwandi, Thane

Manager

OMKAR CORPORATION

Factory Address: - Bldg. No. D-1, Gala No. 110 - 115 & Bldg. D-2, Gala No 110-112, Harihar C
Dapoda, Bhiwandi-421302

CYBER SECURITY POLICY

It is the policy of the company to safeguard company's inform technology and assets such as company intellectual property, cust information, financial and trade data, employees records.

This is achieved by installing sufficient software/hardware protection f malware, identifying, analysing, accessing, and communicating a cyber rela risk and accepting, avoiding, transferring, or mitigating it to an accepta limit.

साइबर सुरक्षा नीति

कंपनी की सूचना प्रौद्योगिकी और परिसंपत्तियों जैसे कि कंपनी की बौद्धिक संपदा, ग्राहक जानकारी, वित्तीय और व्यापार डेटा, कर्मचारियों के रिकॉर्ड की सुरक्षा करना कंपनी की नीति है।

इसे मैलवेयर से सुरक्षा के लिए पर्याप्त सॉफ्टवेयर / हार्डवेयर स्थापित करने, पहचानने, विश्लेषण करने, एक्सेस करने और साइबर से संबंधित जोखिम का संचार करना, टालना,

CTPAT Policies

Stitching

	Sep 14, 2024 10:03:28 AM Bhiwandi, Konkan Division 421302
Checking	Packing