Audit Date:	
Audit Type:	

XYZ Facility
SECURITY ASSESSMENT

One best practice picture of the audited facility

Disclaimer:
©2020 SGS SA Disclaimer. This report is strictly confidential. Any holder of this document is advised that information contained herein reflects the Company's findings at the time of its intervention only and within the limits of the Client's instructions, if any. The Company's sole responsibility is to its Client and this document does not exonerate parties to a transaction from exercising all their rights and obligations under the transaction documents. This document cannot be reproduced except in full, without prior written approval of the Company. Any unauthorised alteration, forgery or falsification of the content or appearance of this document is unlawful and offenders may be prosecuted to the fullest extent of the law.

SGS conducts all audits according to the highest professional standards, based on ISO 17021. However, it must be advised that each audit is based on a sampling approach. Therefore, there may be issues that have not been discovered or identified during the course of the audit. It is the responsibility of the auditee to identify those issues through its own monitoring processes.

This document is subject to SGS General Conditions for Customized audit services available at: http://www.sgs.com/terms_and_conditions.htm

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

AUDIT SUMMARY

SITE PROFILE

Basic Information

Supplier Name				
Facility Address				
City				
State / Province				
Country				
Postal Code				
Supplier's Telephone No.				
Supplier's Fax No.				
Supplier's E-mail Address				
Supplier's Web-site				
C-TPAT Member		YES		NO
Business Partner to C-TPAT member		YES		NO
Month/Year Started Operations				
Other Location 1				
Other Location 2				
Other Location 3				

Supplier Contacts

President		Email:
Plant Manager		Email:
Quality Manager		Email:
Safety Representative		Email:
HR Manager		Email:
Housing Manager		Email:
Security Manager		Email:
Other - *Type Title here.*		
Other - *Type Title here.*		

Background Information

Product / Service Category(s)	
Operation Process(es)	
Annual Sales (USD)	
Capacity/Year (Units)	
Main Language of Employees	
Language of Management	
Business Nature	

Plant Size

Total Facility		Square Feet
Production Floors		Square Feet

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

Warehouse Areas	Square Feet
Distribution Areas	Square Feet
Canteen & Dormitory Areas	Square Feet
Total Number of Buildings	
Total Number of Warehouses	
Total Number of Gates (Facility access points)	
Total Number of Gate Houses	

Use of Subcontractor

Name of Subcontractor	**Service Type**	**Address**
(i.e. Logistic service providers)	(i.e. Logistic service providers)	
(i.e. External warehouse for storage)	(i.e. External warehouse for storage)	
Other - Additional Subcontractors		
Other - Additional Subcontractors		

Shipment Methods to USA or other countries

By air	%	
By sea	%	
By truck	%	
By rail	%	
Other carrier type		

### Total Employees	On the date of the audit			
No. of Office Staffs	M		F	
No. of Regular Staffs	M		F	
No. of Contractual Staffs	M		F	
No. of Temporary Staffs	M		F	
Others	M		F	
Total no. of employees	M		F	

No. of Staff Recruited (last 12 months)	
No. of Staff Left (last 12 months)	
Average No. of Staff Total (last 12 months)	
Staff Turnover Rate (last 12 months)	%

