SCI PHILIPPINES	Management Systems		Corporate Policy
Document Title:	CTPAT Procedures	Document Number:	SCI-QP-017
Effectivity Date:	July 12,2022	Revision Number:	010
Prepared By:	Roger Batiancila – Compliance Auditor	Revision Date:	July 10,2022
Reviewed By:	Amelita Faro – Compliance Manager Armond Garcia – EHSS Manager	Number of Pages:	74
Approved By:	Vickie Rose Orpilla – Central HR Manager Malou Pacres – Central HR Manager Annie Sy – Central HR Manager Edna Esguerra – Central HR Manager Dino Cordova – Factory Manager MAI Cris Birao – Factory Manager MWI Romil Cabahug – Factory Manager FAC Jayson Chou – Factory Manager GMI Ian Celestial – VT1 Factory Manager Sade Yeh – Sample Room Manager Vincent Lee – Project Manager Cando Yeh – Finance Manager		

REVISION LOG

Revision	Effectivity	Description of Change	Change	Approval
00	August 01, 2011	Initial Release		Edna Esguerra Vickie Rose Orpilla
01	March 1, 2012		Venia D. Alcordo	Edna Esguerra Vickie Rose Orpilla

02	October 16, 2012	**Physical Access Control – item #4 Threat Awareness Program** *Annual conduct of orientation and training to all employees and Security Guards **Personnel Security – item #2 Periodic Checks and Reinvestigation** *2.2 Annual update of all employees' information **Procedural Security – item #1 Contractor's / Supplier's Consideration** *1.4 Conduct annual check and background investigation for contractor's personnel. *1.5 Quarterly conduct of contractor's internal security assessment *1.6 Company to conduct semi-annual announced / unannounced site security assessment to contractors. **Item #6 Receiving** *Take out 17 point inspection for truck and container security checklist	Malou P. Pacres Venia Alcordo	Edna Esguerra Vickie Rose Orpilla
03	September 01, 2013	**Contractor's/Supplier's Consideration** *Change security assessment done by contractor from quarterly to annual *Change announced/unannounced security assessment done by the factory from semi-annual to annual	Malou P. Pacres Venia Alcordo	Edna Esguerra Vickie Rose Orpilla

04	February 01, 2014	**Procedural Security- Contractor's/Supplier's Consideration** ***** 1.2 Selected contractors/suppliers, freight forwarders, trucking companies and security guards are given an orientation of the security standards of the company and are provided with a copy of the standards upon the signing of contract with the company and with the binding contract would mean the contractors/suppliers commitment to abide by the company's security standards. And by so doing /suppliers, freight forwarders, trucking companies and security guards must provide copies of their security policies, including physical security, access control, cargo handling, and others related to the C-TPAT standards. ***** All contractors' employees (canteen, forwarders and trucking companies, Security Guard and others) with access to the factory or restricted areas shall undergo annual check and background investigation to verify community standing. ***** Company should conduct announced / unannounced annually site security assessment to all contractors (canteen, forwarders and trucking companies, Security Guard and others) with access to the factory or restricted areas. **Documentation Processing** ***** All materials for transport to facilities like MWI, MWI2, MAI, MAI2, FAC, and FAC2 are documented using Transfer Slip and all materials for transfer to GMI and GMI2 are documented using Transfer Slip and PEZA 80112.	Luz Soriano Florecita Estella Joren Magbanua	Vickie Rose Orpilla Jane Chu

04	February 01, 2014	**Receives and Check Seals** **FCL** 6.2.1 Shipping seal are received by the Team Leaders from the shipping lines through the trucking service who delivers the empty container. 6.2.2 Dispatch Team Leader checks and verify the shipping seal number, if it coincides from the mail advice provided by the forwarder, to the actual received. 6.2.3 All unused FCL shipping seals are to be returned to the forwarder. **LCL** 6.2.1.1 Shipping seal is received from our purchasing department by the Dispatch Team Leader. 6.2.1.2 Dispatch Team Leader will double check the quantity and the sequence for the seal number. 6.2.1.3 If shipping seal does not coincide as advised, Dispatch Team Leader will inform the Finished Goods Manager regarding the discrepancy. The Finished Goods Manager reports the discrepancy to the forwarder and asks for the correct seal. 6.2.1.4 If the integrity of the shipping seal has been compromised. Dispatch Team Leader will inform immediately to the Finished Goods Manager regarding the problem. The number of the compromised seal is duly recorded.	Luz Soriano Florecita Estella Joren Magbanua	Vickie Rose Orpilla Jane Chu
05	February 01, 2014	Finished Goods Manager will inform the forwarder for the problem and immediately request for a replacement. For LCL seal, the Finished Goods Manager will inform purchasing department for the discrepancy. Records the damaged seal and ask replacement from supplier.	Luz Soriano Florecita Estella Joren Magbanua	Vickie Rose Orpilla Jane Chu

05	February 01, 2014	**Recording and Releasing of Seal *** 6.2.2.1 The Dispatch Team Leader records the FCL and LCL shipping seal number once the shipping seal has been checked for its quality, in the container/security seal log book. *6.2.2.2 Recorded and received shipping seal for both FCL and LCL will only be released, once the container and the truck respectively are already full and ready for sealing. *6.2.2.3 The released FCL and LLC shipping seals are recorded in the container/security seal log book, duly signed by the Finished Goods Associate who receives the seals.	Luz Soriano Florecita Estella Joren Magbanua	Vickie Rose Orpilla Jane Chu
06	February 01, 2014	**Container Storage and Loading** *6.3.2 Only authorized Finished Goods personnel are allowed in the container loading area. *6.3.3 All authorized personnel must always wear their ID badge and access at all times for easy identification and security protection. *6.3.4 Personnel with no ID badge in the loading area must be asked to exit the area and will be subject for investigation.	Luz Soriano Florecita Estella Joren Magbanua	Vickie Rose Orpilla Jane Chu

06	February 01, 2014	**Releasing-Central Warehouse** *7.1.1 All imported materials transferred to facilities shall be monitored upon loading and padlocked upon completion *7.1.2 All imported materials transferred to facilities shall be documented by transfer slip and PEZA 80112 form verified by dispatch guard and close vehicle for transfer; **Finished Goods-Carton Transfer** *7.1.1.1 Empty close vans are padlocked and will proceed to pick up cartons from factories *7.1.1.2 Security guards assigned in the factory will open the empty close vans and forklift operators will start hauling the cartons to the van. *7.1.1.3 Filled vans are then padlocked by the security personnel (keys of the van are kept by the security personnel of each factory and Finished Goods). *7.1.1.4 All carton transfers are being document by Transfer Slip stating the Purchase Order number of the cartons transferred. **Changes under : Cargo Conveyance** ***8.1 Record Container and Truck number** ***8.2 Cargo Examination** ***8.3 Monitoring of Cargoes** **: Cargo Discrepancy** ***9.1 Pilferage Reporting from Forwarders/ Contractors**	Luz Soriano Florecita Estella Joren Magbanua	Vickie Rose Orpilla Jane Chu

07	February 01,2019	**6. Alarm systems and Video Surveillance Cameras** 6.4. Change keeping of CCTV footage from 60 to 180 days **7. List of employees access privilege** Adding some areas are the ff. 7.4.4 PPIC 7.5.5 MD room 7.6.6 QC office 7.7.7 All area **8. Internal/External Communication** 8.1.3. Changes made > Incident logbook to Daily Occurrence Book > Incident logbook to incident report **Physical Access Control** **1. Security Guards' Specific Training and Orientation** **>** Change ID badge to company ID > Change from Department to section **Personnel Security** **1 . Periodic check and back ground investigation** Added 2.1. Updated list of employees in sensitive positions should be reviewed in annual basis or as need arises **Personnel Termination Procedure** Added statement @ 3.2.1.3 while for AWOL (4 times and last notice will be the termination notice **Lost Identification Badges** 4.3. Change sending of list of lost ID from monthly to every occurrence **Information Technology Security** **4. Accountability** Added 4.3 the facility should regularly	Roger Batiancila	Amelita Faro Cando Yeh

08	February 20,2020	From HR department/HR manager to EHSS department/ assistant EHSS manager **Physical Security** **A.** Borrowed facility keys should be returned 1 hour after opening and closing of the facility **B.** Security personnel will call out the attention of the personnel who borrowed key that will not return the keys with in 1hr. and conduct investigation and issue incident report. **C.** Inventory of facility keys should be conducted daily by the security personnel 1. **Fencing:** Perimeter fencing at least 6 feet high with outward -facing barbed wire on top should enclose the areas around cargo handling and storage facilities. 1.1.6.7. Orange for inspection 1.1.9. Daily inventory of access pass should be conducted by the security personnel **D.** Vehicles Vehicles entering/ exiting the factory premises will be inspected with an under chassis mirror and driver or passenger going inside the facility will be checking thru metal detector by factory security to ensure that no firearms or other weapons are brought in the factory. **Physical access control** IT access like password shall be deactivated by the IT In-Charge upon separation of employment after asking the confirmation from the department heads **Personnel security** 2.4 Positions e.g. All factory,	Roger Batiancila	Amelita Faro Cando Yeh

		Procedural Security 6.1. Monthly inventory of shipping seals, PEZA seals and metal seals should be conducted by the authorized logistics personnel		
09	September 15,2020	**1. OBJECTIVES** Deleted 1.5. It shall be the responsibility of the Factory Manager, HR Manager and Assistant EHSS Manager of the facility to ensure all Security Procedures are strictly implemented; furthermore Compliance Manager shall ensure and verify effectiveness of Security Procedures in the different facilities. Added the following: 1.1. To provide highest level of cargo security and properly document the requirements set by the Customs-Trade Partnership against Terrorism (C-TPAT). 1.2. To prevent security threats and possible acts of terrorism in the facility 1.3. To ensure a more secure and expeditious supply chain to employees, suppliers, customers or business partners 1.4. To ensure integrity of the security practices and understanding of the employee related to CTPAT procedures	Roger Batiancila	Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**2. SCOPE** ○ Change Policy to Procedures ○ Deleted SCI Cebu Philippines ○ Added Procedures and Business Partners **3. Responsibility** Deleted ○ The management of the facility and compliance team shall be the responsible for the implementation of this procedures Added the following ○ 3.1. Factory manager shall be the responsible to oversee the security of the facility and will review and approved necessary request in compliance to CTPAT requirement ○ 3.2. Assistant EHSS manager/supervisor shall assist factory manager to oversee the security of the facility and to monitor compliance to CTPAT requirements ○ 3.3. EHSS manager and Compliance manager shall review the procedure for its adequacy and applicability to use ○ 3.4. Security officer shall be the responsible person for the implementation and maintain all records related to CTPAT ○ 3.5. HR manager shall be the responsible person to ensure CTPAT related documents for HR department ○ 3.6. Compliance team shall be responsible to verify the effectiveness of the implementation of this procedure De		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**4. DEFINITIONS** Added the following ○ 4.3. **IDS** – Intrusion Detection System ○ 4.4. **EPASS** – Electronic Pass Access Security System ○ 4.5. **LCL** – Less-than Container Load ○ 4.6. **FCL** – Full Container Load ○ 4.7. **Risk Assessment** – Identify, Analyze, Eliminate/mitigate or manage security threats and/or Vulnerabilities in the facility ○ 4.8. **Business Partners** – Elements of its international supply chain and to ensure that sound security Measures are in place and adhered to in order to achieve an effective secure supply chain globally ○ 4.9. **IIT** – Instrument of International Traffic ○ 4.10. **TS** – Transfer Slip ○ 4.11. **IPPC** – International Plant Protection Convention ○ 4.12. **ISPM** – International Standard for Phytosanitary Measures ○ 4.13. **PAS/ISO** - the standardized document that establishes "uniform procedures for the classification, Acceptance, and withdrawal of mechanical freight container seals. It provides a single Source of Information on mechanical seals which are acceptable for securing freight Containers in international Commerce ○ 4.14. **CFS** – Container Freight Station ○ 4.15. **CIP** – Carriage and Insurance Paid		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 4.14. **CFS** – Container Freight Station ○ 4.15. **CIP** – Carriage and Insurance Paid ○ 4.16. **Cyber Security** - The practice of defending computers, servers, mobile devices, electronic Systems, Networks, and Data from malicious attacks. It's also known as information technology Security or Electronic Information security. ○ 4.17. **Seal Security** - Tamper evident mechanisms used to seal cargo in transit shipping containers in A way that provides tamper evidence and some level of Security. Such seals can help to detect Theft or contamination, either Accidental or deliberate. ○ 4.18. **Procedural Security** - Protection against manifested material being introduced into the supply Chain. Supervised introduction/removal of cargo, the proper marking, weighing, counting and Documenting of Cargo/cargo equipment verified against manifest documents, the Detecting/reporting of Shortages/overages, and Procedures for verifying Seals on containers, Trailers, And railcars. The Movement of incoming/outgoing goods should be monitored 4.19. **Physical Security** – Security of the facility including perimeter fences, locking devices on external		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou

