Audit Date:	28-Sep-20
Audit Type:	☑ Initial Audit ☐ Follow up Audit
	☑ Annual Audit ☐ Follow up Audit

Qiz Group
SECURITY ASSESSMENT

AUDIT SUMMARY

Qiz Group Textile Company Located at Amerya Free Zone at Alexandria city , Egypt , it surround with fencing and next to it different factories inside free zone compound with external Security and entrance Gate and internal Security , Factory had only 1 building with no internal space for parking , all factory monitored with CCTV camera 24/7 , all shipment outgoing or enter as per free zone and governmental cargo approval .

SITE PROFILE

Basic Information

Supplier Name	Qiz Group			
Facility Address	Amerya Free Zone			
City	Alexandria			
State / Province	Alexandria			
Country	Egypt			
Postal Code	None			
Supplier's Telephone No.	4500228			
Supplier's Fax No.	4500229			
Supplier's E-mail Address	bob@americanfreezone.com			
Supplier's Web-site	www.americanfreezone.com			
C-TPAT Member		YES	x	NO
Business Partner to C-TPAT member		YES	X	NO
Month/Year Started Operations	#####			
Other Location 1	None			
Other Location 2	None			
Other Location 3	None			

Supplier Contacts

President	Beshoy Ashraf Helal	Email: bob.qiz@americanfreezone.com
Plant Manager	Botros Badia	Email: botros.qiz@americanfreezone.co
Quality Manager	Aiyda Gargis	Email: ayida.qiz@americanfreezone.com
Safety Representative	Adel Ahmed	Email: adel.qiz@americanfreezone.com
HR Manager	Abnoub Edward	Email: abnoub.qiz@americanfreezone.c
Housing Manager	Mina Nagih	Email: mina.qiz@americanfreezone.com
Security Manager	Adel Ahmed	Email: adel.qiz@americanfreezone.com
Other - *Type Title here.*		
Other - *Type Title here.*		

Background Information

Product / Service Category(s)	Shirt , Short , Pants , Sweater Kids
Operation Process(es)	Sweing , Packing
Annual Sales (USD)	3 Million $
Capacity/Year (Units)	2,500,000 / Year
Main Language of Employees	Arabic
Language of Management	Arabic - English
Business Nature	Local investment

Plant Size

Total Facility	2860 m2	Square Feet
Production Floors	2000 m2	Square Feet
Warehouse Areas	20 m2	Square Feet
Distribution Areas	0	Square Feet
Canteen & Dormitory Areas	20 m2	Square Feet
Total Number of Buildings	1	
Total Number of Warehouses	1	
Total Number of Gates (Facility access points)	2	
Total Number of Gate Houses	1	

Use of Subcontractor

Name of Subcontractor	Service Type	Address

(i.e. Logistic service providers)	Tiffany Logestic service	El Shoohada Square, El Mansheya, Alexandria
(i.e. External warehouse for storage)		
Other - Additional Subcontractors		
Other - Additional Subcontractors		

Shipment Methods to USA or other countries

By air	0	%
By sea	100	%
By truck	0	%
By rail	0	%
Other carrier type		

Total Employees	On the date of the audit			
No. of Office Staffs	M	15	F	10
No. of Regular Staffs	M	125	F	75
No. of Contractual Staffs	M	0	F	0
No. of Temporary Staffs	M	0	F	0
Others	M	0	F	0
Total no. of employees	M	140	F	85

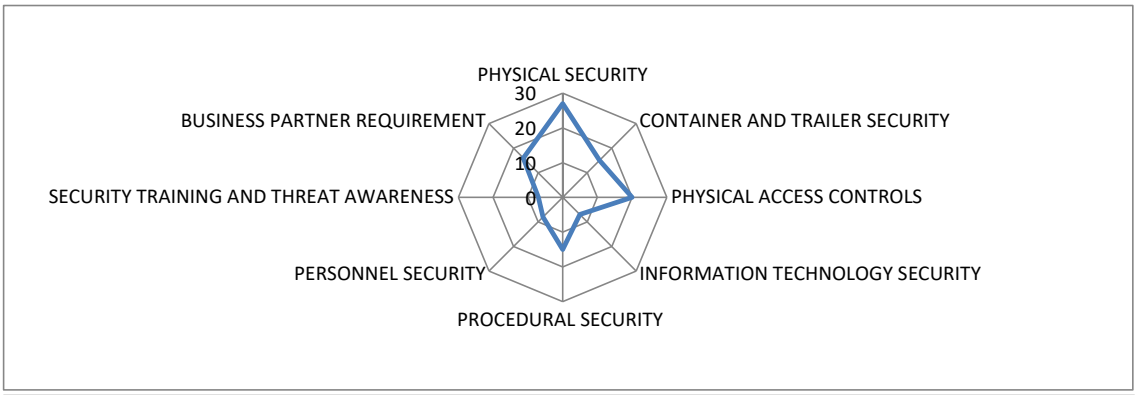
No. of Staff Recruited (last 12 months	55	
No. of Staff Left (last 12 months)	35	
Average No. of Staff Total (last 12 mo	215	
Staff Turnover Rate (last 12 months)	25	%

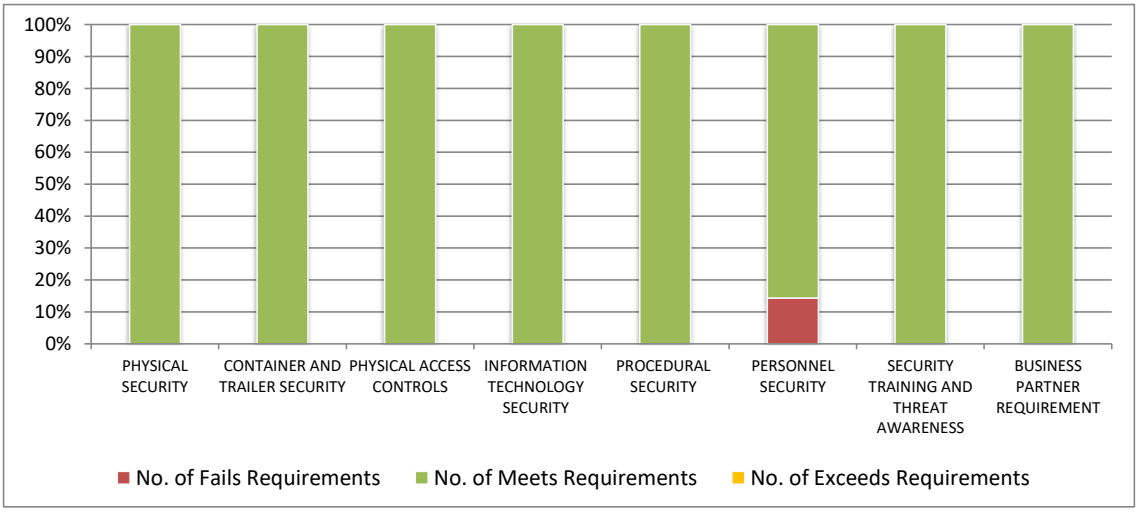
Auditor Name:	Ahmed Hussein
Technical Reviewer Name:	

PERFORMANCE SUMMARY

		No. of Critical Violations	No. of Fails Requirements	No. of Meets Requirements	No. of Exceeds Requirements	Section Score	Section Score (%)
1	PHYSICAL SECURITY	0	0	18	0	27	100%
2	CONTAINER AND TRAILER SECURITY	0	0	8	0	15	100%
3	PHYSICAL ACCESS CONTROLS	0	0	13	0	20	100%
4	INFORMATION TECHNOLOGY SECURITY	0	0	4	0	7	100%
5	PROCEDURAL SECURITY	0	0	9	0	15	100%
6	PERSONNEL SECURITY	0	1	6	0	8	89%
7	SECURITY TRAINING AND THREAT AWARENESS	0	0	6	0	7	100%
8	BUSINESS PARTNER REQUIREMENT	0	0	10	0	16	100%

CRITICAL VIOLATION	FINAL RESULT	OVERALL SCORE
0	LOW RISK	99%





BEST PRACTICE(S) ADOPTED BY AUDIT FACILITY

	Best Practice Observed
PHYSICAL SECURITY	None
CONTAINER AND TRAILER SECURITY	None
PHYSICAL ACCESS CONTROLS	None
INFORMATION TECHNOLOGY SECURITY	None