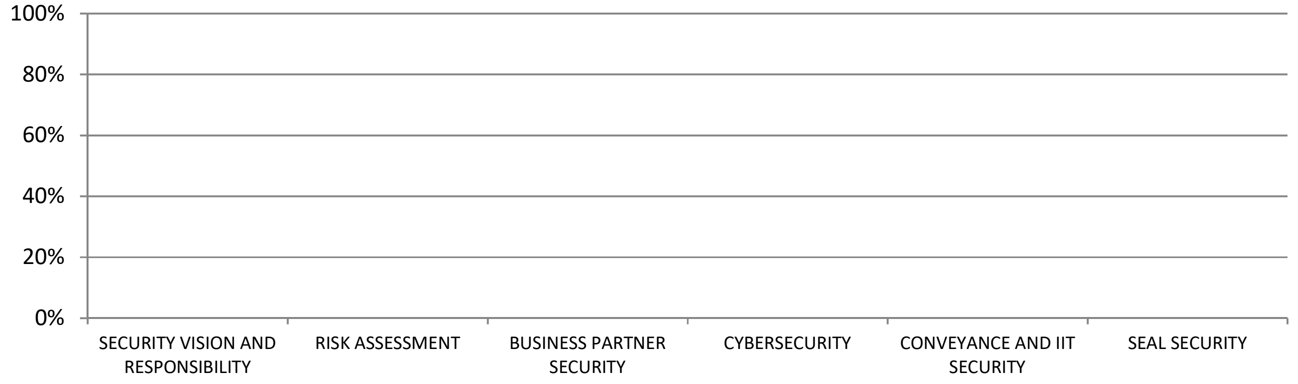
Auditor Name:	
Technical Reviewer Name:	

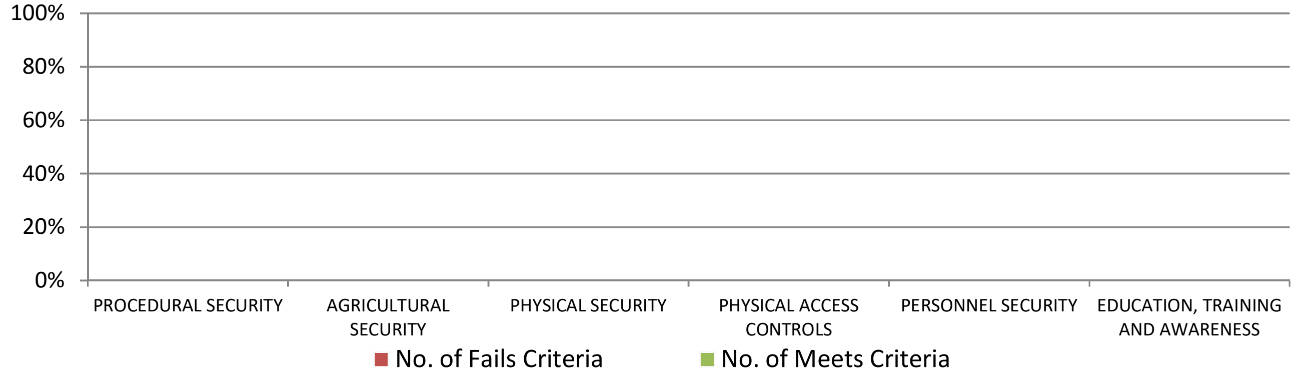
©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

PERFORMANCE SUMMARY

		No. of Critical Violations	No. of Fails Criteria	No. of Meets Criteria	Section Score	Section Score (%)
1.0	SECURITY VISION AND RESPONSIBILITY	0	0	0	#N/A	#N/A
2.0	RISK ASSESSMENT	0	0	0	#N/A	#N/A
3.0	BUSINESS PARTNER SECURITY	0	0	0	#N/A	#N/A
4.0	CYBERSECURITY	0	0	0	#N/A	#N/A
5.0	CONVEYANCE AND IIT SECURITY	0	0	0	#N/A	#N/A
6.0	SEAL SECURITY	0	0	0	#N/A	#N/A
7.0	PROCEDURAL SECURITY	0	0	0	#N/A	#N/A
8.0	AGRICULTURAL SECURITY	0	0	0	#N/A	#N/A
9.0	PHYSICAL SECURITY	0	0	0	#N/A	#N/A
10.0	PHYSICAL ACCESS CONTROLS	0	0	0	#N/A	#N/A
11.0	PERSONNEL SECURITY	0	0	0	#N/A	#N/A
12.0	EDUCATION, TRAINING AND AWARENESS	0	0	0	#N/A	#N/A