09	September 15,2020	○ 4.20. **Physical Access Control** - Controls of positive identification to all employees, visitors, And vendors including Challenging unauthorized/unidentified persons ○ 4.21. **Personnel Security** – An employment screening and interviewing of Prospective employees to Include periodic Background checks and application verifications ○ 4.22. **Education, Training and Awareness** - An awareness program to employees including recognizing internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized Access. These programs should encourage active employee participation in security controls ○ 4.23. **Conveyance Security** - Physical search of all readily accessible areas, the securing all Internal/external compartments and panels as appropriate, and procedures for reporting cases in Which unmanifested materials, or signs of tampering, are discovered ○4.24. **Agricultural Security** - preventing contamination from foreign animal, plant or any organic Material		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**5. PROCEDURES** Added the following ○ **1. Security Vision and Responsibility** ○ **1.1.** To become and remain effective CTPAT Member's supply chain, it must have the support of a company's upper management. Instilling security as an integral part of a company's culture and ensuring that it is a companywide priority is in large part the responsibility of the company's leadership. ○ **1.**2. The factory manager and EHSS manager shall be the responsible person for the security of the facility ○ **1.**3. It is also part of their duties and responsibilities to have a full support and commitment to the following; ○ **1.**3.1. Promoting a work culture of security ○ **1.**3.2. Building a robust supply-chain security program ○ **1.**3.3. Creating a written and documented program ○ **1.**3.4. Having a team knowledgeable of the CTPAT program and its requirements		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**2. Risk Assessment** ○ 2.1. The continuing threat of terrorist groups and criminal organizations targeting supply chains underscores the need for Members to assess existing and potential exposure to these evolving threats, It should focus on geographical areas/supply chains that have higher risk. ○ 2.2. Assistant EHSS manager/supervisor and Security officer should establish a Risk Assessment ○ 2.3. When determining risk within their supply chains, It must consider various factors such as the business model, geographic location of suppliers, and other aspects that may be unique to a specific supply chain ○ 2.4. Risk assessment should include the following; ○ 2.4.1. Identify security threats and vulnerabilities in the facility and its supply chain ○ 2.4.2. Analyze security threats and vulnerabilities based on the frequency and Consequences of the risk ○ 2.4.3. Control risk: mitigate, eliminate or manage risks 2.4.4. Provide action plan to every security threats and vulnerabilities ○ 2.5. Risk assessment shall be approved by EHSS manager and Factory manager. It must be Updated if necessary.		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 2.6. EHSS manager and assistant EHSS manager/Supervisor should established a recovery planning for ○ 2.6.1. Crisis management, Business continuity, Security recovery or Business resumption ○ 2.6.2. Factory managers, sustainability manager and regional factory manager Shall approve and review the document ○ 2.6.3. Security officer should retain copy of recovery planning for Crisis management, Business continuity, Security recovery or Business resumption and Risk Assessment **3. Business Partners Security** ○ 3.1. Security officer in the facility shall keep and maintain an updated list of its business Partners related to CTPAT ○ 3.2. Business partners should be the following; ○ 3.2.1. Product supplier (Cartons/Seals/Packaging tape, Seals and etc.) ○ 3.2.2.Transportation/Logistics provider ○ 3.2.3. Brokers/Customs brokers ○ 3.2.4. IT providers ○ 3.2.5. Security Agency and Canteen concessionaire ○ 3.2.6. Security Technology, Maintenance and repair service provider (CCTV/EAC/IDS) ○ 3.4.4. Binding Contract ○ 3.5. List of personnel who have regular access/transaction to the facility of identified business partners Should be in place		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 3.7. Identified business partners must submit their annual self-assessment to security officer Except for canteen Concessionaire and security agency that will be monitor by Compliance Department on the 1st month of the year ○ 3.8. Once received the self-assessment result, security officer will then send to compliance supervisor For uploading to portal ○ 3.9.2. Security Technology service provider and maintenance (IDS) – Security Officer ○ 3.9.3. Security Technology service provider and maintenance (EAC/CCTV) – IT department ○ 3.9.4. IT providers and maintenance – IT department ○ 3.9.5. Supplier (Cartons/Seals/Packaging tapes/Metal Seals) – FG Security officer ○ 3.9.6. Transportation/Logistics providers – FG personnel ○ 3.9.7. Supplier (Shipping and PEZA Seals) – Shipping department ○ 3.9.8. Brokers/Customs broker – Shipping department ○ 3.10. Security officer should kept records of annual self-assessment and on-site inspection of Business partners ○ 3.11. Business partners must provide copies of their security policies, including physical Security, access control, cargo handling, and others related to the C-TPAT standards		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 3.12. Security officer must conduct annual orientation of CTPAT procedures to all business Partner's representative and provide them a copy of CTPAT procedures and in every update ○ 3.13. Received/signed copy of CTPAT procedures by the business partners should be available **4. Cyber Security** **4.1. Written Policies and Procedures** ○ 4.1.1. The facility through IT personnel should have established IT policy and Procedures ○ 4.1.2. This should be approved by IT manager, Factory managers and Central HR managers ○ 4.1.3. Cyber Security policy and procedures must cover below aspects ○ 4.1.3.1. Responsibilities and duties ○ 4.1.3.2. Hardware and Software ○ 4.1.3.3. User access management ○ 4.1.3.4. Operational Security ○ 4.1.3.5. Backup and recovery ○ 4.1.3.6. Employees/contractor disciplinary policy for IT violations **4.2. Hardware** ○ **4.2.1. Server Central Control** ○ 4.2.1.1. All servers/IT rooms must be physically secured ○ 4.2.1.2. They shall be protected against safety and environment concern ○ 4.2.1.3. IT personnel should conduct daily temperature checking in server room/IT Rooms ○ 4.2.1.4. Server room/IT room should be in a maximum limit of		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	temperature w/c is 27.50C ○ 4.2.1.5. Records of temperature checking should be kept at least 1 year by IT personnel ○ 4.2.1.6. Server room/IT room must equipped with fire extinguisher ○ 4.2.1.7. Monthly inspection of fire extinguisher should be conducted by the safety Officer or electricians ○ 4.2.1.8. Records of fire extinguisher inspection should be kept at least 1 year by the Safety officer ○ 4.2.1.9. Server room should always be kept safe, neat and tidy **4.2.2. Network Setting** ○ 4.2.2.1. To prevent access to internet on all workstations in the Facility, all computers Must be physically blocked or disabled through software (except for Authorized personnel) ○ 4.2.2.2. Network setting must equipped with anti-intrusion hardware ○ 4.2.2.3. IT personnel shall maintain and kept IT access list of employees /list of computer users who are allowed to access information systems e.g. email, intranet, internet, Skype and other management Program and system ○ 4.2.2.4. IT access list shall be updated as need arises (if have newly hired computer users and separated computer users) ○ 4.2.2.5. List of employees allowed to access internet and Skype should be taken from IT access list and updated monthly		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 4.2.2.6. Issued Skype should be a business Skype (with end to end encryption) ○ 4.2.2.7. IT access list and Monthly list of employees allowed to access internet and Skype must be signed by IT personnel and approved by IT manager ○ 4.2.2.8. Employees allowed to access internet and Skype must have the approval from Department heads through accomplished internet application. ○ 4.2.2.9. Internet application must be completely signed by department managers and IT managers ○ 4.2.2.10. Record should be kept by IT personnel **4.2.3. Wiring** ○ 4.2.3.1. Cables, equipment and electrical wiring should be safely installed in order to Eliminate any kinds of employee accidents, data loss and fire accidents **4.2.4. Terminal Units** ○ 4.2.4.1. IT manager shall be the responsible person and should be knowledgeable in server or terminal units, ○ 4.2.4.2. Should be then received letter of appointment (LOA) given by security officer		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**4.2.5. Regularly Maintained** ○ 4.2.5.1. Technology components or software and network components should be check Monthly by the IT personnel ○ 4.2.5.2. Records should be kept at least 1 year **4.2.6. Media and Mobile Working Units** ○ 4.2.6.1. To prevent and block unauthorized data transfers, transfer ports on all Workstations in the facility, all computers must be physically blocked or disabled Through software (except for authorized Users) ○ 4.2.6.2. List of employees allowed to access USB flash drive should be taken from IT access list and updated monthly ○ 4.2.6.3. Monthly list of employees allowed to access USB flash drive must be signed by IT personnel and approved by IT manager ○ 4.2.6.4. Employees allowed to access USB flash drive must have the approval from Department heads through accomplished USB flash drive application. ○ 4.2.6.5. USB flash drive application must be completely signed by department managers and IT managers ○ 4.2.6.6. Record should be kept by IT personnel		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**4.3. Software** ○ 4.3.1. Software use must be license ○ 4.3.2. It department shall secure and retain software license from service provider ○ 4.3.4. All computers must be secured or prohibited from installation of unapproved software ○ 4.3.5. IT personnel should conduct monthly vulnerability scans and penetration test ○ 4.3.6. If found or noted any vulnerabilities, actions must be taken ○ 4.3.7. Records must be keep at least 1 year by the IT personnel **4.4. Access Control** ○ 4.4.2. Password must not be shared and post in public for prevention of unauthorized access to computer ○ 4.4.3. All user computer passwords should be highly secure, following these guidelines ○ 4.4.3.1. Minimum password length: (8) characters ○ 4.4.3.2. Complexity requirements ○ 4.4.3.3. No reuse of three (3) most recent passwords ○ 4.4.3.4. Permanent account lockout (requiring administrator override) after five (5) failed Log in attempts ○ 4.4.6. Annual training or orientation to all computer users shall be conducted by IT department		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 4.4.7. Training record/system generated attendance shall be kept by IT personnel and training personnel at least 1 year **4.5. Regular Meeting** **4.6. Back up Recovery and Disposal** ○ 4.6.1. System and Data should be back up in a weekly basis by the IT personnel ○ 4.6.2. Back up must be made offsite or to other area not located in the facility ○ 4.6.3. All sensitive and confidential data are stored in an encrypted format or protected by Password ○ 4.6.4. All data storing in any used and discarded storage devices, including but are not Limited to hard disk, flash drive, CD/DVD laser discs, magnetic tapes should be erased Completely and disposed of properly ○ 4.6.5. Record must be keep at least 1 year by IT personnel **5. Conveyance and International Traffic Instrument (IIT) System** **5.1. Container/Trailers or any IIT Storage and Monitoring** ○ 5.1.2. Added security personnel authorized in loading area ○ 5.1.4. Loading area or Containers/trailer or any IIT storage parking area should have posted Warning signs e.g. authorized personnel only and list of Authorized personnel ○ 5.1.7. Loaded or empty containers or any IIT storage must be keep locked//sealed for overnight Staging by the FG personnel		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**5.2. Container/Trailer/Other IIT Inspections** ○ 5.2.1. The facility through the FG manager/supervisor should have established procedures on container/trailer/other IIT inspection ○ 5.2.2. Added Pest contamination checking for container/trailer inspection ○ 5.2.3. Inspection shall be conducted by Security guard together with FG personnel ○ 5.2.4. 17 points inspection checklist must contain agricultural security with separate pest Contamination checklist ○ 5.2.5. Seventeen (17) points inspection should cover the ff; ○ 5.2.5.1. Bumper ○ 5.2.5.2. Engine ○ 5.2.5.3. Tires (truck and trailer) ○ 5.2.5.4. Floor (inside truck) ○ 5.2.5.5. Fuel tanks ○ 5.2.5.6. Cab/storage compartment ○ 5.2.5.7. Air tanks ○ 5.2.5.8. Drive shafts ○ 5.2.5.9. Fifth Wheel ○ 5.2.5.10. Outside/under carriage ○ 5.2.5.11. Outside/inside doors ○ 5.2.5.12. Floor (inside trailer) ○ 5.2.5.13. Side wall ○ 5.2.5.14. Front wall ○ 5.2.5.15. Ceiling/Roof ○ 5.2.5.16. Refrigeration unit ○ 5.2.5.17. Exhaust		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 5.2.6. Seven (7) points inspection should cover the ff; ○ 5.2.6.1. Front wall ○ 5.2.6.2. Left Side ○ 5.2.6.3. Right Side ○ 5.2.6.4. Ceiling/Roof ○ 5.2.6.5. Inside/Outside door and locking mechanism ○ 5.2.6.6. Outside/Undercarriage ○ 5.2.6.7. Floor ○ 5.2.7. Pest contamination checking criteria should include the ff; ○ 5.2.7.1. Visible traces of animals, insects, or other invertebrates – dead or alive, in any Lifecycle stage, eggs or rafts ○ 5.2.7.2. Any organic materials of animal origins – blood, bones, hair, flesh, secretions, Excretions ○ 5.2.7.3. Viable or non-viable plants or plants products – fruits, seeds, leaves, twigs, roots, Barks ○ 5.2.7.4. Other organic materials i.e. fungi, soil or water that may cause contamination by Organic mates ○ 5.2.8. Inspection records shall be send to consignee prior to receiving the merchandise ○ 5.2.9. Any discrepancies found during inspections shall be reported to FG manager/supervisor ○ 5.2.10. Corrective action should be in place to address and mitigate issues ○ 5.2.11. FG manager or supervisor should conduct random inspections to make sure the Procedure is being followed		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**5.3. Record Keeping** ○ 17 and 7 points inspection, pest contamination inspection, corrective action and random Inspection result should be keep 1 at least 1 year by FG supervisor/manager **6. Seal Security** **6.1. Seal Security Procedure** **6.1.1. Receiving and Checking of Seals** **6.1. Seal log and record keeping** ○ 6.2.6. Added access only by the authorized personnel in securing of seals ○ 6.2.8. Inventory record must be keep at least 1 year by shipping personnel and dispatch team Leader ○ 6.2.9. Seal number shall be electronically printed on the shipping documents 6.3. **Seal Requirements** ○ 6.3.2. Shipping manager/supervisor and FG manager and supervisor must ensure to secure Certificate from the seals manufacturer/provider to ensure seals meet the standard ○ 6.3.3. Only seals rated as "high security seals" can be used for shipment bounds to US ○ 6.3.4. Security seals must equipped with unique serial number ○ 6.3.5. Seals must have