PROCEDURAL SECURITY	None
PERSONNEL SECURITY	None
SECURITY TRAINING AND THREAT AWARENESS	None
BUSINESS PARTNER REQUIREMENT	None

ACTIONS REQUIRED SUMMARY

Actions Required (Findings of MUST Criteria)	Section Number
There is no employee ID system to control facility access.	3.4
Employees are not sign code of conduct	7.4

ACTIONS RECOMMENDED SUMMARY

Actions Recommended (Findings of SHOULD Criteria)	Section Number

SECTION 1.0 PHYSICAL SECURITY

	Security Measures	Compliance Level	Compliance Weighting	Auditor Remarks	Comments on N/A & Others
1.1	Does the facility have perimeter fencing or walls on all sides of a height of 6 ft. to prevent intrusion?	Meets Requirements	1	The facility has perimeter fencing on all sides of a height of 6 ft. (1.8 m).	
1.2	Does the facility segregate and mark international and domestic cargo in a safe, caged, or otherwise fenced-in area?	Not Applicable	1	Not Applicable	The facility only handles international cargo. No domestic cargo allowed by the law as the factory is free zone area.
1.3	Does the facility segregate and mark hazardous or dangerous cargo in a safe, caged, or otherwise fenced-in area? (Note, please state the nature of the cargo)	Not Applicable	1	Not Applicable	no hazard cargo , company work only in textile
1.4	Does the facility have a documented maintenance program comprised of regularly scheduled inspections to keep security related equipment in good condition and working order? (E.g. building, fencing, gates, lights, alarm system and CCTV.)	Meets Requirements	2	The facility has a maintenance program that requires regular inspections of security related equipment	
1.5	Does the facility have manned gatehouses at all external main access points?	Meets Requirements	2	The facility has manned gatehouses at all external main access points.	
1.6	Is parking at the facility authorized at the gate by a pass and/or decal system?	Meets Requirements	1	Parking authorization is approved from the security gate, but the gate does not issue passes.	company located in freezone area which has gates to go inside but no parking area inside
1.7	Is parking for private vehicles (employees, visitors, vendors, contractors, etc.) restricted to designated areas separate from cargo staging areas and loading docks?	Not Applicable	1	Not Applicable	no space for private parking inside
1.8	Is there a separate loading dock and parking area for trucks and delivery vans?	Meets Requirements	1	There is a separate loading dock and parking area for trucks and delivery vans.	
1.9	Is there a secured area for truck and delivery van drivers to wait while cargo is loaded and unloaded?	Meets Requirements	1	There is a secured waiting area for truck and delivery van drivers.	
1.10	Are buildings designed and constructed with materials appropriate to prevent unlawful entry?	Meets Requirements	2	Buildings are designed and constructed with materials appropriate to prevent unlawful entry (e.g., brick, stone, concrete, heavy gauge steel)	
1.11	Does the facility have locking devices for external and internal doors?	Meets Requirements	2	The facility has locking devices on all internal and external doors.	
1.12	Does the facility have locking devices for external and internal windows and are the external windows protected against intrusion?	Meets Requirements	2	The facility has locking devices on ALL windows. External windows are protected against tampering/intrusion (e.g. by wire mesh or protective coatings, or by utilizing window	
1.13	Does the facility have locking devices for external and internal gates and fences?	Meets Requirements	2	The facility has locking devices on all fences and gates.	
1.14	Does Management or Security Personnel control the issuance of all locks and keys?	Meets Requirements	2	Management or Security Personnel controls the issuance of all locks and keys.	
1.15	Does the facility have internal and external lighting in all required areas (e.g. factory perimeter, parking areas, etc.)?	Meets Requirements	2	The facility has adequate internal and external lighting in all areas, and is properly maintained according to all needs of the factory. (e.g., employees, guards, CCTV)	
1.16	Does the facility have a security alarm system? Is the alarm code reset when employees who have the code resign or are terminated?	Meets Requirements	1	The facility has logs of alarm codes issued, and has a procedure for resetting alarm codes when employees resign or are terminated. The alarm is in proper working order.	
1.17	Do CCTV cameras monitor critical internal and external access areas?	Meets Requirements	1	Entrances to the property or parking areas and other critical areas are monitored by CCTV.	
1.18	Does the company employ a person who is responsible for managing C-TPAT matters and facility security?	Meets Requirements	1	The company does employ a person who is responsible for managing C-TPAT matters and facility security?	
1.19	Does the facility employ security guards?	Meets Requirements	1	Security guards are employed.	
1.20	Do security personnel perform scheduled security patrols?	Meets Requirements	1	Security personnel perform scheduled security patrols during working hours.	

1.21	Does the facility have a designated employee or security officer to supervise the introduction and removal of cargo to include manifest and seal verification?	Meets Requirements	2	There is a designated employee or security officer responsible for supervising the movement of cargo and verifying manifest and seal information.	Security Guard for facility and Free zone Security , Cargo employee

Section 1.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	3
Total No. of Fails Requirements	0		
Total No. of Meets Requirements	18	Section Score	27
Total No. of Exceeds Requirements	0	Section Score (%)	100%

SECTION 2.0 CONTAINER AND TRAILER SECURITY

	Security Measures	Compliance Level	Compliance Weighting	Auditor Remarks	Comments on N/A & Others
2.1	Does the company have written procedures to verify the physical integrity of the container structure prior to stuffing, including the reliability of the locking mechanisms?	Meets Requirements	2	Written procedures exist and the physical integrity of the container structure is verified prior to stuffing. A checklist is completed verifying a seven point inspection. This inspection includes: front wall, left side, right side, floor, ceiling/ roof, inside/outside doors, outside undercarriage.	
2.2	Does the company have written procedures in place at the point of stuffing to maintain the integrity of the shipping container?	Meets Requirements	2	Written procedures exist at the point of stuffing to maintain the integrity of the shipping container.	
2.3	Does the company have written procedures in place for reporting and neutralizing unauthorized entry into containers or container storage areas?	Meets Requirements	2	Written procedures exist to report and neutralize entry into containers or container storage areas.	
2.4	Does the company have written procedures to verify the physical integrity of the trailer prior to stuffing, including the reliability of the locking mechanisms?	Meets Requirements	2	Written procedures exist and the physical integrity of the trailer is verified prior to stuffing. A checklist is completed.	
2.5	Does the company have written procedures in place to control, affix, record and reconcile ISO/PAS 17712 compliant seals on containers and trailers?	Meets Requirements	2	Written procedures are in place to control, affix, record and reconcile ISO/PAS 17712 compliant seals on containers and trailers. Only designated employees distribute container seals. The	
2.6	Does the company secure all loaded containers and trailers with a ISO/PAS 17712 high-security standard seal?	Not Applicable	2	Not Applicable	According to the Egyptian customs regulations, the local governmental customs are responsible for applying the seal and not the facility.
2.7	Does the company secure all empty containers and trailers with a ISO/PAS 17712 high-security standard seal or high-security padlock?	Not Applicable	2	Not Applicable	According to the Egyptian customs regulations, the local governmental customs are responsible for applying the seal and not the facility.
2.8	Does the company have a secure storage area for empty and full containers to prevent unauthorized access?	Meets Requirements	2	Empty and full containers are stored in a secure area (e.g. an area with a locked perimeter fence and adequate lighting).	
2.9	Does the facility have written incident reporting procedures to report thefts, tampering and unmanifested items both internally and externally to management and Customs and other law enforcement agencies?	Meets Requirements	2	There are written incident reporting procedures to report thefts, tampering and unmanifested items both internally and externally.	
2.10	Are there procedures in place to track the timely movement of incoming and outgoing goods?	Meets Requirements	1	Drivers are tracked using electronic communication or other monitoring methods.	

Section 2.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	2
Total No. of Fails Requirements	0		
Total No. of Meets Requirements	8	Section Score	15
Total No. of Exceeds Requirements	0	Section Score (%)	100%

SECTION 3.0 PHYSICAL ACCESS CONTROLS

	Security Measures	Compliance Level	Compliance Weighting	Auditor Remarks	Comments on N/A & Others
3.1	Does the company have a documented procedure defining access controls?	Meets Requirements	2	The company has a documented procedure defining access controls.	
3.2	Are all employees required to present identification upon entering the facility?	Meets Requirements	2	Identification is required for all employees and checked upon entrance.	
3.3	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 resign or are terminated?	Meets Requirements	2	The facility has logs of control keys and has a documented procedure for lost keys including changing locks when relevant employees resign or are terminated.	
3.4	Does the company utilize an effective, employee ID system to control access? Employees should only be given access to those areas that are necessary for the performance of their duties.	Meets Requirements	1	There is an effective employee ID system to control facility access. Employees are only given access to those areas needed for the performance of one's duties. Access codes are	
3.5	Does the company have a documented procedure defining the controls for visitor access to facility?	Meets Requirements	2	Documented procedure in place defining controls for visitor access to facility.	