CRITICAL VIOLATIONS		FINAL RESULT		OVERALL SCORE
0	→	**#N/A**	←	**#N/A**





©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

ACTIONS REQUIRED SUMMARY

Actions Required (Findings of MUST Criteria)	Section Number

ACTIONS RECOMMENDED SUMMARY

Actions Recommended (Findings of SHOULD Criteria)	Section Number

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 1.0 SECURITY VISION AND RESPONSIBILITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
1.1	Does the company have documented procedures for reviewing their supply chain security program?		MUST	#N/A	
1.1.1	If yes, does this process include participation of different stakeholders within the company outside of security?		Should	#N/A	
1.2	Is the company's point of contact (POC) on C-TPAT knowledgeable about the C-TPAT program requirements and security practices?		MUST	#N/A	
1.3	Does the company have a written policy on its commitment to supply chain security?		Should	#N/A	
1.3.1	If yes, is the policy signed by a senior company official and reviewed annually?		Should	#N/A	
1.3.2	If yes, is that policy displayed in key locations?		Should	#N/A	

Section 1.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 2.0 RISK ASSESSMENT

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
2.1	For facilities within the company's control: Do they conduct a self-assessment of security practices, procedures and policies according to risk?		MUST	#N/A	
2.2	For facilities NOT within the company's control: Do they conduct a security-based risk assessments of their business partners and other facilities in their supply chain?		MUST	#N/A	
2.2.1	If yes, does this assessment include consideration of relevant factors to supply chain security, such as volume, country of origin, routing, terrorist threat, etc.?		Should	#N/A	
2.2.2	If yes, does the company maintain a list of all business partners by name, type of service provided, role in the supply chain, address of physical office location, contact information (e.g. telephone numbers, fax numbers, email), and contact name?		Should	#N/A	
2.2.3	If yes, does this assessment include a mapping of the movement of cargo throughout the company's supply chain, including locations where cargo is "at rest" for an extended period of time?		Should	#N/A	
2.3	Is the security risk assessment reviewed or updated at least annually?		MUST	#N/A	
2.4	Does the company have procedures that address crisis management, business continuity, security recovery plans and business resumption?		Should	#N/A	

Section 2.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 3.0 BUSINESS PARTNER SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
3.1	Does the company have a risk-based process for the **selection** of all business partners?		MUST	#N/A	
3.1.1	If yes, do contracts with business partners address compliance with C-TPAT's minimum security criteria?		MUST	#N/A	
3.1.2	[Canada and Mexico] If yes, does the company only use C-TPAT certified highway carriers or ensure that the actual entity carrying the cargo across a U.S. land border meets C-TPAT's minimum security criteria?		MUST	#N/A	
3.2	Does the company have a risk-based process for the **monitoring** of all business partners?		MUST	#N/A	
3.2.1	If yes, does the company require business partners to complete a security questionnaire or provide evidence that their security practices meet C-TPAT's minimum security criteria?		MUST	#N/A	
3.2.2	If yes, does this include timely correction of deficiencies in their business partners' security practices?		MUST	#N/A	
3.2.3	If yes, is the security assessment of the company's business partners updated on a regular basis?		Should	#N/A	
3.2.4	If yes, does the company provide guidance or training to its business partners regarding C-TPAT's security requirements?		Should	#N/A	
3.3	Does the company have a social compliance program that prohibits the use of forced, imprisoned, indentured, or indentured child labor in the production of its products?		Should	#N/A	