manufactures name or logo indicated on seals and have mark or Stamp to identify its classifications as high security ○ ('H) (preferable)		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**7. Procedural Security** **7.1. Protection of Cargo** **7.1.1. Empty Container** ○ 7.1.1.1. Added pest contamination checking for container/trailer inspection ○ 7.1.1.2. Inspection shall be conducted outside or before entering the facility perimeter ○ 7.1.1.3. Added pest contamination checking for inspection of container/trailer replacement **7.2.2. Loading Process of Finish Goods for Shipment** ○ 7.2.2.2. Proceed to loading of finish goods ○ 7.2.2.3. Loading activity should be monitored and supervised by security personnel, dispatch team leader and FG supervisor ○ 7.2.2.4. There should be no unauthorized personnel present at loading area during loading activity ○ 7.2.2.5. If loading area in the factory is not enclosed with gate, a need to provide barriers/barricade upon loading activity ○ 7.2.2.6. Dispatch team leader or FG supervisor should take pictures during loading process and affixing of seals to container ○ 7.2.2.7. Pictures take of the ff; ○ 7.2.2.7.1. Cargo markings (carton mark/crate mark, etc.) ○ 7.2.2.7.2.Loading process – empty, half, 2/3 and finish loading ○ 7.2.2.7.3. Seal affixing and close up image where the seals has been affixed and where seal number clearly appear ○ 7.2.2.7.4. Finish loading and closing a door		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**7.2.3. How to affix seal security** ○ 7.2.3.1. FG team leader in the presence of FG manager/supervisor and security personnel will be the responsible Person to affix the seal to container/ other IITs ○ 7.2.3.2. When affixing security seal, must follow seal VVTT process are the ff; ○ 7.2.3.3. View the seal and container locking mechanism, and ensure they are in good working condition. ○ 7.2.3.4. Report to FG supervisor/manager of found damage/broken or other discrepancies noted ○ 7.2.3.5. Verify seal numbers for accuracy. Compare with shipping documents and look for alterations to seal numbers ○ 7.2.3.6. Tug on the seal to make sure it is affixed firmly. Seals that come apart must be reported to FG manager/supervisor ○ 7.2.3.7. Twist and turn seal to make sure its components do not unscrew or separate from one another ○ 7.2.3.8. Authorized personnel who affixed the security seal must have proper training ○ 7.2.3.9. Training record must be keep by FG supervisor at least 1 year **7.5. Monitoring of Cargoes** ○ 7.5.4. Any activity should be closely monitored hourly via GPS system monitored by FG manager, so that any unforeseen illegal activities will be suppressed		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**7.6. Documentations** ○ 7.6.3. Shipping documents shall be sent to consignee prior to receiving the shipment ○ 7.6.4. Documents are verified by the authorized Shipping Supervisors before submission. ○ 7.6.5. All shipping documents and all documents pertinent to business partners CTPAT credentials and use such as reference for selection of business partners shall be safety stored after office hours and keep by shipping supervisor ○ 7.6.6. Record must be keep at least 1 year by FG supervisors and shipping supervisor **7.11. Security Assessment and Improvement Plan** ○ 7.11.4. Audit report and CAP should be monitored by assigned auditor ○ 7.11.5. Record keeping of documents will be kept by compliance supervisor at least 1 year **7.12. Loaded Container or Wing van of Export Raw materials** ○ 7.12.12. If no discrepancies found upon verification of cargo against the packing list, unloading of materials will be proceed **7.15. Delivering of finish goods from Factory to Finish Goods Warehouse** ○ 7.15.2. There should be no unauthorized personnel in loading area during loading activity		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 7.15.3. Loading activity should be barricade to prevent unauthorized access **7.16. Receiving of Finish Goods in Finish Goods Warehouse from Factory** ○ 7.16.5. There should be no unauthorized personnel in loading area during unloading activity ○ 7.16.6. Unloading activity should be barricade to prevent unauthorized access **7.17. Documentation** ○ 7.17.1. Raw Materials – Warehouse material checklist shall be kept by central warehouse team leaders (Original copy) and factory warehouse by warehouse team leaders (copy) ○ 7.17.2. Finish Goods - Transfer slip shall be kept by both factory logistics team leaders and finish goods warehouse receiving team leaders ○ 7.17.3. Records must be kept at least 1 year **7.18. Incident Reporting process** ○ 7.18.5. Added MEM-CHR-013 – Anti-Theft and Pilferage Reward for security incentives ○ 7.18.9. Security officer shall conduct monthly meeting to all security officer ○ 7.18.10. Attendance shall be kept by Security officer at least 1 year		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**8. Agricultural Security** **8.1. Wood Packaging Materials used for Shipment** ○ 8.1.1. The facility should have established fumigation procedure for preventing pest contamination that is in compliance with IPPC and ISPM 15 requirements ○ 8.1.2. Fumigation procedures shall be prepared by FG and shipping supervisors and approved by FG and shipping managers ○ 8.1.3. Wood pallets for finish goods must be fumigated (MB-Methyl bromide) or heat treated (HT) at least once a month ○ 8.1.4. Shipping documents shall include fumigation certificate in every shipment of goods Secured by the shipping supervisor/manager ○ 8.1.5. Shipping supervisor/manager will request/coordinate 3rd party authorized to conduct fumigation during shipment ○ 8.1.6. Sipping supervisor/manager shall kept record of fumigation certificate in every shipment **8.2. Pest contamination Inspection for Pallets** ○ 8.2.1. Finish goods warehouse and logistics warehouse in the factory must conduct pest contamination inspection to wood pallets storing of finish goods by FG and factory logistics warehouse personnel at least once a month		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 8.2.2. Pest contamination checking criteria should include the ff;, insects, or other ○ 8.2.2.2. Any organic materials of animal origins – blood, bones, hair, flesh, secretions, Excretions ○ 8.2.2.3. Viable or non-viable plants or plants products – fruits, seeds, leaves, twigs, Roots, barks ○ 8.2.2.4. Other organic materials i.e. fungi, soil or water that may cause contamination by Organic materials ○ 8.2.3. Records of monthly pest contamination shall be kept by FG supervisors and factory Logistics team leader at least 1 Year **9. Physical Security** **9.1. Fencing and Building** ○ 9.1.1. Exterior perimeter fencing separates the facility to protect against unauthorized access. Alternatively, below are acceptable; ○ 9.1.1.1. Dividing wall ○ 9.1.1.2. Steep Cliff –Dense Thickets ○ 9.1.2. Interior Fencing – Physical fencing enclosed the cargo handling and storage ○ 9.1.3. Domestic, international, high value and hazardous cargo shall be segregated by Physical interior fencing ○ 9.1.4. All fencing and building structures are built with materials that are strongly and not Easy to break to resist unauthorized entry		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**9.3. Lighting** ○ 9.3.2. Lighting shall be equipped with a backup power supply in case of an electrical blackout ○ 9.3.3. Access to power switch panel should be restricted with posted warning signs of authorized personnel only ○ 9.3.4. Lighting turns on automatically/manually as the natural light dims **9.4. Locks and Keys** ○ 9.4.1. Deleted HR Department and replaced Security officer ○ 9.4.2. Security officer shall provide list of authorized personnel allowed to borrowed facility keys including keys to sensitive areas to guard house and must be updated in every changes ○ 9.4.3. Keys master list should be made available at guard station ○ 9.4.8. Deleted HR Department and replace EHSS department when reporting stolen keys **9.5. Security Technologies** ○ 9.5.1. Security technology should be utilized to monitor activities inside and outside, detection and prevention of unauthorized entry to sensitive areas this may include but not limited to : ○ 9.5.1.1. Finish goods storage ○ 9.5.1.2. Shipping and receiving areas ○ 9.5.1.3. Shipping office ○ 9.5.1.4. HR office ○ 9.5.1.5. IT server/room ○ 9.5.1.6. Inspection room ○ 9.5.1.7. Logistics warehouse/office ○ 9.5.1.8. PPIC		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 9.5.1.9. MD room ○ 9.5.1.10. QC office ○ 9.5.1.11. Loading/dispatch area ○ 9.5.1.12. Washlab ○ 9.5.1.13 Outside and facility perimeter the facility to monitor activities both inside And outside the facilities ○ 9.5.2. The security technology here may refer to ○ 9.5.2.1. CCTV ○ 9.5.2.2. IDS ○ 9.5.2.3. EAC ○ 9.5.3. General requirements for security technology ○ 9.5.3.1. Security officer shall ensure that only certified equipment are installed ○ 9.5.3.2. Security officer shall ensure to secure certificate from service providers and Maintenance of security technology ○ 9.5.3.3. Inspection of security technologies should be conducted monthly by the ff; ○ 9.5.3.3.1. CCTV/EAC – IT personnel ○ 9.5.3.3.2. IDS – Security officer ○ 9.5.3.4. Responsible to conduct inspection to security technology must be Knowledgeable and received training in particular ○ 9.5.3.5. Training record must be kept by security officer ○ 9.5.3.6. Access to security technology should be restricted to authorized personnel only ○ 9.5.3.7. UPS backup for a minimum of four (2) hours (or one (1) hour if backup power Generator is in place		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**9.8. Electronic Access Control** ○ 9.8.1. Electronic Access Control system should be provided to sensitive areas to prevent unauthorized entry ○ 9.8.2. IT personnel should review EAC logs week and send to department heads weekly for review ○ 9.8.3. Any abnormalities or unauthorized entry found upon review should be reported to assistant EHSS manager/supervisor via incident report for investigation ○ 9.8.4. EAC system installed must meet the following minimum standards ○ 9.8.4.1. Biometric access control ○ 9.8.4.2. UPS backup for a minimum of four (4) hours (or one (1) hour if backup Power generator is in place) ○ 9.8.4.3. Control panel and all devices fixed on secure side of doors ○ 9.8.4.4. Hardwired and secure from tampering; no accessible plugs or transformers ○ 9.8.5. EAC monthly test at least include the following criteria: ○ 9.8.5.1. Functioning ○ 9.8.5.2. Authorized user list ○ 9.8.5.3. Administrator password ○ 9.8.5.4. Hardware installations ○ 9.8.5.5.Real Time ○ 9.8.5.6. Unauthorized personnel ○ 9.8.5.7. Abnormal entry ○ 9.8.6. Incident report/record must kept at least 1 year by the security officer		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**9.9. Opening and closing of the facility** ○ 9.9.1. Deleted PCSO and replace Safety officers for opening and closing protocols ○ 9.9.2. Opening and closing logbook shall be in place and maintain by security officers ○ 9.9.3. Opening and closing of facilities shall be signed by both safety officers/electrician personnel ○ 9.9.4. Any abnormalities found upon opening and closing shall be reported to assistant EHSS manager and supervisor via incident report for investigation ○ 9.9.5. Investigation report shall be kept by security officer at least 1 year 9.10. **Gate and Gate Houses:** ○ 9.11. Identified issues found during weekly physical security inspection must have corrective action and should be monitored and verify until closure ○ 9.12. All identified issues during weekly physical security inspection should be reported to security officer or assistant EHSS manager/supervisor for investigation ○ 9.13. Weekly inspection records and investigation report must be kept by security officer at least 1 year **9.15. List of Employees Access Privilege** ○ 9.15.1. Deleted HR and replace Security officer in giving access privilege list to security guard and adding (All areas pass) and approving signatories		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ 9.15.2. List of employees should be posted at entrance to every sensitive areas for verification Purposes of non-organic person wish to entry ○ 9.15.3. Copy of list of employees at guard house and posted to sensitive areas must have an Approval by department heads and assistant EHSS manager/supervisor ○ 9.15.4. Security officer should also kept copy of list of employee's access privilege to sensitive Areas 10. **Physical Access Control** **10.1. Employees Access Control** ○ 10.1.1. Added upon entering in wearing of company ID ○ 10.1.4. Consolidated company ID'S subject for replacement should be in place ○ 10.1.5.Record of ID replacement should be available **10.2. Access to Sensitive Areas** ○ 10.2.3. Other employees and non-organic personnel must log in/out to unauthorized access Logbook ○ 10.2.6. Lost access pass should be report and make incident report by the security personnel To security officer ○ 10.2.7. Access pass must have affixed signature by HR manager/Assistant EHSS manager/Supervisor		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	10.3. **Challenging and Removing Unauthorized Persons** **Deleted** ○ 10.3.6. Any person, may it be employees or visitors including factory management, adidas Group personnel and courier, should be subjected to standard and prescribed entry/exit control measures, including visitor escort, baggage check and vehicle search. ○ 10.3.7. Any Security Violation found by any contractor should be immediately reported to the Security Personnel and Human Resource Manager. **10.5. Visitors Access Control** ○ 10.5.6. All visitors, applicants, sub/ contractors, Couriers, suppliers shall be check via metal detector to check if no fire arms brought inside the facility **10.7. Control of Access to mails and parcel** ○ 10.7.4. Responsible person to conduct inspection of mails and parcel must be trained ○ 10.7.5. Training record shall be kept by security officer **10.8. List of logbooks maintained in the guard station** ○ 10.8.11. Keeping of books shall be in 1 year by the security SIC/Head guard		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	**11. Personnel Security** **11.3. Periodic Checks and Reinvestigation** ○ 11.3.1. Deleted HR and replace by the security officer in updating list of employees in sensitive positions ○ 11.3.2. List of employees in sensitive positions shall be prepared by security officer, noted by assistant EHSS manager/supervisor and approved by factory manager ○ 11.3.4. All employees in sensitive positions shall renew their NBI clearance one (1) month prior the expiry date annually ○ 11.3.7. NBI clearance and background investigation shall be kept by security officer and annual update of employees information shall be kept by HR department at least 1 year **11.5.Employees Code of Conduct** ○ 11.5.1. All employees must receive copy for the outline of behaviors that are prohibited Stating policy of disciplinary actions for violations ○ 11.5.2. Proof/acknowledgement receipt must be kept to employees individual 201 file by HR Department **11.6.Lost Identification Badges** ○ 11.6.4. If security personnel recognizes and confirm employees had no/lost their company ID's, security personnel will immediately notify to HR department ○ 11.6.5. Employees having lost company ID shall log in/out every day to lost ID monitoring logbook while waiting of ID replacement for recording and		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