3.6	Are all visitors required to present a valid photo ID for positive identification before being allowed access to the facility?	Meets Requirements	2	All visitors, without exception, are required to present an official photo ID.	
3.7	Does the company maintain a log of all visitors entering the facility?	Meets Requirements	2	All visitors' names and companies are written in a logbook at either the security gate, loading area	
3.8	Are all visitors issued temporary ID's?	Meets Requirements	1	Temporary ID's are issued for all visitors.	
3.9	Are employee escorts required for all visitors while on the premises?	Meets Requirements	1	Employee escorts are required to remain with visitors throughout their visit.	
3.10	Are all visitor's packages screened prior to being granted admission to the facility?	Meets Requirements	1	Visitors and their possessions are searched before entering the facility without exception.	
3.11	Are visitors required to have an appointment prior to being granted admission to the facility?	Meets Requirements	1	All visitors are required to have an appointment prior to being granted admission to the facility.	
3.12	Are packages and mail periodically screened for dangerous materials prior to dissemination?	Meets Requirements	1	Packages and mail are periodically screened for dangerous materials prior to dissemination.	
3.13	Does the company have written procedures for challenging unauthorized and unidentified persons attempting to gain access to the facility?	Meets Requirements	2	There are written procedures for challenging unauthorized or unidentified persons that have gained or are attempting to gain access.	

Section 3.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Requirements	0		
Total No. of Meets Requirements	13	Section Score	20
Total No. of Exceeds Requirements	0	Section Score (%)	100%

SECTION 4.0 INFORMATION TECHNOLOGY SECURITY

	Security Measures	Compliance Level	Compliance Weighting	Auditor Remarks	Comments on N/A & Others
4.1	Does the company have IT security policies and procedures in place?	Meets Requirements	2	The company has IT security policies and procedures in place. IT personnel provide policy	
4.2	Are all automated systems assigned individual accounts that require a periodic change of password?	Not Applicable	2	Not Applicable	no domain automatic system
4.3	Does the company IT security policy cover automatic time-out functions with forced logoffs? Does it also deny user access after a failed number of attempts to log-in?	Meets Requirements	1	The company IT security policy covers automatic time-out functions with forced logoffs and denies user access after a failed number of attempts to log-in.	
4.4	Does the company have a system in place to identify tampering and potential system violators?	Meets Requirements	2	The company has a system in place to identify tampering and potential system violators. All system violators are subject to disciplinary action.	
4.5	Does the company have a policy safeguarding computer information?	Meets Requirements	2	The company has a policy safeguarding computer information which includes securing all servers and performing a periodic backup of all systems.	backup every 15 days on external hard disc

Section 4.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	1
Total No. of Fails Requirements	0		
Total No. of Meets Requirements	4	Section Score	7
Total No. of Exceeds Requirements	0	Section Score (%)	100%

SECTION 5.0 PROCEDURAL SECURITY

	Security Measures	Compliance Level	Compliance Weighting	Auditor Remarks	Comments on N/A & Others
5.1	Does the company have documented security procedures in place to ensure the integrity and security of processes relevant to the transportation, handling and storage of cargo in the supply chain?	Meets Requirements	2	The company has documented security procedures in place to ensure the integrity and security of processes relevant to the transportation, handling and storage of cargo in	
5.2	Does the company have written procedures in place to ensure that manifest information received from business partners is reported accurately and timely?	Meets Requirements	2	Written procedures are in place to ensure that manifest information received from business partners is accurate and timely.	
5.3	Are procedures in place to control documents that include proprietary company and shipment information?	Meets Requirements	2	There are written procedures in place to control documents that include proprietary company and	
5.4	Are drivers required to present photo identification prior to cargo being received or released to/from their custody?	Meets Requirements	2	Drivers are required to present photo identification prior to cargo being received or	
5.5	Are finished products properly marked, counted, weighed, documented, and reported on the manifest and bills of lading?	Meets Requirements	1	Finished products are properly marked, counted, weighed, documented, and reported on the	
5.6	Does the company have procedures and security controls in place to track the movement of all departing cargo?	Meets Requirements	1	Procedures and security controls exist to track the movement of all departing cargo. These procedures include reconciling the goods against the manifest and ensuring they are accurately	
5.7	Does the company have procedures in place to protect inbound and outbound shipments against un-manifested material being introduced?	Meets Requirements	1	Procedures are in place to protect and verify shipments. They include verifying all goods against the manifest and all pertinent shipping documents.	Facility is located at free zone area where all shipment is inspected and verified by free zone security staff.
5.8	Does the company have written procedures in place to resolve all cargo discrepancies prior to cargo being released or received?	Meets Requirements	2	The company has written procedures in place to resolve all cargo discrepancies prior to cargo being released or received. Those procedures	
5.9	Does the company have documented procedures to report shortages and overages of cargo to the relevant authorities?	Meets Requirements	2	Documented procedures are in place to notify the appropriate authorities of any cargo discrepancy.	

Section 5.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Requirements	0		
Total No. of Meets Requirements	9	Section Score	15
Total No. of Exceeds Requirements	0	Section Score (%)	100%

SECTION 6.0 PERSONNEL SECURITY

	Security Measures	Compliance Level	Compliance Weighting	Auditor Remarks	Comments on N/A & Others
6.1	Does the company verify the information on employment applications submitted from prospective employees in compliance with federal, state, provincial, and local government regulations and statutes?	Meets Requirements	2	Management verifies information on applications in compliance with federal, state, provincial, and local government regulations and statutes. Verification results are maintained for the length	
6.2	Does the company interview prospective employees in compliance with federal, state, provincial, and local government regulations and statutes?	Meets Requirements	1	Prospective employees are interviewed consistent with federal, state, provincial, and local government regulations and statutes. All records are kept in a secure place for the length	
6.3	Does the company perform background checks of prospective employees in compliance with federal, state, provincial, and local government regulations and statutes?	Fails Requirements	1	No background checks are performed, or are performed at random.	3 of 10 checked worker's files do not contain criminal records as required by facility procedures and local law
6.4	Does the company conduct periodic background checks and/or screen existing employees, in compliance with federal, state, provincial, and local government regulations and statutes?	Meets Requirements	1	Periodic rescreening of employee background checks are performed on all employees in compliance with federal, state, provincial and local government regulations and statutes.	
6.5	Does the company perform driving record background checks of existing company drivers?	Not Applicable	1	Not Applicable	no drivers for the company
6.6	Does the company have documented procedures describing actions to take upon employee separation?	Meets Requirements	2	Documented termination procedures are in place and include the use of a termination/separation checklist.	
6.7	Does the Company have processes established for reporting and managing problems related to personnel security?	Meets Requirements	1	Procedures for managing personnel security problems and recording incidents are in effect.	
6.8	Are employees required to sign a Code of Conduct?	Meets Requirements	1	All employees are required to sign a Code of Conduct.	