Section 3.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 4.0 CYBERSECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
4.1	Does the company have comprehensive written policies or procedures covering IT protection and cybersecurity?		MUST	#N/A	
4.1.1	If yes, are the policies and procedures reviewed, updated and endorsed by management at least once a year?		MUST	#N/A	
4.1.2	If yes, do the procedures clearly state what is considered abuse of its IT systems?		MUST	#N/A	
4.1.3	If yes, does the company have a clear process for disciplining violators of these procedures?		MUST	#N/A	
4.1.4	If yes, does the company have processes to identify, prevent and address the loss of data in the event of attacks via social engineering (such as phishing)?		MUST	#N/A	
4.1.5	If yes, does the company only allow remote access to its IT systems through secure technologies, such as virtual private networks (VPNs)?		MUST	#N/A	
4.1.6	If yes, do all employee personal devices used for company business adhere to the company's cybersecurity policies and procedures?		MUST	#N/A	
4.1.7	If yes, does the company utilize an effective employee ID system to control access only to IT systems necessary for the performance of their duties?		MUST	#N/A	
4.1.8	If yes, are employees assigned individual accounts that require a periodic change of password?		MUST	#N/A	
4.1.9	If yes, does the company's IT systems include automatic time-outs of users and the disabling of accounts after a number of failed log-in attempts?		Should	#N/A	
4.1.10	If yes, does the company have a policy to share cybersecurity threats with governments and business partners?		Should	#N/A	
4.2	Does the company use software to conduct business or manage data?		MUST	#N/A	
4.2.1	If yes, is the software capable of identifying and preventing unauthorized access?		MUST	#N/A	
4.2.2	If yes, does the company have sufficient software solutions to protect their IT systems from malware (viruses, spyware, worms, Trojans, etc.) and external intrusions?		MUST	#N/A	
4.2.3	If yes, does the company's software receive automatic security updates?		MUST	#N/A	
4.2.4	If yes, does the company prevent the use of counterfeit or improperly licensed technology or software?		Should	#N/A	
4.2.5	If yes, are all sensitive and confidential data stored in an encrypted format and backed up at least once a week?		Should	#N/A	
4.3	Does the company conduct business using hardware or store data on physical electronic media?		MUST	#N/A	
4.3.1	If yes, does the company regularly test the security of their IT infrastructure and, if vulnerabilities are found, implement corrective actions promptly?		MUST	#N/A	
4.3.2	If yes, does the company ensure regular inventories are done for all media, hardware and/or other IT equipment and follow appropriate industry guidelines for media sanitization upon disposal?		MUST	#N/A	

Section 4.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 5.0 CONVEYANCE AND INSTRUMENTS OF INTERNATIONAL TRAFFIC (IIT) SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
5.1	Does the company have written procedures covering both security and agricultural inspections of containers, cargo handling and storage areas?		MUST	#N/A	
5.1.1	If yes, does this include appropriate seven- or eight-point inspections of all empty containers, unit load devices (ULDs), and other IIT, both refrigerated and unrefrigerated?		MUST	#N/A	
5.1.2	If yes, does this include inspection of all external hardware to ensure that it can withstand attempts to remove it and detect any tampering?		MUST	#N/A	
5.1.3	If yes, are there procedures for the cleaning of containers or areas found to have pest contamination?		MUST	#N/A	
5.1.4	If yes, are all the points of the inspection documented on a checklist and included in the shipping documentation sent to the recipient?		Should	#N/A	
5.1.5	If yes, are these inspections done in a secured area and, if available, monitored via CCTV?		Should	#N/A	
5.2	Is the integrity of containers and other IIT maintained during loading/stuffing/packing using clearly written procedures?		Should	#N/A	
5.3	Are random searches conducted by management on containers and other IIT post-inspection?		Should	#N/A	
5.4	Does the company have secure areas where they handle their cargo?		MUST	#N/A	
5.4.1	If yes, does this include a secure storage area for empty and full containers and other IIT to prevent unauthorized access?		MUST	#N/A	
5.4.2	If yes, are loading docks for trucks and pick-ups/deliveries separate from all other vehicles and traffic?		Should	#N/A	
5.4.3	If yes, is there a secured area for truck and pick-up/delivery drivers to wait while cargo is loaded and unloaded?		Should	#N/A	
5.5	Does the company have written procedures for reporting incidents, such as thefts, tampering and unmanifested items, to affected business partners and law enforcement agencies?		MUST	#N/A	
5.6	Are there procedures to track the movement of all cargo during transit via their transportation providers?		Should	#N/A	
5.7	Does the company have access to their transportation providers GPS monitoring system so that they can track their shipments?		Should	#N/A	
5.8	[Canada and Mexico] Does the company have a “no-stop” policy with regards to unscheduled stops for shipments if they are in proximity to a U.S. land border?		Should	#N/A	
5.9	[Canada and Mexico] Does the company conduct final inspections verifying seal and container integrity before crossing a U.S. border in high risk areas?		Should	#N/A	