09	September 15,2020	○ **Education Training and Awareness** ○ 12.1. Deleted HR and replaced EHSS Department in coordination with training department for the annual orientation of CTPAT procedures ○ 12.3. All newly hired employees shall undergo CTPAT procedures orientation on their first day of work ○ 12.4. Documented security procedures shall publicized throughout the facility such as posters and bulletin boards ○ 12.5. Training record e.g. system generated attendance must be kept by Security officer at least 1 year ○ Security officer through the department heads shall ensure internal procedures to the following special activity/process; ▪ Logistics ▪ Loading/Unloading ▪ 7 and 17 points inspection ▪ Shipping ▪ Receiving of mails and packages ▪ Cargo handling ○ Security officer in coordination with the department heads shall conduct annual special training to the following; ▪ Logistics ▪ Loading/Unloading ▪ 7 and 17 points inspection ▪ Pest Contamination inspection ▪ Shipping ▪ Receiving of mails and packages ▪ Cargo handling		Vickie Rose Orpilla Malou Pacres Annie Sy Edna Esguerra Dino Cordova Cris Birao Romil Cabahug Jayson Chou Ian Celestial Sade Yeh Vincent Lee Cando Yeh

1. OBJECTIVES

1.1. To provide highest level of cargo security and properly document the requirements set by the Customs-Trade Partnership against Terrorism (C-TPAT).
1.2. To prevent security threats and possible acts of terrorism in the facility
1.3. To ensure a more secure and expeditious supply chain to employees, suppliers, customers or business partners
1.4. To ensure integrity of the security practices and understanding of the employee related to CTPAT procedures

2. SCOPE

2.1. This procedures applies to all employees, its contractors, sub-contractors, business partners, and visitors.

3. RESPONSIBILITY

3.1. Factory Manager shall be responsible to oversee the security of the facility and will review And approve necessary request in compliance to CTPAT requirements
3.2. Assistant EHSS manager/Supervisor shall assist factory manager to oversee the security of the Facility and to monitor compliance to CTPAT requirements
3.3. EHSS manager and compliance manager shall review the procedure for its adequacy and Applicability for use.
3.4. Security officer shall be the responsible for the implementation and maintain all records related To this procedure.
3.5. HR Manager shall be the responsible person to ensure CTPAT related documents for HR department
3.6. Compliance team shall be the responsible to verify the effectiveness of the implementation of this procedures

4. DEFINITIONS:

4.1. **CCTV** – Close Circuit Television Surveillance System
4.2. **DOB** – Daily Occurrence Book
4.3. **IDS** – Intrusion Detection System
4.4. **EPASS** – Electronic Pass Access Security System
4.5. **LCL** – Less-than Container Load
4.6. **FCL** – Full Container Load
4.7. **Risk Assessment** – Identify, Analyze, Eliminate/mitigate or manage security threats and/or Vulnerabilities in the facility
4.8. **Business Partners** – Elements of its international supply chain and to ensure that sound security

Measures are in place and adhered to in order to achieve an effective secure supply chain globally

4.9. **IIT** – Instrument of International Traffic

4.10. **TS** – Transfer Slip

4.11. **IPPC** – International Plant Protection Convention

4.12. **ISPM** – International Standard for Phytosanitary Measures

4.13. **PAS/ISO** - the standardized document that establishes "uniform procedures for the classification, Acceptance, and withdrawal of mechanical freight container seals. It provides a single Source of Information on mechanical seals which are acceptable for securing freight Containers in international commerce

4.14. **CFS** – Container Freight Station

4.15. **CIP** – Carriage and Insurance Paid

4.16. **Cyber Security** - The practice of defending computers, servers, mobile devices, electronic Systems, Networks, and data from malicious attacks. It's also known as information technology Security or Electronic information security.

4.17. **Seal Security** - Tamper evident mechanisms used to seal cargo in transit shipping containers in A way that provides tamper evidence and some level of security. Such seals can help to detect Theft or contamination, either accidental or deliberate.

4.18. **Procedural Security** - Protection against unmanifested material being introduced into the supply Chain. Supervised introduction/removal of cargo, the proper marking, weighing, counting and Documenting of Cargo/cargo equipment verified against manifest documents, the Detecting/reporting of shortages/overages, and procedures for verifying seals on containers, Trailers, and railcars. The Movement of incoming/outgoing goods should be monitored

4.19. **Physical Security** – Security of the facility including perimeter fences, locking devices on external And internal doors, windows, gates and fences, adequate lighting inside and outside the facility, And the segregation and marking of international, domestic, high-value, and dangerous goods Cargo Within the warehouse by a safe, caged or otherwise fenced-in area.

4.20. **Physical Access Control** - Controls of positive identification to all employees, visitors, And vendors including challenging unauthorized/unidentified persons

4.21. **Personnel Security** – An employment screening and interviewing of Prospective employees to Include periodic background checks and application verifications

4.22. **Education, Training and Awareness** - An awareness program to employees including recognizing Internal conspiracies, maintaining cargo integrity, and determining and addressing unauthorized Access. These programs should encourage active employee participation in security controls

4.23. **Conveyance Security** - Physical search of all readily accessible areas, the securing all Internal/external compartments and panels as appropriate, and procedures for reporting cases in Which unmanifested materials, or signs of tampering, are discovered

4.24. **Agricultural Security** - preventing contamination from foreign animal, plant or any organic Material

5. PROCEDURES

1. Security Vision and Responsibility

1.1. To become and remain effective CTPAT Member's supply chain, it must have the support of a company's upper management and commitment to a culture of security throughout the organization

1.2. The factory manager and EHSS manager shall be the company's upper management/senior company officials for the security of the facility

1.3. The facility, as a CTPAT member through the security officer should established a statement of support demonstrating their commitment to supply chain security and CTPAT program for promoting a culture of security of the facility.
1.4. Statement of support should highlight the importance of protecting the supply chain from criminal activities such as drug trafficking, terrorism, human smuggling, and illegal contraband
1.5. The statement of support should be signed by the Factory manager, EHSS manager, Assistant EHSS manager/supervisor and regional director
1.6. It is also part of their duties and responsibilities to have a full support and commitment to the following;
1.3.1. Promoting a work culture of security
1.3.2. Building a robust supply-chain security program to all of the relevant departments into a Cross-functional team
1.3.3. Creating a written and documented program
1.3.4. Having a team knowledgeable of the CTPAT program and its requirements
1.7. Assistant EHSS manager/supervisor and Security officer shall conduct an overall general review At least twice a year to ensure that all areas of the security program are working as designed
1.8. Records during general review should be in place
1.9. Issues found during general review shall be provided with corrective action
1.10. Record and Corrective action shall be kept by security officer
1.11. Security Officer shall be the designated company's point of contact (POC) for the CTPAT Requirements of the facility
1.12. Company's Point(s) of Contact (POC) for CTPAT must be knowledgeable about CTPAT program Requirements.
1.13. These individuals need to provide regular updates to upper management i.e. factory manager and EHSS manager on issues related to the Program, including the progress or outcomes of any audits, Security related exercises, and CTPAT validations

2. Risk Assessment

2.1. The continuing threat of terrorist groups and criminal organizations targeting supply chains underscores the need for Members to assess existing and potential exposure to these evolving threats, it should focus on geographical areas/supply chains that have higher risk.
2.2. Assistant EHSS manager/supervisor and Security officer should establish a Risk Assessment
2.3. The overall risk assessment (RA) is made up of two key parts
2.4. The first part is a self-assessment of the Member's supply chain security practices, procedures, and policies within the facilities that it controls to verify its adherence to CTPAT's minimum-security criteria, and an overall management review of how it is managing risk
2.5. The second part of the RA is the international risk assessment. This portion of the RA includes the identification of geographical threat(s) based on the Member's business model and role in the supply chain
2.4. Risk assessment should include the following;
2.4.1. Identify security threats and vulnerabilities in the facility and its supply chain
2.4.2. Analyze security threats and vulnerabilities based on the frequency and Consequences of the risk
2.4.3. Control risk: mitigate, eliminate or manage risks
2.4.4. Provide action plan to every security threats and vulnerabilities
2.5. Risk assessment shall be approved by EHSS manager and Factory manager.
2.6. Risk assessments must be reviewed annually, or more frequently as risk factors dictate.