Section 6.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	1
Total No. of Fails Requirements	1		
Total No. of Meets Requirements	6	Section Score	8
Total No. of Exceeds Requirements	0	Section Score (%)	89%

SECTION 7.0 SECURITY TRAINING AND THREAT AWARENESS

	Security Measures	Compliance Level	Compliance Weighting	Auditor Remarks	Comments on N/A & Others
7.1	Does the company provide security training to employees which includes maintaining cargo integrity, recognizing internal conspiracies and protecting access controls during new hire orientation?	Meets Requirements	1	The company provides security training to employees which includes maintaining cargo integrity, recognizing internal conspiracies and protecting access controls.	
7.2	Does the company provide threat awareness training by company management or security personnel through routine briefings or memoranda?	Meets Requirements	1	Company management or security personnel provide threat awareness programs that include up-to-date information on emerging security threats.	training awareness dated 4 July 2019 , 6 July 2019 , 14 July 2019 for CTPAT requirements and refreshment in September 2020.
7.3	Are there written procedures in place instructing employees on recognizing suspicious situations and how to report them?	Meets Requirements	2	There are written procedures in place instructing employees on recognizing suspicious situations and how to report them.	emergency number posted in case of any suspicious situation
7.4	Is additional training provided to employees in the shipping and receiving areas?	Meets Requirements	1	There is additional periodic training regarding cargo security provided to employees in the shipping and receiving areas.	wworkers have on job training related to job nature been checked through workers' interview. External training dated 6 July 2020
7.5	Is there an incentive scheme in place which encourages staff to report security incidents? Note whether financial or non-financial scheme.	Meets Requirements	1	There is an incentive scheme to report security incidents. Indicate financial or non-financial.	incentive scheme bonus in security rules posted in different work locations
7.6	Does the company provide training to employees in detecting fraudulent documentation and computer security?	Meets Requirements	1	Training is provided in both detecting fraudulent documentation and computer security.	While all documents go through free zone area, all workers have on job training related to job nature been checked through workers'

Section 7.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Requirements	0		
Total No. of Meets Requirements	6	Section Score	7
Total No. of Exceeds Requirements	0	Section Score (%)	100%

SECTION 8.0 BUSINESS PARTNER REQUIREMENT

	Security Measures	Compliance Level	Compliance Weighting	Auditor Remarks	Comments on N/A & Others
8.1	Does the company have a documented risk based process in place for the selection of all business partners?	Meets Requirements	2	The company has a documented risk based process in place for the selection of all business partners. Internal requirements should include financial soundness (e.g. credit check, bank reference, annual report) and the capability of meeting contractual requirements.	
8.2	If the auditee is a CTPAT member, is a SVI number requested and periodically verified for those business partners eligible for C-TPAT?	Meets Requirements	2	A SVI number is requested and periodically verified for those business partners eligible for C-TPAT.	
8.3	Does the company require service providers to complete a security questionnaire or provide evidence of their security procedures ensuring compliance with C-TPAT minimum security criteria?	Meets Requirements	2	The company does require service providers to complete a security questionnaire or provide written security procedures confirming compliance with C-TPAT minimum security criteria.	

8.4	Do contracts with vendors and service providers address compliance with C-TPAT minimum security standards?	Meets Requirements	2	Written contracts specify that C-TPAT minimum security standards are required and maintained for all vendors and service providers.	
8.5	Does the Company maintain a list of all service providers by name, type of service provided, address of physical office location, telephone number, faxes number, email, and contact name?	Meets Requirements	1	List is maintained.	company have suppliers list checked
8.6	Does the company have a documented and verifiable risk analysis procedure for determining appropriate security measures throughout their supply chain based on its business model? (e.g. volume, country of origin, routing, terrorist threat)	Meets Requirements	2	There is a documented procedure in place with records to provide evidence that all business partners have been included in the risk assessment.	
8.7	Does the company conduct security assessments of areas under their internal control within the supply chain?	Meets Requirements	2	The company conducts security assessments and evidence in the form of a checklist or report is available.	
8.8	Does the company have documented procedures and security controls in place for service provider audits?	Meets Requirements	1	Service provider audits are conducted and documented.	
8.9	Does the company participate in a supply chain security program administered by a foreign Customs Administration?	Meets Requirements	1	The company does participate in a supply chain security program administered by a foreign Customs Administration.	
8.10	Does the company require that all sub-contracted partners within the supply chain maintain C-TPAT minimum security criteria?	Meets Requirements	1	The company requires that all sub-contracted partners within the supply chain maintain C-TPAT minimum security criteria.	

Section 8.0 Summary

Total No. of Critical Violations	0	Total No. of Not Applicable (NA)	0
Total No. of Fails Requirements	0		
Total No. of Meets Requirements	10	Section Score	16
Total No. of Exceeds Requirements	0	Section Score (%)	100%

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

SECTION 9.0 PHOTO REPORT

Photo Remarks: Facility Entrance

Photo Remarks: Facility Gate from inside

Photo Remarks: Facility Building

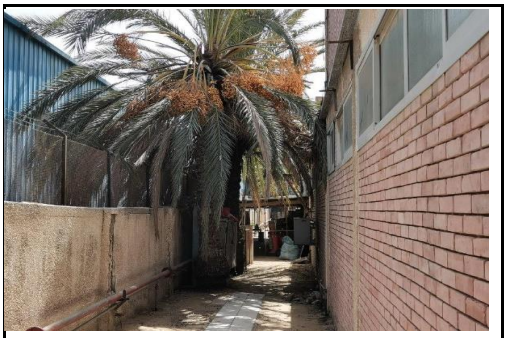


Photo Remarks: Facility Fencing

Photo Remarks: Loading & Docking Area

Photo Remarks: Storage of Final Product

Photo Remarks: Packing Area

Photo Remarks: cctv Camera montering

Photo Remarks: Facility need employee ID more control for packing area

Photo Remarks: Athourized workers for packing area

Photo Remarks: Security Room

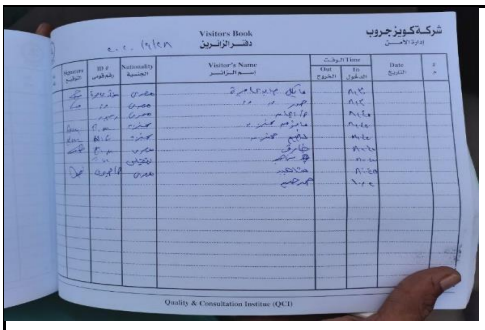


Photo Remarks: Visitor Log

Photo Remarks: Security Alarm Button

Photo Remarks: CCTV Unit

Access control

Scoring Guidelines

SECTION 1.0 PHYSICAL SECURITY

Cargo handling and storage facilities in international locations MUST have physical barriers and deterrents that guard against unauthorized access.

Fencing: Perimeter fencing SHOULD enclose the areas around cargo handling and storage facilities. Interior fencing within a cargo handling structure SHOULD be used to segregate domestic, international, high value and hazardous cargo. All fencing MUST be regularly inspected for integrity and damage.

Section	Security Measures	Fails Requirements = 0	Meets Requirements = 1	Exceeds Requirements = 2
1.1	Does the facility have perimeter fencing or walls on all sides of a height of 6 ft. to prevent intrusion?	The facility has no perimeter fencing, or incomplete perimeter fencing, or the fencing is less than 6 feet (1.8 m) in height.	The facility has perimeter fencing on all sides of a height of 6 ft. (1.8 m).	The perimeter has fencing on all sides of a height of 8 ft. (2.4 m) and the fence or wall is constructed of steel or flat surface stone, and further secured by materials preventing scaling over the fence (e.g., razor wire, barbed
1.2	Does the facility segregate and mark international and domestic cargo in a safe, caged, or otherwise fenced-in area?	International and Domestic Cargo is not segregated or marked.	International and Domestic Cargo is segregated, marked and placed in a safe, caged or otherwise fenced-in area.	In addition International and Domestic Cargo is monitored by CCTV or alarm systems.
1.3	Does the facility segregate and mark hazardous or dangerous cargo in a safe, caged, or otherwise fenced-in area? (Note, please state the nature of the cargo)	Hazardous or Dangerous Cargo is not segregated or marked.	Hazardous or Dangerous Cargo is segregated, marked and placed in a safe, caged or otherwise fenced-in area.	Hazardous or Dangerous cargo is segregated, marked and placed in a safe, caged, or otherwise fenced-in area, which is monitored by CCTV or alarm systems.
1.4	Does the facility have a documented maintenance program comprised of regularly scheduled inspections to keep security related equipment in good condition and working order? (E.g. building, fencing, gates, lights, alarm system and CCTV.)	The facility has no formal maintenance program of regularly scheduled inspections of security related equipment.	The facility has a maintenance program that requires regular inspections of security related equipment	Additionally, corrective action is taken and the inspection results are documented.

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

1.5	Does the facility have manned gatehouses at all external main access points?	Not all external main access points have a manned gatehouse.	The facility has manned gatehouses at all external main access points.	Manned gatehouses have communications systems back to the front office, and are automated with alarms and cameras.

Parking: Private passenger vehicles SHOULD be prohibited from parking in or adjacent to cargo handling and storage areas.