Section 5.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 6.0 SEAL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
6.1	Does the company have written procedures to control, record and affix ISO 17712 compliant seals on all containers and IIT?		MUST	#N/A	
6.1.1	If yes, are these procedures maintained and accessible at the local, operating level?		MUST	#N/A	
6.1.2	If yes, are these procedures reviewed and updated at least once a year?		MUST	#N/A	
6.1.3	If yes, do they document that all seals meet or exceed the current ISO 17712 standard?		MUST	#N/A	
6.1.4	If yes, are all containers and IIT secured with a ISO 17712 compliant seal immediately after loading/stuffing/packing?		MUST	#N/A	
6.1.5	If yes, are all seals verified using the VVTT process?		MUST	#N/A	
6.2	Are periodic audits of seals conducted that include an inventory of stored seals, reconciliation against seal documentation, and the periodic verification of seal numbers on containers or IIT?		MUST	#N/A	

Section 6.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 7.0 PROCEDURAL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
7.1	If cargo is held at the facility for an extended period of time, such as overnight, is it stored in a secure area?		MUST	#N/A	
7.2	Does the company ensure that cargo staging and storage areas are regularly inspected for pest contamination?		MUST	#N/A	
7.3	Does the company keep international cargo separate from domestic cargo?		Should	#N/A	
7.4	Does the company keep hazardous or dangerous cargo separate from other cargo?		Should	#N/A	
7.5	Does the facility have a designated employee, preferably a security officer, to supervise the loading/stuffing/packing of cargo into containers and IIT?		Should	#N/A	
7.6	Does the company require digital images to be taken of the properly installed seals during loading/stuffing/packing to be compared with the images taken at the destination?		Should	#N/A	
7.7	Are all cargo properly marked, counted, weighed, documented and reported on the manifests and bills of lading (BOL)?		MUST	#N/A	
7.8	Is all information used in the clearing of cargo legible, complete, accurate, protected against exchange, loss, or the introduction of erroneous information and reported on time?		MUST	#N/A	
7.9	Does the company have procedures to verify both arriving and departing cargo against manifests, purchase orders, or other shipment documentation?		MUST	#N/A	
7.9.1	If yes, do these procedures cover the process for resolving any cargo discrepancies (shortages, overages, etc.) found?		MUST	#N/A	
7.10	Are seal numbers electronically printed on the BOL or other shipping documents and transmitted to the receiver of the delivery prior to departure?		Should	#N/A	
7.11	If paper documents are used for recording cargo or shipment information, are these documents properly secured?		Should	#N/A	
7.12	Does the company have written procedures for challenging unauthorized or unidentified persons attempting to gain access to the facility?		MUST	#N/A	
7.13	Are all cargo and shipping documentation reviewed by personnel appropriately training on how to identify suspicious cargo shipments?		MUST	#N/A	
7.14	Does the company have procedures for a prompt internal investigation of any security-related incident, which is made available to CBP or other law enforcement agencies upon request?		MUST	#N/A	
7.15	Does the company have written procedures for reporting security incidents to relevant customs or law enforcement agencies, depending on the severity of incident?		MUST	#N/A	
7.15.1	If yes, does the company have documented procedures for anonymously reporting security incidents to relevant parties?		Should	#N/A	
7.15.2	If yes, is there an incentive scheme which encourages staff to report security incidents?		Should	#N/A	

Section 7.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 8.0 AGRICULTURAL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
8.1	Does the company have written procedures to prevent pest contamination from wood packaging materials (WPM) (see the IPPC's International Standards for Phytosanitary Measures No. 15)?		MUST	#N/A	
8.1.1	If yes, do all wood packaging aterials (WPM) used at the facility bear a mark (conforming to Annex 2 of ISPM 15) indicating that the WPM has been subjected to approved phytosanitary treatment?		MUST	#N/A	
8.1.2	If yes, do these procedures instruct personnel how to manage reused, repaired or remanufactured WPM so that they meet all treatment and marking standards (according to ISPM 15)?		MUST	#N/A	
8.1.3	If yes, do these procedures instruct personnel how to manage and securely dispose of pest contaminated or otherwise non-compliant WPM according to the requirements of ISPM 15 and/or the country's National Plant Protection Organization (NPPO)?		MUST	#N/A	