2.7. The facility through EHSS manager and assistant EHSS manager/Supervisor should established a Procedures that address crisis management, business continuity, security recovery plans, and Business resumption.

2.8. These procedures shall be reviewed annually by the Factory managers, sustainability manager and Regional factory manager

2.9. Established procedures shall be signed by the Factory managers, sustainability manager and Regional factory manager

2.10. A crisis may include the disruption of the movement of trade data due to a cyber attack, a fire, or a carrier driver being hijacked by armed individuals

2.11. A contingency plans may include additional security notifications or support; and how to recover what was destroyed or stolen to return to normal operating conditions

3. Business Partners Security

3.1. Security officer in the facility shall keep and maintain an updated list of its business Partners related to CTPAT

3.2. Business partners should be the following;

3.2.1. Product supplier (Cartons/Seals/Packaging tape, Seals and etc.)

3.2.2. Transportation/Logistics provider

3.2.3. Brokers/Customs brokers

3.2.4. IT providers

3.2.5. Security Agency and Canteen concessionaire

3.2.6. Security Technology, Maintenance and repair service provider (CCTV/EAC/IDS)

3.3. Updated list of business partners should contain the following:

3.3.1. Name of Company/Business

3.3.2. Name of the Owner/Manager

3.3.3. Business Address

3.3.4. Products/Services Provided

3.3.5. Contact Numbers

3.3.6. Authorized Representative, if any

3.4. In selecting business partners, the facility shall consider the following:

3.4.1. Financial Stability

3.4.2. Corporate History

3.4.3. Hiring Practices

3.4.4. Binding Contract

3.5. List of personnel who have regular access/transaction to the facility of identified business partners Should be in place

3.6. Security officer for security agency and HR department for canteen concessionaire shall conduct Background Investigation to business partners Personnel With access to the facility and required Them to secure NBI clearance annually to verify community standing.

3.7. Identified business partners must submit their annual self-assessment to security officer Except for canteen concessionaire and security agency that will be monitor by Compliance Department on the 1st month of the year

3.8. If found any security weakness during self-assessment, corrective action plan and evidences Should be in place

3.9. Once received the self-assessment result, security officer will then send to compliance supervisor For uploading to portal

3.10. Annual On-site inspection should be conducted to all business partners by the following;

3.10.1. Compliance team – Security agency and canteen concessionaire
3.10.2. Security Technology service provider and maintenance (IDS) – Security Officer
3.10.3. Security Technology service provider and maintenance (EAC/CCTV) – IT department
3.10.4. IT providers and maintenance – IT department
3.10.5. Supplier (Cartons/Seals/Packaging tapes/Metal Seals) – FG Security officer
3.10.6. Transportation/Logistics providers – FG personnel
3.10.7. Supplier (Shipping and PEZA Seals) – Shipping department
3.10.8. Brokers/Customs broker – Shipping department

3.11. Security officer should kept records of annual self-assessment and on-site inspection of Business partners

3.12. Business partners must provide copies of their security policies, including physical Security, access control, cargo handling, and other related to the C-TPAT standards

3.13. Security officer must conduct annual orientation of CTPAT procedures to all business Partner's representative and provide them a copy of CTPAT procedures and in every update

3.14. Received/signed copy of CTPAT procedures by the business partners should be available

3.15. The facility through the security officer shall establish procedure for in-country carriers to report Security violations to the facility's management

4. Cyber Security

4.1. Written Policies and Procedures

4.1.1. The facility through IT personnel should have established Cyber Security/IT policy and Procedures
4.1.2. This should be approved by IT manager, Factory managers and Central HR managers
4.1.3. Cyber Security policy and procedures must cover below aspects;
- 4.1.3.1. Responsibilities and duties
- 4.1.3.2. Hardware and Software
- 4.1.3.3. User access management
- 4.1.3.4. Operational Security
- 4.1.3.5. Backup and recovery
- 4.1.3.6. Employees/contractor disciplinary policy for IT violations

4.1.4. Cyber security policies/procedures shall be review and Updated by the IT management at least annually, or more frequently, as risks or Circumstances dictate

4.2. Hardware

4.2.1. Server Central Control

4.2.1.1. All servers/IT rooms must be physically secured
4.2.1.2. They shall be protected against safety and environment concerns
4.2.1.3. IT personnel should conduct daily temperature checking in server room/IT Rooms
4.2.1.4. Server room/IT room should be in a maximum limit of temperature w/c is 24ºC
4.2.1.5. Records of temperature checking should be kept at least 1 year by IT personnel
4.2.1.6. Server room/IT room must equipped with fire extinguisher
4.2.1.7. Monthly inspection of fire extinguisher should be conducted by the safety

Officer or electricians

4.2.1.8. Records of fire extinguisher inspection should be kept at least 1 year by the Safety officer

4.2.1.9. Server room should always be kept safe, neat and tidy

4.2.2. Network Setting

4.2.2.1. To prevent access to internet on all workstations in the Facility, all computers Must be physically blocked or disabled through software (except for Authorized personnel)

4.2.2.2. Network setting must equipped with anti-intrusion hardware

4.2.2.3. IT personnel shall maintain and kept IT access list of employees /list of Computer users who are allowed to access information systems e.g. email, Intranet, internet, Skype and other management Program and system

4.2.2.4. IT access list shall be updated as need arises (if have newly hired computer users and separated computer users)

4.2.2.5. List of employees allowed to access internet and Skype should be taken from IT access list and updated monthly

4.2.2.6. Issued Skype should be a business Skype (with end to end encryption)

4.2.2.7. IT access list and Monthly list of employees allowed to access internet and Skype must be signed by IT personnel and approved by IT manager

4.2.2.8. Employees allowed to access internet and Skype must have the approval from Department heads through accomplished internet application.

4.2.2.9. Internet application must be completely signed by department managers and IT managers

4.2.2.10. Record should be kept by IT personnel

4.2.3. Wiring

4.2.3.1. Cables, equipment and electrical wiring should be safely installed in order to Eliminate any kinds of employee accidents, data loss and fire accidents

4.2.4. Terminal Units

4.2.4.1. IT manager shall be the responsible person and should be knowledgeable in server or terminal units,

4.2.4.2. Should be then received letter of appointment (LOA) given by security officer

4.2.5. Regularly Maintained

4.2.5.1. Technology components or software and network components should be check Monthly by the IT personnel

4.2.5.2. Records should be kept at least 1 year

4.2.6. Media and Mobile Working Units

4.2.6.1. To prevent and block unauthorized data transfers, transfer ports on all Workstations in the facility, all computers must be physically blocked or disabled

Through software (except for authorized Users)

4.2.6.2. List of employees allowed to access USB flash drive should be taken from IT access list and updated monthly

4.2.6.3. Monthly list of employees allowed to access USB flash drive must be signed by IT personnel and approved by IT manager

4.2.6.4. Employees allowed to access USB flash drive must have the approval from Department heads through accomplished USB flash drive application.

4.2.6.5. USB flash drive application must be completely signed by department managers and IT managers

4.2.6.6. Record should be kept by IT personnel

4.3. Software

4.3.1. Software use must be license

4.3.2. It department shall secure and retain software license from service provider

4.3.3. Anti-virus program with high detection installed in each workstation and firewall to Server and all software for prevention, and recovery controls to protect against malware

4.3.4. All computers must be secured or prohibited from installation of unapproved software

4.3.5. IT personnel should conduct monthly vulnerability scans and penetration test

4.3.6. If found or noted any vulnerabilities, actions must be taken

4.3.7. Records must be keep at least 1 year by the IT personnel

4.4. Access Control

4.4.1. All Computer workstations must be password protected

4.4.2. Password must not be shared and post in public for prevention of unauthorized access to Computer

4.4.3. All user computer passwords should be highly secure, following these guidelines:

4.4.3.1. Minimum password length: (8) characters

4.4.3.2. Complexity requirements

4.4.3.3. No reuse of three (3) most recent passwords

4.4.3.4. Permanent account lockout (requiring administrator override) after five (5) failed Log in attempts

4.4.3.5. Password must be changed by user every thirty (30) days

4.4.4. All invalid password attempts and file access shall be maintained and reviewed weekly by The IT personnel

4.4.5. Employees with computer access must sign user regulations and receive computer Security Training.

4.4.6. Annual training or orientation to all computer users shall be conducted by IT department

4.4.7. Training record/printed master list of attendance shall be kept by IT personnel and training personnel at least 1 year

4.5. Regular Meeting

4.5.1.IT personnel should conduct quarterly meeting to the facility attended by management/manager to Address IT security issues.

4.6. Back up Recovery and Disposal

4.6.1. System and Data should be back up in a weekly basis by the IT personnel

4.6.2. Back up must be made offsite or to other area not located in the facility

4.6.3. All sensitive and confidential data are stored in an encrypted format or protected by Password

4.6.4. All data storing in any used and discarded storage devices, including but are not Limited to hard disk, flash drive, CD/DVD laser discs, magnetic tapes should be erased Completely and disposed of properly

4.6.5. Record must be keep at least 1 year by IT personnel

5. Conveyance and International Traffic Instrument (IIT) System

5.1. Container/Trailers or any IIT Storage and Monitoring

5.1.1. Containers/trailers or any IIT storage parking area must be enclosed with barrier, adequate Lighting, enclose perimeter fence, away from the parking area of employees, visitors and Suppliers to prevent unauthorized access and/or manipulation

5.1.2. Only authorized personnel and security personnel are allowed in the loading area/containers/trailers area.

5.1.3. Authorized personnel must have loading access pass (yellow) for identification Purposes

5.1.4. List of authorized personnel at Loading area or Containers/trailer or any IIT storage parking area should be posted Warning signs e.g. authorized personnel only and list of Authorized personnel

5.1.5. Personnel with no ID badge in the loading area containers/trailers or any IIT storage parking Area must be asked to exit and will be subject for investigation.

5.1.6. Loading area or Containers/trailer or any IIT storage parking area must have installed CCTV Cameras and also focusing inside container van

5.1.7. Loaded or empty containers or any IIT storage must be keep locked//sealed for overnight Staging

5.1.8. Any unauthorized personnel entry, un-manifested materials, signs of tampering, anomalies And/or contrabands or incoherent shipping document in relation to cargo or goods upon Discovery must be notified immediately any local law enforcement authority and Customs Authority.

5.2. Container/Trailer/ Wing Van and Vehicles /Other IIT Inspection

5.2.1. The facility through the FG and CWH manager/supervisor should have established procedures on container/trailer/Tractor/other IIT inspection

5.2.2. Incoming and outgoing Empty/loaded container/trailer/Tractor or other IIT shall undergo pest contamination checking and 17 point Inspection to ensure safety of the facility and security of shipment.