Scoring Guidelines

1.6	Is parking at the facility authorized at the gate by a pass and/or decal system?	There are no authorization measures for the parking facility.	Parking authorization is approved from the security gate, but the gate does not issue passes.	Parking authorization is approved at the security gate with a gate pass and/or decal system with a serial number traceable to the employee and/or visitor.
1.7	Is parking for private vehicles (employees, visitors, vendors, contractors, etc.) restricted to designated areas separate from cargo staging areas and loading docks?	There are no parking restrictions for private vehicles.	Parking for private vehicles is restricted to designated areas separate from cargo staging and loading docks.	In addition, security personnel routinely direct visitors and monitor and patrol private vehicle parking areas. Access to cargo staging areas and loading docks is controlled by checkpoint.
1.8	Is there a separate loading dock and parking area for trucks and delivery vans?	There is no separate loading dock and parking area for trucks and delivery vans.	There is a separate loading dock and parking area for trucks and delivery vans.	In addition parking areas are enforced/monitored and patrolled by dock or security personnel. Access to cargo staging areas and loading docks is controlled by checkpoint.
1.9	Is there a secured area for truck and delivery van drivers to wait while cargo is loaded and unloaded?	There is no secured waiting area for drivers to wait. Drivers are allowed to wait in the loading area.	There is a secured waiting area for truck and delivery van drivers.	Drivers are required to show photo identification and log in and out in accordance with the visitor policy. In addition, the secure waiting area is monitored by security personnel or CCTV.
Building Structure: Buildings MUST be constructed of materials that resist unlawful entry. The integrity of structures MUST be maintained by periodic inspection and repair.				
1.10	Are buildings designed and constructed with materials appropriate to prevent unlawful entry?	Buildings are not designed and constructed with materials designed to prevent unlawful entry.	Buildings are designed and constructed with materials appropriate to prevent unlawful entry (e.g., brick, stone, concrete, heavy gauge steel)	In addition, physical components of the facility are reinforced or further secured (e.g. roof sealing, steel door frames, etc.) to prevent unlawful entry.
Locking Devices and Key Controls: All external and internal windows, gates and fences MUST be secured with locking devices. Management or security personnel MUST control the issuance of all locks and keys.				
1.11	Does the facility have locking devices for external and internal doors?	The facility does not have locking devices on all external and internal doors or the devices are not adequate in that they are easily violated (e.g., simple physical pressure or tampering)	The facility has locking devices on all internal and external doors.	In addition, doors and doorframes are made of reinforced materials (e.g., steel) or are connected to redundant systems (e.g., alarm).

Scoring Guidelines

1.12	Does the facility have locking devices for external and internal windows and are the external windows protected against intrusion?	The facility does not have locking devices on internal and external windows and external windows are not protected against intrusion.	The facility has locking devices on ALL windows. External windows are protected against tampering/intrusion (e.g. by wire mesh or protective coatings, or by utilizing window materials such as heavy	In addition, the facility has locking devices and protection against tampering/intrusion on all windows, and the windows are connected to an alarm system.
1.13	Does the facility have locking devices for external and internal gates and fences?	The facility does not have locking devices on internal and external gates and fences.	The facility has locking devices on all fences and gates.	The facility has locking devices on all fences and gates. Gates and fences at cargo areas and access points are connected to an alarm system.
1.14	Does Management or Security Personnel control the issuance of all locks and keys?	Management or Security Personnel does not control the issuance of all locks and keys.	Management or Security Personnel controls the issuance of all locks and keys.	Management or Security Personnel controls the issuance of all locks and keys and keeps a written or electronic log.
Lighting: Adequate lighting MUST be provided inside and outside the facility including the following areas: entrances and exits, cargo handling and storage areas, fence lines and parking areas.				
1.15	Does the facility have internal and external lighting in all required areas (e.g. factory perimeter, parking areas, etc.)?	The facility does not have any internal and external lighting systems.	The facility has adequate internal and external lighting in all areas, and is properly maintained according to all needs of the factory. (e.g., employees, guards, CCTV)	The facility has internal and external lighting systems in all areas and the systems are properly maintained according to all needs of the factory. (e.g., workers, guards, CCTV) There is also a back up generator for security, computer and lighting
Alarm Systems and Video Surveillance Cameras: Alarm systems and video surveillance cameras SHOULD be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas.				
1.16	Does the facility have a security alarm system? Is the alarm code reset when employees who have the code resign or are terminated?	The facility has no electronic alarm system, or if it has an electronic system there is no log of employee access to alarm codes and no attempt is made to reset alarm codes after employment	The facility has logs of alarm codes issued, and has a procedure for resetting alarm codes when employees resign or are terminated. The alarm is in proper working order	The alarm is connected to a third party security company and/or local authorities.
1.17	Do CCTV cameras monitor critical internal and external access areas?	There are no CCTV cameras monitoring critical internal and external access areas.	Entrances to the property or parking areas and other critical areas are monitored by CCTV.	In addition, CCTV transmissions from critical areas are recorded in color and stored for a minimum of
1.18	Does the company employ a person who is responsible for managing C-TPAT matters and facility security?	The company does not employ a person who is responsible for managing C-TPAT matters and facility security?	The company does employ a person who is responsible for managing C-TPAT matters and facility security?	There is a security manager employed who is solely responsible for managing C-TPAT matters and facility security.

Scoring Guidelines

1.19	Does the facility employ security guards?	No security guards are employed.	Security guards are employed.	Security guards are employed, undergo periodic training, and wear uniforms.
1.20	Do security personnel perform scheduled security patrols?	Security personnel do not perform scheduled security patrols.	Security personnel perform scheduled security patrols during working hours.	Security personnel perform scheduled security patrols 24 hours per day, 7 days per week.
1.21	Does the facility have a designated employee or security officer to supervise the introduction and removal of cargo to include manifest and seal verification?	There is no designated employee or security officer to supervise the introduction and removal of cargo.	There is a designated employee or security officer responsible for supervising the movement of cargo and verifying manifest and seal information.	There is a designated employee or security officer assigned to shipping and receiving. This officer controls all movement of cargo and is further responsible for the issuance and removal of high-security seals.

SECTION 2.0 CONTAINER AND TRAILER SECURITY

Container and trailer integrity MUST be maintained to protect against the introduction of unauthorized material and/or persons. At the point-of-stuffing, procedures MUST be in place to properly seal and maintain the integrity of the shipping containers and trailers. A high security seal MUST be affixed to all loaded containers and trailers bound for the U.S. All seals MUST meet or exceed the current PAS ISO 17712 standard for high security seals.

In those geographic areas where risk assessments warrant checking containers or trailers for human concealment or smuggling, such procedures SHOULD be designed to address this risk at the manufacturing facility or point-of-stuffing.

Container Inspection: Procedures MUST be in place to verify the physical integrity of the container structure prior to stuffing, to include the reliability of the locking mechanisms of the doors. A seven-point inspection process is recommended for all containers: Front Wall, Left Side, Right Side, Floor, Ceiling/Roof, Inside/Outside Doors, Outside/Undercarriage.

Section	Security Measures	Fails Requirements = 0	Meets Requirements = 1	Exceeds Requirements =
2.1	Does the company have written procedures to verify the physical integrity of the container structure prior to stuffing, including the reliability of the locking mechanisms?	No procedures exist.	Written procedures exist and the physical integrity of the container structure is verified prior to stuffing. A checklist is completed verifying a seven point inspection. This inspection includes: front wall, left side, right side, floor, ceiling/ roof, inside/outside doors,	In addition, a security officer or cargo supervisor verifies the inspection process.
2.2	Does the company have written procedures in place at the point of stuffing to maintain the integrity of the shipping container?	No procedures exist.	Written procedures exist at the point of stuffing to maintain the integrity of the shipping container.	In addition, procedures are enforced and container stuffing is witnessed by an authorized security person.