Section 8.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 9.0 PHYSICAL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
9.1	Are facilities designed and constructed with materials appropriate to prevent unauthorized access?		MUST	#N/A	
9.2	Does the facility have perimeter fencing or walls on all sides of a height of 6 ft (1.8 m) and, where appropriate, interior fencing or walls to segregate cargo such as domestic, international, high value, and/or hazardous materials?		Should	#N/A	
9.3	Does the facility have functional locking devices for all internal and external doors, windows, gates and fences, where appropriate to prevent unauthorized access?		MUST	#N/A	
9.4	Does the facility have written procedures to control the issuance of keys, and are keys recovered and/or locks changed when employees who have them change positions within or leave the company?		Should	#N/A	
9.5	Does the facility have internal and external lighting in all required areas (e.g. entrances and exits, cargo handling and storage areas, the factory perimeter, parking areas, etc.)?		MUST	#N/A	
9.6	Does the facility monitor all external access points either using manned positions or technology?		MUST	#N/A	
9.7	Is parking at the facility authorized using a decal system or using passes issued from a security gate?		Should	#N/A	
9.8	Is parking for private vehicles (employees, visitors, vendors, contractors, etc.) clearly separated from cargo staging areas and loading docks?		Should	#N/A	
9.9	Does the facility have documented policies for the use, maintenance and protection of security technology (e.g. building, fencing, gates, lights, alarm system and CCTV) including regular inspections?		MUST	#N/A	
9.10	Is access to all security technology infrastructure physically restricted?		MUST	#N/A	
9.11	Are security technologies used to prevent unauthorized access to sensitive areas?		Should	#N/A	
9.12	Does the facility have a security alarm system, which is appropriately managed when employees leave the company?		Should	#N/A	
9.13	Does the company only use licensed or certified resources when designing or installing security technology?		Should	#N/A	
9.14	In event of power loss, are all critical security technology systems connected to alternate power sources?		Should	#N/A	
9.15	Are cameras systems (e.g. CCTV) used?		Should	#N/A	
9.15.1	If yes, are these camera systems used to monitor the facility's premises including the key areas related to cargo and container security?		MUST	#N/A	
9.15.2	If yes, are these camera systems set to record on a 24 hour, 7 days a week basis and at the highest picture quality setting reasonably available?		MUST	#N/A	
9.15.3	If yes, are periodic reviews of the camera footage conducted by relevant personnel and documented in writing including any corrective actions that were taken?		MUST	#N/A	
9.15.4	If yes, do these camera systems have an alarm or other notification feature that signals when the camera is not operating properly or not recording?		Should	#N/A	
9.15.5	If yes, is camera footage of all key import and export processes maintained for a sufficient amount of time to allow for investigations of monitored shipments?		Should	#N/A	