5.2.3. Incoming and outgoing wing van and vehicles shall undergo 7 points inspection

5.2.4. Inspection shall be conducted outside/before entering the facility perimeter

5.2.5. Inspection shall be conducted by Security guard together with factory representatives

5.2.5. 17 points inspection checklist must contain agricultural security with separate pest Contamination checklist

5.2.6. Seventeen (17) points inspection of Tractor/Trailer/Container should cover the ff;

5.2.6.1. Bumper

5.2.6.2. Engine/Battery box

5.2.6.3. Tires (Truck/Trailer)

5.2.6.4. Floor (inside truck)

5.2.6.5. Fuel tanks

5.2.6.6. Cab/compartment (interior and exterior)/tool compartment

5.2.6.7. Air tanks

5.2.6.8. Drive Shafts

5.2.6.9. Fifth Wheel/tires/Rims

5.2.6.10. Outside/undercarriage

5.2.6.11. Outside/inside doors and locking mechanism

5.2.6.12. Floor (inside trailer)

5.2.6.13. Side walls (left and right sides)

5.2.6.14. Front wall/Rear – bumper/doors

5.2.6.15. Ceiling/Roof

5.2.6.16. Refrigeration unit

5.2.6.17. Exhaust/Air breather

5.2.7. Pest contamination checking criteria should include the ff;

5.2.7.1. Visible traces of animals, insects, or other invertebrates – dead or alive, in any Lifecycle stage, eggs or rafts

5.2.7.2. Any organic materials of animal origins – blood, bones, hair, flesh, secretions, Excretions

5.2.7.3. Viable or non-viable plants or plants products – fruits, seeds, leaves, twigs, roots, Barks

5.2.7.4. Other organic materials i.e. fungi, soil or water that may cause contamination by Organic materials.

5.2.8. If pest contamination is found, contaminations shall be remove by washing/vacuuming, cleaning or other means of treatment.

5.2.9. Inspection records of Tractor/Trailer/Container shall be send to consignee prior to Receiving the merchandise

5.2.10. FG manager or supervisor should conduct random inspections of Tractor/Trailer/Container To make sure the Procedure is being followed

5.2.11. Seven (7) points inspection to wing van and vehicles should cover the ff:

5.2.11.1. Bumpers

5.2.11.2. Tires/Rims

5.2.11.3. Cab Compartment/fuel tank/Air breather

5.2.11.4. Outside/Undercarriage/Exhaust

5.2.11.5. Interior Cab compartment/ Tool Compartment

5.2.11.6. Roof/Ceiling

5.2.11.7. Outside/ inside doors and locking mechanism

5.2.12. Any discrepancies found during inspections shall be reported to Factory manager/Security officers through incident report by the security personnel

5.2.13. Corrective action should be in place to address and mitigate issues

5.2. Record Keeping

5.3.1. 17 and 7 points inspection, pest contamination inspection, corrective action and random Inspection result should be keep 1 at least 1 year by FG supervisor/manager

6. Seal Security

6.1. Seal Security Procedure

6.1.1. The facility through the shipping and FG manager shall established Seal Security Procedure and shall be reviewed at least annually and updated as necessary

6.2. Receiving and Checking of Seals

6.2.1. Shipping seal from the shipping lines through the trucking service who delivers the Empty container and PEZA seal purchased from PEZA shall receive by the shipping Personnel

6.2.2. Metal seal from purchasing department shall receive by the Dispatch Team Leader.

6.2.3. Shipping personnel will then check and verify the shipping seal number, if it Coincides from the mail advice provided by the forwarder to the actual received as Well as the PEZA and Metal seals will double check the quantity and the sequence of Metal seal number

6.2.4. If shipping seals does not coincide as advised, shipping personnel will inform the Finished Goods Manager regarding the discrepancy. The Finished Goods Manager Reports the discrepancy to the forwarder and asks for the correct seal.

6.2.5. If found discrepancy on the metal seals, the Finished Goods Manager will inform Purchasing department for the discrepancy. Records the damaged metal seal and Ask replacement from supplier

6.2.6. If the integrity of the shipping seal has been compromised. Shipping personnel will Inform immediately to the Finished Goods Manager regarding the problem. The Number of the compromised seal is duly recorded. Finished Goods Manager will Inform the forwarder for the problem and immediately request for a replacement.

6.2.7. Unused/compromised shipping seals are duly reported to the local customs of the Said unused/compromised Shipping seal.

6.2.8. All unused FCL/LCL shipping seals are to be returned to the forwarder.

6.3. Seal log and record keeping

6.3.1. Shipping personnel will records the shipping seal and PEZA seals while dispatch team

Leader will record the metal seals upon receiving and once the seals has been checked For its quality in the security seal log book.

6.3.2. Upon receipt of the Shipping Seal, metal seals and PEZA Seal, the control numbers will Be recorded and verify by logistic staff

6.3.3. Shipping, PEZA and metal seals will only be released, once the container and the truck Respectively are already full and ready for sealing.

6.3.4. Shipping and PEZA seals should release by shipping personnel while metal seals will Release by dispatch team leader

6.3.5. Releasing of shipping, PEZA and metal seals should be recorded in security Seal log book

6.3.6. Shipping, metal and PEZA seals should be kept in a secured storage with locking System and access only by the authorized personnel

6.3.7. Monthly inventory of PEZA seals should be conducted by shipping Personnel and metal seals by dispatch team leader

6.3.8. Inventory record must be keep at least 1 year by shipping personnel and dispatch team Leader

6.3.9. Seal number shall be electronically printed on the shipping documents

6.4. **Seal Requirements**

6.4.1. All seals used must meet or exceed the most current PAS/ISO 17712 standard for high Security seals

6.4.2. Shipping manager/supervisor and FG manager and supervisor must ensure to secure Certificate from the seals manufacturer/provider to ensure seals meet the standard

6.4.3. Only seals rated as "high security seals" can be used for shipment bounds to US

6.4.4. Security seals must equipped with unique serial number

6.4.5. Seals must have manufactures name or logo indicated on seals and have mark or Stamp to identify its classifications as high security ('H) (preferable)

7. Procedural Security

7.1. Protection of Cargo

7.2. Container Checking and Recording

7.2.1. Empty Container

7.2.1.1. All delivered empty containers shall undergo the 17 point inspection and pest contamination checking prior entering the facility

7.2.1.2. Security personnel will check the driver through metal detector if no fire arms brought and should stay beside guard station

7.2.1.3. Inspection shall be conducted by the security guard and one of the FG personnel for safety purposes and to check on the integrity of the container and measure with the use of the laser measuring device and chassis mirror to check on the accuracy of the container specifications

7.2.1.4. Inspection shall be conducted outside or before entering the facility perimeter

7.2.1.5. Container number is reconciled with the Shipping Advice

7.2.1.6. Hazardous materials, ammunitions, explosives and other dangerous cargos must be identified for proper handling and storage.

7.2.1.7. The security personnel shall inform facility management or local authorities (Peza Security) from any discovery of broken, dented, wrecked, compromise, Tampered seal/padlock and menace container/trailer during inspection

7.2.1.8. Any discrepancy with the integrity and measurement of the container will be reported to the FG Manager and will be sent back to its point of origin.

7.2.1.9. FG manager will then request for replacement of the container with discrepancy

7.2.1.10. Replacement arrives, this will still undergo the 17 point inspection and pest contamination checking

7.2.1.11. Empty container/trailer must be logged by security personnel on duty at container logbook following below information;

1. Date
2. Time in
3. Driver's Name
4. Driver License Number
5. Helper name
6. Trailer number
7. Plate Number
8. Container Number
9. Trucking name
10. Seal Number, if any
11. Guard on duty
12. Purpose of Visit

7.2.2. Loading Process of Finish Goods for Shipment

7.2.2.1. FG team leaders and supervisors will check cargo based on loading sequence And Purchase order number

7.2.2.2. Proceed to loading of finish goods

7.2.2.3. Loading activity should be monitored and supervised by security personnel, dispatch team leader and FG supervisor

7.2.2.4. There should be no unauthorized personnel present at loading area during loading activity

7.2.2.5. If loading area in the factory is not enclosed with gate, a need to provide barriers/barricade upon loading activity

7.2.2.6. Dispatch team leader or FG supervisor should take pictures during loading process and affixing of seals to container

7.2.2.7. Pictures take of the ff;

- 7.2.2.7.1. Cargo markings (carton mark/crate mark, etc.)
- 7.2.2.7.2. Loading process – empty, half, 2/3 and finish loading
- 7.2.2.7.3. Seal affixing and close up image where the seals has been affixed and where seal number clearly appear
- 7.2.2.7.4. Finish loading and closing a door

7.2.2.8. Records must be keep at least 1 year by FG supervisor

7.2.3. How to affix seal security

7.2.3.1. FG team leader in the presence of FG manager/supervisor and security personnel will be the responsible Person to affix the seal to container/ other IITs

7.2.3.2. When affixing security seal, must follow seal VVTT process are the ff;

7.2.3.3. View the seal and container locking mechanism, and ensure they are in good working condition.

7.2.3.4. Report to FG supervisor/manager of found damage/broken or other discrepancies noted

7.2.3.5. Verify seal numbers for accuracy. Compare with shipping documents and look for alterations to seal numbers

7.2.3.6. Tug on the seal to make sure it is affixed firmly. Seals that come apart must be reported to FG manager/supervisor

7.2.3.7. Twist and turn seal to make sure its components do not unscrew or separate from one another

7.2.3.8. Authorized personnel who affixed the security seal must have proper training

7.2.3.9. Training record must be keep by FG supervisor at least 1 year

7.3. Shipping

7.3.1. FCL and LCL departing cargo must be verified against purchase orders or delivery orders before the cargo is released and should be logged to loaded container cargo following below information:

1. Date
2. Time out
3. Driver's Name
4. Driver License Number
5. Helper name
6. Trailer number
7. Plate Number
8. Container Number
9. Trucking name
10. Seal Numbers
11. Guard on duty
12. Destination
13. Delivery receipt

7.3.2. For LCL goods send to forwarder's CFS warehouse via a closed top truck

7.3.3. Security personnel must ask/required delivery drivers to show truck manifest on entry and/or exit

7.3.4. Cargo or any other IIT must equipped with security seals upon departure from finish goods warehouse

7.3.5. Delivery

7.4. Cargo Examination

7.4.1. For both LCL and FCL shipments, trucks will go directly to PEZA Admin Office for Cargo Examination.

7.4.2. View the approved ED in workstation and makes the export shipment available for inspection.

7.4.3. PEZA personnel will tag the inspection details into the system and affix their signature in the 2 ED copies. The system will be updated as Approved and Inspected.

7.5. Monitoring of Cargoes

7.5.1. During Cargo transport, if the truck (LCL shipment) experiences engine breakdown, flat tire or any occurrence due to natural calamities that cannot be avoided, while on transit. The personnel, who escort the delivery, should inform immediately the Dispatch Team Leader of their situation.

7.5.2. For FCL shipments, the driver through their handheld radio frequency communicator, should transmit information to their head office of their situation, thus the head office will inform their customer through the Finished Goods Manager.

7.5.3. The personnel accompanying the delivery should safeguard the cargoes during these unforeseen events for our LCL and FCL deliveries respectively.

7.5.4. Any activity should be closely monitored hourly via GPS system monitored by FG manager, so that any unforeseen illegal activities will be suppressed.

7.5.5. The accompanying personnel and the container truck driver should call back up so that cargoes stalled, will be attended and directly be delivered to forwarder's warehouse for LCL and to CIP for FCL shipments.

7.5.6. Personnel escorting the cargoes will report to Dispatch Team Leader once the cargo arrived at forwarder's warehouse for LCL and at the CIP for FCL.

7.5.7. Cargo arrived at the Port (Airport and Seaport). The accompanying personnel present ED to BOC Port of Loading – Export Division.

7.5.8. BOC – Port Loading Personnel – Export Division scans the barcode and validates the ED and stamps the ED: Approved for Loading. System accepts the barcode and updates the status as Transferred inspected including date and time of transfer of the cargoes.