Scoring Guidelines

2.3	Does the company have written procedures in place for reporting and neutralizing unauthorized entry into containers or container storage areas?	No procedures exist.	Written procedures exist to report and neutralize entry into containers or container storage areas.	In addition, procedures are enforced and unauthorized or unidentified individuals are detained.
Trailer Inspection: Procedures MUST be in place to verify the physical integrity of the trailer structure prior to stuffing, to include the reliability of the locking mechanisms of the doors.				
2.4	Does the company have written procedures to verify the physical integrity of the trailer prior to stuffing, including the reliability of the locking mechanisms?	No procedures exist.	Written procedures exist and the physical integrity of the trailer is verified prior to stuffing. A checklist is completed.	In addition the company deploys a thorough inspection process to include: Fifth wheel area-check natural compartment/skid plate, exterior front/sides, rear-bumpers/doors, front walls, left side, right side, floor, ceiling roof, inside/outside doors, outside undercarriage.
Container and Trailer Seals: The sealing of trailers and containers, to include continuous seal integrity, are crucial elements of a secure supply chain and remains a critical part of a foreign manufacturers commitment to C-TPAT. The foreign manufacturer MUST affix a high security seal to all loaded trailers and containers bound for the U.S. All seals MUST meet or exceed the current PAS ISO 17712 standards for high security seals.				
Written procedures MUST stipulate how seals are to be controlled and affixed to loaded containers and trailers, to include procedures for recognizing and reporting compromised seals and/or containers/trailers to U.S. Customs and Border Protection or the appropriate foreign authority. Only designated employees SHOULD distribute seals for integrity purposes.				
2.5	Does the company have written procedures in place to control, affix, record and reconcile ISO/PAS 17712 compliant seals on containers and trailers?	There are no written procedures in place to control, affix, record and reconcile ISO/PAS 17712 compliant seals on containers and trailers.	Written procedures are in place to control, affix, record and reconcile ISO/PAS 17712 compliant seals on containers and trailers. Only designated employees distribute container seals. The procedures include recognizing and reporting compromised seals or seal discrepancies.	In addition, procedures are enforced by more than one system, (e.g. visual and electronic.), and container sealing is randomly monitored by a third party inspection company.
2.6	Does the company secure all loaded containers and trailers with a ISO/PAS 17712 high-security standard seal?	The company does not secure all loaded containers and trailers with a ISO/PAS 17712 high-security standard seal.	The company secures all loaded containers and trailers with a ISO/PAS 17712 high-security standard seal.	In addition, container sealing is randomly monitored by a third party inspection company.
2.7	Does the company secure all empty containers and trailers with a ISO/PAS 17712 high-security standard seal or high-security padlock?	The company does not secure all empty containers and trailers with a ISO/PAS 17712 high-security standard seal or high-security padlock.	The company secures all empty containers and trailers with a ISO/PAS 17712 high-security standard seal or high-security padlock.	In addition, container sealing is randomly monitored by a third party inspection company.

Scoring Guidelines

Container and Trailer Storage: Containers and trailers under foreign manufacturer control or located in a facility of the foreign manufacturer MUST be stored in a secure area to prevent unauthorized access and/or manipulation. Procedures MUST be in place for reporting and neutralizing unauthorized entry into containers/trailers or container/trailer storage areas.

2.8	Does the Company have a secure storage area for empty and full containers to prevent unauthorized access?	There are no secure storage areas for empty and full containers.	Empty and full containers are stored in a secure area (e.g. an area with a locked perimeter fence and adequate lighting).	In addition they are monitored by a redundant security system (e.g. CCTV, security patrols, etc.).
2.9	Does the facility have written incident reporting procedures to report thefts, tampering and unmanifested items both internally and externally to management and Customs and other law enforcement agencies?	There are no written incident reporting procedures to report thefts, tampering and unmanifested items either internally or externally.	There are written incident reporting procedures to report thefts, tampering and unmanifested items both internally and externally.	In addition, instances are documented and Corrective Action Plans are required to be implemented in 30 days.
2.10	Does the Company communicate with truck drivers delivering cargo, containers and raw materials? Comment on the method of communication.	There are no procedures in place to track the timely movement of incoming and outgoing goods.	Drivers are tracked using electronic communication or other monitoring methods.	Satellite tracking is used and a truck can be disabled by dispatch.

SECTION 3.0 PHYSICAL ACCESS CONTROLS

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

Employees: An employee identification system MUST be in place for positive identification and access control purposes. Employees SHOULD only be given access to those secure areas needed for the performance of their duties. Company management or security personnel MUST adequately control the issuance and removal of employee, visitor and vendor identification badges. Procedures for the issuance, removal and changing of access devices (keys, cards, etc.) MUST be documented.

Section	Security Measures	Fails Requirements = 0	Meets Requirements = 1	Exceeds Requirements =
3.1	Does the company have a documented procedure defining access controls?	The company does not have a documented procedure defining access controls.	The company has a documented procedure defining access controls.	In addition, the procedure includes notifying authorities of unwanted persons on the premises.
3.2	Are all employees required to present identification upon entering the facility?	There is no requirement for employee identification.	Identification is required for all employees and checked upon entrance.	In addition, the company provides photo ID's for all employees, and the ID must be worn at all times.
3.3	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 resign or are	The facility has no log of parties receiving keys and no attempt is made to recover keys after employment ceases.	The facility has logs of control keys and has a documented procedure for lost keys including changing locks when relevant employees resign or are terminated.	The facility uses electronic card keys and has a documented procedure or checklist to deactivate the card when an employee resigns or is terminated.

Scoring Guidelines

3.4	Does the company utilize an effective, employee ID system to control access? Employees should only be given access to those areas that are necessary for the performance of their duties.	There is no employee ID system to control facility access.	There is an effective employee ID system to control facility access. Employees are only given access to those areas needed for the performance of one's duties. Access codes are kept in a secure log and are randomly monitored. Access codes are when an employee resigns or is	The company utilizes an electronic identification system to control employee access. Electronic logs are randomly monitored.
Visitors: Visitors MUST present photo identification for documentation purposes upon arrival. All visitors SHOULD be escorted and SHOULD visibly display temporary identification.				
Deliveries and Mail: Proper vendor ID and/or photo identification MUST be presented for documentation purposes upon arrival by all vendors. Arriving packages and mail SHOULD be periodically screened prior to being disseminated.				
3.5	Does the company have a documented procedure defining the controls for visitor access to facility?	There is no documented procedure.	Documented procedure in place defining controls for visitor access to facility.	In addition, the documented procedure includes actions related to visitor rejection and reporting to the authorities.
3.6	Are all visitors required to present a valid photo ID for positive identification before being allowed access to the facility?	There are no photo identification requirements for visitors to enter the facility.	All visitors, without exception, are required to present an official photo ID.	In addition, a copy of the visitor's identification is maintained by security until visitor departs facility.
3.7	Does the company maintain a log of all visitors entering the facility?	There are no logs for visitors.	All visitors' names and companies are written in a logbook at either the security gate, loading area or the front office.	In addition, arrival and departure times are monitored for reconciliation each day by security personnel or management.
3.8	Are all visitors issued temporary ID's?	No temporary ID's are issued for visitors.	Temporary ID's are issued for all visitors.	In addition, all temporary ID's are required to be returned upon departure and lost ID's are tracked.
3.9	Are employee escorts required for all visitors while on the premises?	Employee escorts are not required.	Employee escorts are required to remain with visitors throughout their visit.	In addition, escorts ensure visitors are logged in and out; the escorts name is recorded in the log book; and the escort is responsible for retrieving and returning the visitors temporary
3.10	Are all visitor's packages screened prior to being granted admission to the facility?	There is no procedure to screen visitor's packages prior to being granted admission to the facility.	Visitors and their possessions are searched before entering the facility without exception.	In addition, visitors and their possessions are scanned with metal detectors prior to entering the facility.

Scoring Guidelines

3.11	Are visitors required to have an appointment prior to being granted admission to the facility?	Visitors are not required to have an appointment prior to being granted admission to the facility.	All visitors are required to have an appointment prior to being granted admission to the facility.	In addition, a daily visitor log is maintained at the security gate, loading area and the front office. Each log is reconciled daily.
3.12	Are packages and mail periodically screened for dangerous materials prior to dissemination?	Packages and mail are not periodically screened for dangerous materials prior to dissemination.	Packages and mail are periodically screened for dangerous materials prior to dissemination.	There are procedures in place for screening and logging packages and mail prior to dissemination.
Challenging and Removing Unauthorized Persons: Procedures MUST be in place to identify, challenge and address unauthorized/unidentified persons.				
3.13	Does the company have written procedures for challenging unauthorized and unidentified persons attempting to gain access to the facility?	There are no written procedures for challenging unauthorized and unidentified persons attempting to gain access to the facility.	There are written procedures for challenging unauthorized or unidentified persons that have gained or are attempting to gain access.	In addition, procedures are enforced and unauthorized or unidentified individuals are detained.
SECTION 4.0 INFORMATION TECHNOLOGY SECURITY				
Password Protection: Automated systems MUST use individually assigned accounts that require a periodic change of password. IT security policies, procedures and standards MUST be in place and provided to employees in the form of training.				
Section	**Security Measures**	**Fails Requirements = 0**	**Meets Requirements = 1**	**Exceeds Requirements =**
4.1	Does the company have IT security policies and procedures in place?	The company does not have IT security policies and procedures in place.	The company has IT security policies and procedures in place. IT personnel provide policy training to all relevant employees.	In addition, a signed copy of the policy is held in the employees' personnel file.
4.2	Are all automated systems assigned individual accounts that require a periodic change of password?	Not all automated systems are assigned individual accounts that require a periodic change of password.	All automated systems are assigned individual accounts that require a password change once every 90 days.	All automated systems are assigned individual accounts that require a password change once every 30 days.
4.3	Does the company IT security policy cover automatic time-out functions with forced logoffs? Does it also deny user access after a failed number of attempts to log-in?	The company IT security policy does not cover automatic time-out functions with forced logoffs and does not deny user access after a failed number of attempts to log-in.	The company IT security policy covers automatic time-out functions with forced logoffs and denies user access after a failed number of attempts to log-in.	The company IT security policy requires computers to automatically time-out after 15 minutes of idle time and denies user access after three failed attempts to log-in.
Accountability: A system MUST be in place to identify the abuse of IT including improper access, tampering or the altering of business data. All system violators MUST be subject to appropriate disciplinary actions for abuse.				