Section 9.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

SECTION 10.0 PHYSICAL ACCESS CONTROLS

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
10.1	Does the company have a documented procedure defining access controls for employees and drivers?		MUST	#N/A	
10.1.1	If yes, are all employees required to present identification upon entering the facility?		MUST	#N/A	
10.1.2	If yes, are drivers required to present photo identification prior to cargo being received or released to/from their custody?		MUST	#N/A	
10.1.3	If yes, does the company maintain a cargo pickup log for all registered drivers?		MUST	#N/A	
10.1.4	If yes, are deliveries and pickups allowed by appointment only?		Should	#N/A	
10.1.5	If yes, do carriers notify the company before drivers arrive at the facility with relevant details of the pickup?		Should	#N/A	
10.1.6	If yes, is pickup and delivery of cargo limited only to monitored areas of the facility?		Should	#N/A	
10.1.7	If yes, are arriving packages and mail periodically screened for dangerous materials or contraband before being admitted?		Should	#N/A	
10.2	Does the company have a documented procedure defining access controls for visitors?		MUST	#N/A	
10.2.1	If yes, are all visitors required to present a valid photo ID for positive identification before being allowed access to the facility?		MUST	#N/A	
10.2.2	If yes, are all visitors issued temporary ID's?		MUST	#N/A	
10.2.3	If yes, does the company maintain a log of all visitors entering the facility?		MUST	#N/A	
10.2.4	If yes, are employee escorts required for all visitors while on the premises?		MUST	#N/A	
10.2.5	If yes, are visitors required to have an appointment prior to being granted admission to the facility?		Should	#N/A	
10.2.6	If yes, are all visitor's packages screened prior to being granted admission to the facility?		Should	#N/A	
10.3	Does the facility employ security guards?		Should	#N/A	
10.3.1	If yes, are there written work instructions for the security guards that management periodically checks for compliance and appropriateness?		MUST	#N/A	

Section 10.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 11.0 PERSONNEL SECURITY

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
11.1	Does the company verify the information on employment applications submitted from prospective employees prior to employment as permitted by law?		MUST	#N/A	
11.2	Does the company interview prospective employees as permitted by law?		MUST	#N/A	
11.3	Does the company perform background checks of prospective employees prior to employment as permitted by laws?		Should	#N/A	
11.4	Does the company conduct periodic background checks or screening on existing employees as permitted by law?		Should	#N/A	
11.5	Are employees required to sign a Code of Conduct?		MUST	#N/A	

Section 11.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

SECTION 12.0 EDUCATION, TRAINING AND AWARENESS

	Security Measures	Compliance Level	Criteria Type	Auditor Remarks	Comments on N/A & Others
12.1	Does the company provide security and agricultural training to new employees that is appropriate to their position and job responsibilities?		MUST	#N/A	
12.1.1	If yes, are employees provided training to on how to conduct security and agricultural inspections of containers and other IIT?		MUST	#N/A	
12.1.2	If yes, are employees provided training on the company's cybersecurity policies and procedures?		MUST	#N/A	
12.1.3	If yes, are employees managing security technology systems provided training on or have previous experience in their operation and maintenance?		MUST	#N/A	
12.1.4	If yes, are employees trained on how to recognize suspicious situations and the methods to report them?		MUST	#N/A	
12.1.5	If yes, are employees trained on how to identify and prevent the spread of pest contamination?		MUST	#N/A	
12.1.6	If yes, are employees trained or provided regular updates on warning indicators of trade-based money laundering and terrorism financing?		Should	#N/A	
12.1.7	If yes, do these trainings include measures to verify that the training objectives have been met, such as quizzes, exercises or audits?		Should	#N/A	
12.2	Are refresher trainings conducted, either on a regular basis or after incidents, to ensure that employees are current on all updated policies and procedures?		MUST	#N/A	

Section 12.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Criteria	0	Section Score	#N/A
Total No. of Meets Criteria	0	Section Score (%)	#N/A

This document is issued by the Company under its General Conditions of Service accessible at http://www.sgs.com/terms_and_conditions.htm. Attention is drawn to the limitation of liability, indemnification and jurisdiction issues defined therein.

Any holder of this document is advised that information contained hereon is solely limited to visual examination of the safely and readily accessible portions of the consignment and reflects the Company’s findings at the time of its intervention only and within the limits of Client’s instructions, if any. The Company’s sole responsibility is to its Client and this document does not exonerate parties to a transaction from exercising all their rights and obligations under the transaction documents. Any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful and offenders may be prosecuted to the fullest extent of the law.”

END OF CHECKLIST

PHOTO REPORT

Photo Remarks: Facility Entrance

Photo Remarks: Facility Building

Photo Remarks: Loading & Docking Area

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.

Photo Remarks: Packing Area

Photo Remarks: Non-Conformity (if any)

Photo Remarks: Others

©SGS SA 2020. All rights reserved. Confidential and Proprietary information.