7.6. Documentations

7.6.1. Documents of departing cargo are reconciled against information in the cargo manifest

7.6.2. Documents of departing cargo are accurately described and verified in terms of weight, labels, marks and piece count

7.6.3. Shipping documents shall be sent to consignee prior to receiving the shipment

7.6.4. Documents are verified by the authorized Shipping Supervisors before submission.

7.6.5. All shipping documents and all documents pertinent to business partners CTPAT credentials and use such as reference for selection of business partners shall be safety stored after office hours and keep by shipping supervisor

7.6.6. Record must be keep at least 1 year by FG supervisors and shipping supervisor

7.7. Manifesting Procedures

7.7.1. Export Declaration and Final documents are validated by the Shipping Supervisor before submission.

7.7.2. Document submission follows the corresponding cut-off dates as stipulated by the forwarders.

7.7.3. After cartons are being examined, the factory shall maintain records showing which cartons have been selected for examination.

7.8. Cargo Discrepancy

7.8.1. Any shortages or overages and other significant discrepancies are immediately reported to the Shipping Supervisor and HRD Manager for investigation
7.8.2. Positive identification of illegal/suspicious activities must be immediately reported to the US Customs and Border Protection through the Shipping Supervisor and local law enforcements
7.8.3. For discrepancies on LCL cargoes, it will be addressed to the Importation Shipping Supervisor then to the Broker
7.8.4. For containerized cargoes, inform Taipei Office
7.8.5. Shipping of external cargo is applicable to Finished Goods operations

7.9. Pilferage Reporting from Forwarders/ Contractors

7.9.1. Shipping Team Leader receives mail and notice from forwarder regarding loose tapes, unsecured cartons and damage cartons with possibility of lacking garments and pilferage.
7.9.2. Shipping Team Leader must then ask the forwarder on the details of the affected PO. The following information must be taken:
7.9.3. PO Number, Destination and Carton Numbers affected.
7.9.4. How many cartons needed to be replaced if any
7.9.5. Shipping Team Leader shall call Finished Goods Supervisor or Manager to send Representative to check the reported Goods.
7.9.6. FG Supervisor or Manager must send representative to check the claim.
7.9.7. FG Representative will then check the reported problem/claim.
7.9.8. FG Representative shall take pictures and document the findings.
7.9.9. Forwarders/contractors must be present during the documentation process of the findings
7.9.10. Security Personnel must accompany the FG Representative
7.9.11. FG Representative must bring camera and tapes needed.
7.9.12. FG Representative conducts checking of the goods.
7.9.13. If no lacking garments found, FG Rep checks the condition of the cartons
7.9.14. If carton is in good condition, cartons will be closed and secured properly.
7.9.15. If carton is damaged, FG Representative should provide reports and identify who is responsible of the damage carton, the forwarder or the other entity or the company
7.9.16. If the forwarder is the one responsible of the damage, FG Representative prepares Initial Report and give to FG Supervisor or FG Manager in which he or she will then email the Final Claim Report to Forwarder.
7.9.17. Claim Report must contain the following information:
    7.9.17.1.1. Dimension of the damage carton
    7.9.17.1.2. Price
    7.9.17.1.3. Quantity of carton
    7.9.17.1.4. PO #
    7.9.17.1.5. SP #
7.9.18. If other entity (the company) is the one responsible, FG Representative automatically replaces the carton.
7.9.19. If lacking garments found and other findings, FG Representative will take pictures to each finding and assess or clarify below situation and ask approval from FG Manager for the following circumstances :

7.9.19.1. Need to replace the lacking garments
7.9.19.2. Close and ship-out the cartons despite lacking garments and forwarder will shoulder any claims.
7.9.20. FG Representative will give the pictures of discrepancy to FG Supervisor and Shipping Team leader for final reporting and documentation.
7.9.21. Shipping Team Leader must prepare Claim Report of the lacking garments. Claim Report must contain the following:
7.9.21.1. SP #
7.9.21.2. PO#
7.9.21.3. Quantity
7.9.21.4. Price
7.9.22. Shipping Team Leader emails the final report or Claim Report to forwarder/contractors including the concerned parties.
7.9.23. Final Report or Claim Report should contains the important details including the Following:
7.9.24. How many Garments/Accessories Lost
7.9.25. Cause of Damages
7.9.26. Were the Standard Operating Procedure followed or not
7.9.27. Total Cost of Charge Back
7.9.28. Other important and needed details.
7.9.29. Shipping Team Leader must ensure that confirmation of report from the forwarder/contractor is received.

7.10. In-country carriers' security violations

7.10.1. Any in-country carrier's security violations shall be reported by accompanying Security Guards to Factory Management.

7.11. Security Assessment and Improvement Plan

7.11.1. Facilities must undergo a yearly security assessment to be conducted by 3rd party, in which case the Security Agency will conduct assessment
7.11.2. All results will be submitted to the assistant EHSS Manager/supervisor for verification and Corrective Actions to be taken with specific timelines.
7.11.3. Compliance team will conduct bi-annual CTPAT audit
7.11.4. Audit report and CAP should be monitored by assigned auditor
7.11.5. Record keeping of documents will be kept by compliance supervisor at least 1 year

7.12. Loaded Container or Wing van of Export Raw materials

7.12.1. Container is examined by PEZA and Customs against the Import Documents
7.12.2. Container number is reconciled with the Shipping Advice sent by the Main Office;
7.12.3. Container/trailer/tractor or wing van are inspected through 17 points inspection
7.12.4. Cargo is checked against the Container Security Checklist by the Security Guard on duty and verifies container number, trailer number, truck number, seal number, Driver Name and License number, time, date and Name of inspector likewise take photo of the container

7.12.5. If no discrepancies upon checking the container, security guard will logged loaded container and also during pull out in container monitoring logbook following below information's:

14. Date
15. Time in/out
16. Drivers Complete Name
17. License Number
18. Company Badge (ID)
19. Truck Number/Plate Number
20. Container Number
21. Seal Number, if any
22. Name of Carrier of Company
23. Pulled out by
24. Purpose of Visit

7.12.6. The security personnel shall inform facility management or local authorities (Peza Security) from any discovery of broken, dented, wrecked, compromise, tampered seal/padlock and menace container/trailer during inspection.

7.12.7. The receiving personnel will verify cargos receive against the packing list provided by the Main Office.

7.12.8. Receiving personnel shall inform facility management if there are discrepancies noted upon verification of the cargos received.

7.12.9. Any shortages or overages and other significant discrepancies are immediately reported through the use of Discrepancy Report to Central Warehouse for immediate investigation

7.12.10. The facility management conducts investigation and make official report.

7.12.11. If no discrepancies found upon verification of cargo against the packing list, unloading of materials will be proceed

7.13. Delivering of Raw materials from Raw Materials Warehouse to Factory

7.13.1. Loading of raw materials to wing van for transferred to facilities shall be monitored by the security guard, warehouse dispatcher and factory in-charge

7.13.2. All raw materials transferred to facilities shall be documented through warehouse material checklist and electronic pass system/TS verified by dispatch guard

7.13.3. Warehouse material checklist, EPASS system and TS should be signed by the warehouse team leader, warehouse supervisor and warehouse manager

7.13.4. Loaded wing van of raw materials must be padlock by the security guard at all times upon exiting in the facility.

7.13.5. Security guard will conduct 7 points inspection to wing van in and out in the facility by using the chassis mirror

7.13.6. Wing van delivery of raw materials should be logged in and out in wing van/container logbook

7.13.7. Wing van/container logbook must cover the following e.g. date, time in/out, Driver Name, delivering factory and assigned security guard who conduct inspection

7.13.8. Keys of wing van must be kept both at central warehouse and factory security guard house

7.13.9. Security guards assigned in the factory shall open the loaded wing van

7.13.10. Delivery

7.14. Receiving of Raw Materials in Factory from Raw Materials Warehouse

7.14.1. Delivered loaded wing van of raw materials shall be inspected for 7 points inspection In and out in the facility

7.14.2. Delivered loaded wing van of raw materials should be logged in and out in wing van/container logbook

7.14.3. Wing van/container logbook must cover the following e.g. date, time in/out, Driver Name, delivering factory and assigned security guard who conduct inspection

7.14.4. Security guard will check/verify delivered wing van against EPASS/TS

7.14.5. If no abnormality found during inspection, guard in the presence of receiving Personnel will proceed to open the wing van

7.14.6. Proceed to unloading

7.14.7. Receiving in-charge will check the materials against warehouse materials checklist, then Received if no discrepancies

7.14.8. Once the unloading activity is done, security guard will padlocked the wing van

7.14.9. Travel back to origin

7.15. Delivering of finish goods from Factory to Finish Goods Warehouse

7.15.2. Loading of finish goods to wing van for transferred to finish goods warehouse shall be monitored the security guard and factory logistics personnel

7.15.3. There should be no unauthorized personnel in loading area during loading activity

7.15.4. Loading activity should be barricade to prevent unauthorized access

7.15.5. All finish goods transferred to finish goods warehouse shall be documented through transfer slip and electronic pass system verified by dispatch guard

7.15.6. Transfer slip and EPASS system should be signed by the factory logistic team leader, factory logistics supervisor and factory managers

7.15.7. Loaded wing van of finish goods must be padlock by the security guard at all times upon exiting in the facility.

7.15.8. Security guard will conduct 7 points inspection to wing van in and out in the facility

7.15.9. Wing van delivery of finish goods should be logged in and out in wing van/container logbook

7.15.10. Wing van/container logbook must cover the following e.g. date, time in/out, Driver Name, Transfer slip, delivering factory, and assigned security guard who conduct inspection

7.15.11. Keys of wing van must be kept both at factory and finish goods warehouse security guard house

7.15.12. Security guards assigned in finish goods warehouse shall open the loaded wing van

7.16.12. Delivery

7.16. Receiving of Finish Goods in Finish Goods Warehouse from Factory

7.16.2. Delivered loaded wing van of finish goods shall be inspected for 7 points inspection Prior entering to the facility by security guard on duty

7.14.2. Delivered loaded wing van of finish goods should be logged in and out in wing van/container logbook

7.14.3. Wing van/container logbook must cover the following e.g. date, time in/out, Driver Name, Transfer slip ,delivering factory and assigned security guard who conduct inspection

7.16.2. Security guard will check/verify delivered wing van against EPASS/TS

7.16.3. If no abnormality found during inspection, guard in the presence of finish goods

Personnel will proceed to open the wing van

7.16.4. Proceed to unloading

7.16.5. There should be no unauthorized personnel in loading area during unloading activity

7.16.6. Unloading activity should be barricade to prevent unauthorized access

7.16.7. Receiving in-charge will check the materials against transfer slip, then Received if no discrepancies

7.16.8. Once the unloading activity is done, security guard will padlocked the wing van

7.16.9. Travel back to origin

7.17. Documentation

7.17.1. Raw Materials – Warehouse material checklist shall be kept by central warehouse team leaders (Original copy) and factory warehouse by warehouse team leaders (copy)

7.17.2. Finish Goods - Transfer slip shall be kept by both factory logistics team leaders and finish goods warehouse receiving team leaders

7.17.3. Records must be kept at least 1 year

7.18. Inspection/Maintenance

7.18.1. Equipment's/tools e.g. under chassis mirror and flash light that utilized during 17 points inspection and metal detector, hand held radio, thermal moisture, laser measurement should be inspected or have a regular maintenance in a monthly basis by the security personnel

7.18.2. In case of abnormalities, corrective action shall be in place to address the issues via incident report

7.19. Incident Reporting process

7.19.1. Any employee who has identified unauthorized personnel in the facility or in restricted areas where issued pass prohibits entry level of the badge, the employee shall challenge the unauthorized personnel by asking for his identification and address the latter's concerns in the area.

7.19.2. Should unauthorized personnel's entry to restricted areas is verified, the employee shall escort the person to the security guard on duty for investigation

7.19.3. Should the employee is hesitant to apprehend the unauthorized person he/she shall report to the security guard on duty for investigation

7.19.4. Once the security guard on duty received the report, he/she will immediately apprehend the said person and endorse the situation to the factory management particularly to the Factory Manager, Assistant EHSS manager/Supervisor or to the HR Manager for further investigation

7.19.5. Factory management will conduct further investigation and take necessary actions Factory management will give reward or incentive to the security personnel who has Reported the Incident based on our MEM-CHR-013 – Anti-Theft and Pilferage Reward

7.19.6. Any employee who has identified any suspicious or unlawful activities is encouraged to immediately apprehend involved personnel and thus reporting such activity to the facility Management.