Scoring Guidelines

4.4	Does the company have a system in place to identify tampering and potential system violators?	The company does not have a system in place to identify tampering and potential system violators.	The company has a system in place to identify tampering and potential system violators. All system violators are subject to disciplinary action.	All system violators are subject to disciplinary action up to and including dismissal. In addition, a table of offenses and subsequent disciplinary action is included in the IT policy signed by employees.
4.5	Does the company have a policy safeguarding computer information?	The company does not have a policy safeguarding computer information.	The company has a policy safeguarding computer information which includes securing all servers and performing a periodic backup of all systems.	In addition, the backup file is stored off-site.

SECTION 5.0 PROCEDURAL SECURITY

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

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

Manifesting Procedures: To help ensure the integrity of cargo, procedures MUST be in place to ensure that information received from business partners is reported accurately and timely.

Section	Security Measures	Fails Requirements = 0	Meets Requirements = 1	Exceeds Requirements =
5.1	Does the company have documented security procedures in place to ensure the integrity and security of processes relevant to the transportation, handling and storage of cargo in the supply chain?	There are no procedures in place.	The company has documented security procedures in place to ensure the integrity and security of processes relevant to the transportation, handling and storage of cargo in the supply chain.	In addition, employees responsible for maintaining cargo security procedures have been trained in those procedures by management and corresponding training records are maintained.
5.2	Does the company have written procedures in place to ensure that manifest information received from business partners is reported accurately and timely?	There are no procedures in place.	Written procedures are in place to ensure that manifest information received from business partners is accurate and timely.	In addition, employees responsible for verifying manifest information have been trained in verification procedures.
5.3	Are procedures in place to control documents that include proprietary company and shipment information?	There are no procedures in place.	There are written procedures in place to control documents that include proprietary company and shipment information. These procedures include keeping such documents in a locked filing cabinet or secure area.	In addition, the duration for keeping documents is defined according to legal regulations.

Scoring Guidelines

Shipping and Receiving: Departing cargo being shipped SHOULD be reconciled against information on the cargo manifest. The cargo SHOULD be accurately described and the weights, labels, marks and piece count indicated and verified. Departing cargo SHOULD be verified against purchase or delivery orders. Drivers delivering or receiving cargo MUST be positively identified before cargo is received or released. Procedures SHOULD also be established to track the timely movement of incoming and outgoing goods.				
5.4	Are drivers required to present photo identification prior to cargo being received or released to/from their custody?	Drivers are not required to present photo identification prior to cargo being received or released to/from their custody.	Drivers are required to present photo identification prior to cargo being received or released to/from their custody. Drivers are further required to log their arrival and departure times, as well as manifest information on the shipment they are delivering or receiving.	In addition, drivers' information and identification are verified by a shipping supervisor.
5.5	Are finished products properly marked, counted, weighed, documented, and reported on the manifest and bills of lading?	Finished products are not properly marked, counted, weighed, documented, and reported on the manifest and bills of lading.	Finished products are properly marked, counted, weighed, documented, and reported on the manifest and bills of lading.	In addition, personnel and policy directives are clear and followed, records are complete and retained.
5.6	Does the company have procedures and security controls in place to track the movement of all departing cargo?	No procedures or controls exist.	Procedures and security controls exist to track the movement of all departing cargo. These procedures include reconciling the goods against the manifest and ensuring they are accurately marked.	In addition, the goods are electronically tracked by bar code or other scanning device.
5.7	Does the company have procedures in place to protect inbound and outbound shipments against un-manifested material being introduced?	There are no procedures in place.	Procedures are in place to protect and verify shipments. They include verifying all goods against the manifest and all pertinent shipping documents.	In addition, employees responsible for maintaining cargo security procedures have been trained in those procedures by management and corresponding training records are maintained.
Cargo Discrepancies: All shortages, overages and other significant discrepancies or anomalies MUST be resolved and/or investigated appropriately. Customs and/or other appropriate law enforcement agencies MUST be notified if anomalies or illegal or suspicious activities are detected.				
5.8	Does the company have written procedures in place to resolve all cargo discrepancies prior to cargo being released or received?	No documented procedures exist.	The company has written procedures in place to resolve all cargo discrepancies prior to cargo being released or received. Those procedures include notifying a security guard or shipping supervisor to investigate as	In addition, a corrective action plan is implemented to prevent further discrepancies.

Scoring Guidelines

5.9	Does the Company have documented procedures to report shortages and overages of cargo to the relevant authorities?	No documented procedures exist.	Documented procedures are in place to notify the appropriate authorities of any cargo discrepancy.	In addition, a corrective action plan is implemented to prevent further discrepancies.

SECTION 6.0 PERSONNEL SECURITY

Processes must be in place to screen prospective employees and to periodically check current employees.

Pre-Employment Verification: Application information such as employment history and references MUST be verified prior to employment.

Section	Security Measures	Fails Requirements = 0	Meets Requirements = 1	Exceeds Requirements =
6.1	Does the company verify the information on employment applications submitted from prospective employees in compliance with federal, state, provincial, and local government regulations and statutes?	Applicant information is not verified at any stage prior to employment.	Management verifies information on applications in compliance with federal, state, provincial, and local government regulations and statutes. Verification results are maintained for the length of employment.	Applicant information is verified with management and an outside security firm in compliance with local law.
6.2	Does the Company interview prospective employees in compliance with federal, state, provincial, and local government regulations and statutes?	Prospective employees are not interviewed.	Prospective employees are interviewed consistent with federal, state, provincial, and local government regulations and statutes. All records are kept in a secure place for the length of employment and may be submitted to the appropriate authority	Additionally, prospective employees undergo several interviews, initially by the personnel department and then by functional department managers.

Background Checks/Investigations: Consistent with foreign regulations, background checks and investigations SHOULD be conducted for prospective employees. Once employed, periodic checks and reinvestigations SHOULD be performed based on cause and/or sensitivity of the employee's position

6.3	Does the Company perform background checks of prospective employees in compliance with federal, state, provincial, and local government regulations and statutes?	No background checks are performed, or are performed at random.	Background checks are performed on all prospective employees in compliance with federal, state, provincial and local government regulations and statutes.	Background checks are performed by company personnel, as well as an outside certified agency.
6.4	Does the Company conduct periodic background checks and/or screen existing employees, in compliance with federal, state, provincial, and local government regulations	No periodic rechecks are performed.	Periodic rescreening of employee background checks are performed on all employees in compliance with federal, state, provincial and local government regulations and statutes.	Periodic rescreening of background checks are performed by company personnel, as well as an outside certified agency.

Scoring Guidelines

6.5	Does the Company perform driving record background checks of existing company drivers?	No background checks are performed. No records of driving violations are kept in the employee files.	Management or security personnel perform background checks. Management and employees regularly review driving records and violations, as required. All related records are maintained in employee files.	In addition, the company sponsors driver training, and training on security related issues to enhance driver awareness and preparedness.
Personnel Termination Procedures: Companies MUST have procedures in place to remove identification, as well as facility and system access for terminated employees.				
6.6	Does the company have documented procedures describing actions to take upon employee separation?	There are no documented procedures.	Documented termination procedures are in place and include the use of a termination/separation checklist.	In addition, an exit interview is performed and personnel folders for all terminated employees are archived.
6.7	Does the Company have processes established for reporting and managing problems related to personnel security?	There are no processes for managing or reporting personnel security problems.	Procedures for managing personnel security problems and recording incidents are in effect.	In addition, all incidents resulting in criminal activity or threats to security are reported to the local authorities.
6.8	Are employees required to sign a Code of Conduct?	Employees are not required to sign a code of conduct.	All employees are required to sign a Code of Conduct.	In addition, training regarding the Code of Conduct is provided annually to employees.
SECTION 7.0 SECURITY TRAINING AND THREAT AWARENESS				
Security Training and Threat Awareness: A threat awareness program SHOULD be established and maintained by security personnel to recognize and foster awareness of the threat posed by terrorists and contraband smugglers at each point in the supply chain. Employees MUST be made aware of the procedures the company has in place to address a situation and how to report it. Additional training SHOULD be provided to employees in the shipping and receiving areas, as well as those receiving and opening mail.				
Additionally: specific training SHOULD be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies and protecting access controls. These programs SHOULD offer incentives for active employee participation.				
Section	**Security Measures**	**Fails Requirements = 0**	**Meets Requirements = 1**	**Exceeds Requirements =**
7.1	Does the company provide security training to employees which includes maintaining cargo integrity, recognizing internal conspiracies and protecting access	There is no security awareness training provided.	The company provides security training to employees which includes maintaining cargo integrity, recognizing internal conspiracies and protecting access	Employees are mandated to attend annual training.

Scoring Guidelines

7.2	Does the company provide threat awareness training by company management or security personnel through routine briefings or memoranda?	There is no training on threat awareness provided.	Company management or security personnel provide threat awareness programs that include up-to-date information on emerging security threats.	Training is mandatory and also includes written materials illustrating important information regarding notifying proper authorities, conducting investigations, and appropriate response. Memoranda are also provided which includes
7.3	Are there written procedures in place instructing employees on recognizing suspicious situations and how to report them?	There are no written procedures in place instructing employees on recognizing suspicious situations and how to report them.	There are written procedures in place instructing employees on recognizing suspicious situations and how to report them.	There are written procedures in place and training on said procedures is provided annually to all employees.
7.4	Is additional training provided to employees in the shipping and receiving areas?	There Is no additional training provided to employees in the shipping and receiving areas.	There Is additional periodic training regarding cargo security provided to employees in the shipping and receiving areas.	Cargo security training is provided to employees in the shipping and receiving areas at orientation and reviewed every six months.
7.5	Is there an incentive scheme in place which encourages staff to report security incidents? Note whether financial or non-financial scheme.	There is no incentive scheme.	There is an incentive scheme to report security incidents. Indicate financial or non-financial.	In addition, there is an appreciation announcement/notice from management published or posted for any employee reporting a security incident.
7.6	Does the Company provide training to employees in detecting fraudulent documentation and computer security?	There is no training provided in detecting fraudulent documentation and computer security.	Training is provided in both detecting fraudulent documentation and computer security.	In addition, the company provides training updates regarding detecting fraudulent documentation and computer security once every six months.

SECTION 8.0 BUSINESS PARTNER REQUIREMENT

Foreign Manufacturers MUST have written and verifiable processes for the selection of business partners including carriers, other manufacturers, product suppliers and vendors. A business partner is any entity doing business with the foreign manufacturer in any capacity. (e.g. parts and raw materials suppliers, distribution centers, foreign forwarders, contracted service providers, etc.)

Security Procedures: For those business partners eligible for C-TPAT certification, the foreign manufacturer MUST have documentation in the form of a Status Verification Interface (SVI) number indicating whether these business partners are or are not C-TPAT certified.

For those business partners not eligible for C-TPAT certification, the foreign manufacturer MUST require that their business partners demonstrate that they are meeting C-TPAT security criteria via written/electronic confirmation. This can be accomplished through a contractual obligation or a completed and signed security questionnaire. Based upon a documented risk assessment process, non-CTPAT eligible business partners MUST be subject to verification of compliance with C-TPAT security criteria by the foreign manufacturer.

Section	Security Measures	Fails Requirements = 0	Meets Requirements = 1	Exceeds Requirements =

Scoring Guidelines

8.1	Does the company have a documented risk based process in place for the selection of all business partners?	No internal documented risk based process is in place for the selection of business partners.	The company has a documented risk based process in place for the selection of all business partners. Internal requirements should include financial soundness (e.g. credit check, bank reference, annual report) and the capability of meeting contractual	Business partner evaluations include financial soundness, capability of meeting contractual security requirements and the ability to identify security deficiencies. The company also has an internal management team that determines internal risk assessment
8.2	If the auditee is a CTPAT member, is a SVI number requested and periodically verified for those business partners eligible for C-TPAT?	A SVI number is not requested and/or periodically verified for those business partners eligible for C-TPAT.	A SVI number is requested and periodically verified for those business partners eligible for C-TPAT.	A SVI number is requested and verified once every 30 days.
8.3	Does the company require service providers to complete a security questionnaire or provide evidence of their security procedures ensuring compliance with C-TPAT minimum security	The company does not require service providers to complete a security questionnaire or provide evidence of their security procedures ensuring compliance with C-TPAT minimum security	The company does require service providers to complete a security questionnaire or provide written security procedures confirming compliance with C-TPAT minimum security	The company evaluates the service providers written security procedures annually and makes recommendations to improve any security deficiencies.
8.4.	Do contracts with vendors and service providers address compliance with C-TPAT minimum security standards?	Contracts with vendors and service providers do not address C-TPAT minimum security standards.	Written contracts specify that C-TPAT minimum security standards are required and maintained for all vendors and service providers.	The company requires each vendor and service provider comply with the C-TPAT minimum security standards. Vendor and service provider contracts stipulate penalties or sanctions if C-TPAT minimum security standards are not met.
8.5.	Does the Company maintain a list of all service providers by name, type of service provided, address of physical office location, telephone number, faxes number, email, and	No lists are maintained.	List is maintained.	List is maintained and details are updated periodically.

Point of Origin: Foreign manufacturers MUST ensure that business partners develop security processes and procedures consistent with the C-TPAT security criteria to enhance the integrity of the shipment at point of origin, assembly or manufacturing. Periodic reviews of business partners' processes and facilities SHOULD be conducted based on risk and SHOULD maintain the security standards required by the foreign manufacturer.

Scoring Guidelines

8.6	Does the company have a documented and verifiable risk analysis procedure for determining appropriate security measures throughout their supply chain based on its business model? (e.g. volume, country of origin, routing, terrorist threat)	There is no documented risk analysis procedure.	There is a documented procedure in place with records to provide evidence that all business partners have been included in the risk assessment.	In addition, evidence is available to show that documented corrective action was taken in cases where risk was elevated. Semi-annual reviews are also conducted.
8.7	Does the company conduct security assessments of areas under their internal control within the supply chain?	No security assessments are conducted.	The company conducts security assessments and evidence in the form of a checklist or report is available.	In addition, evidence is available to show that documented corrective action was taken in cases where risk was elevated.
8.8	Does the company have documented procedures and security controls in place for service provider audits?	No service provider audits are conducted.	Service provider audits are conducted and documented.	In addition, service provider audits are accompanied by written mutually agreed upon improvement plans.
Participation/Certification in a Foreign Customs Administration Supply Chain Security Program: Current or prospective business partners who have obtained a certification in a supply chain security program being administered by a foreign Customs Administration SHOULD be required to indicate their status of participation to the foreign manufacturer.				
8.9	Does the company participate in a supply chain security program administered by a foreign Customs Administration?	The company does not participate in a supply chain security program administered by a foreign Customs Administration.	The company does participate in a supply chain security program administered by a foreign Customs Administration.	The company does participate in a supply chain security program administered by a foreign Customs Administration and has documentation to prove the level of participation in said program.
Security Procedures: On U.S. bound shipments, foreign manufacturers SHOULD monitor that C-TPAT carriers that subcontract transportation services to other carriers use other C-TPAT approved carriers or non-C-TPAT carriers that are meeting the C-TPAT security criteria as outlined in the business partner requirements.				
8.10	Does the company require that all sub-contracted partners within the supply chain maintain C-TPAT minimum security criteria?	The company does not require that all sub-contracted partners within the supply chain maintain C-TPAT minimum security criteria.	The company requires that all sub-contracted partners within the supply chain maintain C-TPAT minimum security criteria.	The company requires that sub-contracted carriers sign a contract committing to C-TPAT minimum security criteria and stipulate penalties if standards are not met.