7.19.7. Any employee who has contributed to the apprehension of unauthorized personnel shall receive an incentive as per MEM-CHR-013 – Anti-Theft and Pilferage Reward

7.19.8. All facility HR Associates – Recruitment must be trained on how to conduct background checks based on employment references
7.19.9. Security officer shall conduct monthly meeting to all security officer
7.19.10. Attendance shall be kept by Security officer at least 1 year

8. Agricultural Security

8.17. Wood Packaging Materials used for Shipment

8.17.1. The facility should have established fumigation procedure for preventing pest contamination that is in compliance with IPPC and ISPM 15 requirements
8.17.2. Fumigation procedures shall be prepared by FG and shipping supervisors and approved by FG and shipping managers
8.17.3. Wood pallets for finish goods must be fumigated (MB-Methyl bromide) or heat treated (HT) at least once a month
8.17.4. Wood packaging items stamped or branded with an IPPC mark of compliance
8.17.5. Shipping documents shall include fumigation certificate in every shipment of goods Secured by the shipping supervisor/manager
8.17.6. Shipping supervisor/manager will request/coordinate 3rd party authorized to conduct fumigation during shipment
8.17.7. Sipping supervisor/manager shall kept record of fumigation certificate in every shipment

8.18. Pest contamination Inspection for Pallets

8.18.1. Finish goods warehouse and logistics warehouse in the factory must conduct pest contamination inspection to wood pallets storing of finish goods by FG and factory logistics warehouse personnel at least once a month
8.18.2. Pest contamination checking criteria should include the ff;
8.2.2.1. Visible traces of animals, insects, or other invertebrates – dead or alive, in any Lifecycle stage, eggs or rafts
8.2.2.2. Any organic materials of animal origins – blood, bones, hair, flesh, secretions, Excretions
8.2.2.3. Viable or non-viable plants or plants products – fruits, seeds, leaves, twigs, Roots, barks
8.2.2.4. Other organic materials i.e. fungi, soil or water that may cause contamination by Organic materials
8.18.3. Records of monthly pest contamination shall be kept by FG supervisors and factory Logistics team leader at least 1 year

9. Physical Security

9.1. Fencing and Building

9.1.1. Exterior perimeter fencing separates the facility to protect against unauthorized access. Alternatively, below are acceptable;
9.1.2.1. Dividing wall
9.1.2.2. Steep Cliff –Dense Thickets

9.1.2. Perimeter fence should be kept free from any obstruction to detect unauthorized Access/any intrusion in the Facility
9.1.3. Domestic, international, high value and hazardous cargo shall be segregated by Physical interior fencing
9.1.4. All fencing and building structures are built with materials that are strongly and not Easy to break to resist unauthorized entry
9.1.5. Perimeter fencing at least 6 feet high with outward -facing barbed wire on top should Enclose the areas around cargo handling and storage facilities.

9.2. Parking Area

9.2.1. Private vehicles should be prohibited from parking in or adjacent to cargo handling and storage areas are and shipping conveyance
9.2.2. Parking areas must equipped with CCTV cameras

9.3. Lighting

9.3.1. Adequate lighting should be provided inside and outside the facility for 24 hours to include the following areas: entrance and exits, cargo handling, storage areas, fence lines and parking areas
9.3.2. Lighting shall be equipped with a backup power supply in case of an electrical blackout
9.3.3. Access to power switch panel should be restricted with posted warning signs of authorized personnel only
9.3.4. Lighting turns on automatically/manually as the natural light dims

9.4. Locks and Keys

9.4.1. Security officer through security personnel must control the issuance and distribution of all locking devices, keys, codes, cards.
9.4.2. Security officer shall provide list of authorized personnel allowed to borrowed facility keys including keys to sensitive areas to guard house and must be updated in every changes
9.4.3. Keys master list should be made available at guard station
9.4.4. Keys shall be kept inside the Key Box located at the Guard Station and properly locked.
9.4.5. Key Box must be labeled "Do Not Duplicate"
9.4.6. Key of the Key Box must be at the custody of the Guard-on-Duty.
9.4.7. All keys must be numbered and labeled with department / section name.
9.4.8. Cases of Lost, misplaced or stolen keys, concerned employee is required to report such incident within 24 hours to the EHSS Department for immediate action
9.4.9. EHSS department shall conduct investigation upon receiving the report with corrective action
9.4.10. If lost, misplace or stolen keys are not retrieved, automatically replace the locking system, update key inventory and master list
9.4.11. Security officer shall communicate the changes to responsible personnel for monitoring

9.4.12. Sanction will be based on CCD or escalation policy
9.4.13. Issuance and usage of locking devices and keys should be properly recorded and monitored in the Key Borrowers' Logbook maintained by the security personnel.
9.4.14. Borrowed keys for facility doors and door of every rooms should be returned 1 hour after opening and closing of the facility
9.4.15. Security personnel will call out the attention of the personnel who borrowed key that will not return the keys with in 1hr. and conduct investigation and issue incident report.
9.4.16. Inventory of facility keys should be conducted daily by the security personnel
9.4.17. EHSS department is the only authorized department to keep duplicates of these
9.4.18. Asset Management will keep the triplicates of these access keys.

9.5. Security Technologies

9.5.1. The facility through IT department shall established policy and procedures governing the use, maintenance and protection of security technology in place? Security technology includes but is not limited to: intrusion alarm system (IDS), CCTV system, electronic access system (EAC)
9.5.2. Security technology policies and procedures been reviewed and updated annually, or more frequently as risks or circumstances dictate
9.5.3. Security technology should be utilized to monitor activities inside and outside, detection and prevention of unauthorized entry to sensitive areas this may include but not limited to :
9.5.1.1. Finish goods storage
9.5.1.2. Shipping and receiving areas
9.5.1.3. Shipping office
9.5.1.4. HR office
9.5.1.5. IT server/room
9.5.1.6. Inspection room
9.5.1.7. Logistics warehouse/office
9.5.1.8. PPIC
9.5.1.9. MD room
9.5.1.10. QC office
9.5.1.11. Loading/dispatch area
9.5.1.12. Washlab
9.5.1.13. Outside and facility perimeter the facility to monitor activities both inside And outside the facilities
9.5.2. The security technology here may refer to
9.5.2.1. CCTV
9.5.2.2. IDS
9.5.2.3. EAC
9.5.3. General requirements for security technology
9.5.3.1. Security officer shall ensure that only certified equipment are installed
9.5.3.2. Security officer shall ensure to secure certificate from service providers and Maintenance of security technology
9.5.3.3. Inspection of security technologies should be conducted monthly by the ff;
9.5.3.3.1. CCTV/EAC – IT personnel
9.5.3.3.2. IDS – Security officer
9.5.3.4. Responsible to conduct inspection to security technology must be

Knowledgeable and received training in particular

9.5.3.5. Training record must be kept by security officer

9.5.3.6. Access to security technology should be restricted to authorized personnel only

9.5.3.7. Cases of Lost or stolen Security technology such as CCTV, EAC, and IDS, concerned employee is required to report such incident within 24 hours to the EHSS Department for immediate action

9.5.3.8. EHSS department shall conduct investigation upon receiving the report with corrective action

9.5.3.9. If lost or stolen Security technology are not retrieved, automatically replace items and update

9.5.3.10. Sanction will be based on CCD or escalation policy

9.1. CCTV

9.1.1. Video surveillance cameras should be provided and utilized to sensitive areas to monitor the activities inside and outside of the sensitive areas

9.1.2. Recording of CCTV camera should be 24/7

9.1.3. The facility shall keep a record of the CCTV monitoring for at least 60 days

9.1.4. IT personnel must be logged thru monitoring logbook in the event of changing DVR, during review of compliance auditor and etc.

9.1.5. Monitoring of the CCTV shall be done by the assistant EHSS Manager/Supervisor, IT personnel and the guard on duty hence, CCTV monitors shall be provided at the IT room and at the guard's station.

9.1.6. Access to viewing recorded CCTV activities shall be authorized by the Assistant EHSS Manager

9.6.7. Assistant EHSS manager/supervisor or security officer shall conduct random weekly Review of CCTV footage to check/identify any incidents

9.1.7. Any incident found during review of CCTV footage should have incident report and Corrective action

9.6.9. Records of review and incident report must be kept at least 1 year by security office

9.6.10. The entire system, including the digital video recorder (DVR) server, field cameras, Power supplies, and other head-end equipment, should meet the following standards:

9.6.10.1. UPS backup for a minimum of four (4) hours (or one (1) hour if backup power generator is in place)

9.6.10.2. Control panel and all devices fixed on secure side of doors

9.6.10.3. Hardwired and secure from tampering; no accessible plugs or transformers

9.6.11. Basic requirements and settings of CCTV camera and DVR:

9.6.11.1. CCTV camera and DVR video resolution preferably HD compatible (1280 x 720 pixels). Minimum standard: 640 x 480 pixels

9.6.11.2. Minimum Refresh / frame rate: twelve (12) frames/second

9.6.11.3. Uninterrupted and continuous recording

9.6.11.4. Able to re-start recording automatically after power outage

9.6.11.5. DVR is able to playback and record simultaneously

9.6.12. CCTV cameras should be able to record properly during day and night (colour / B&W switching) with night vision capability. Cameras should be properly installed to compensate for any backlight situation or over-brightness. All video footage should clearly capture any movement of a subject

9.6.13. In case of system failure, the CCTV recorder will sound an alarm, or send an email/SMS to IT in-charge HR manager/supervisor and safety officer. IT in-charge and

safety officer should record all system failure of CCTV camera and submit incident report to HR manager. Incident report should be kept by safety officer and IT in-charge.

9.7. Intrusion Detection System

9.7.1. Automatic intrusion detection or automatic alarm systems should be provided to sensitive areas to detect unauthorized entry

9.7.2. UPS backup for a minimum of four (4) hours (or one (1) hour if backup power generator is in place

9.7.3. In case of intrusion detected through the Alarm Systems, Guard-on-duty will check the Control Panel of the Burglar Alarm System in its location or at the lobby. Once determined the specific area or location based on the numbering system in the Burglar Alarm System (in red lightning as indicator). Guard-on-duty shall:

9.7.4. Proceed to the area to check or investigate the intrusion.

9.7.5. In case of confirmed intrusion, Guard-on-duty will report the incident by calling Assistant EHSS Manager/Supervisor or Factory Manager, when facility has no duty.

9.7.6. Guard-on-duty will document the intrusion through an Incident Report and submit to Assistant EHSS Manager/Supervisor.

9.7.7. Assistant EHSS manager will further investigate the incident and take necessary action.

9.7.8. Incident report/record must kept at least 1 year by the security officer

9.8. Electronic Access Control

9.8.1. Electronic Access Control system should be provided to sensitive areas to prevent unauthorized entry

9.8.2. Security officer through security personnel must control the issuance and distribution of access biometrics to employees

9.8.3. IT personnel should review EAC logs week and send to department heads weekly for review

9.8.4. Any abnormalities or unauthorized entry found upon review should be reported to assistant EHSS manager/supervisor via incident report for investigation

9.8.5. EAC system installed must meet the following minimum standards

- 9.8.5.1. Biometric access control
- 9.8.5.2. UPS backup for a minimum of four (4) hours (or one (1) hour if backup Power generator is in place)
- 9.8.5.3. Control panel and all devices fixed on secure side of doors
- 9.8.5.4. Hardwired and secure from tampering; no accessible plugs or transformers

9.8.6. EAC monthly test at least include the following criteria:

- 9.8.6.1. Functioning
- 9.8.6.2. Authorized user list
- 9.8.6.3. Administrator password
- 9.8.6.4. Hardware installations
- 9.8.6.5. Real Time
- 9.8.6.6. Unauthorized personnel
- 9.8.6.7. Abnormal entry

9.8.7. Incident report/record must kept at least 1 year by the security officer

9.9. Opening and closing of the facility

9.9.1. Both Safety officers/Electrical Personnel on duty and Security Personnel on duty to conduct and implement this protocol without fail
9.9.2. Opening and closing logbook shall be in place and maintain by security officers
9.9.3. Opening and closing of facilities shall be signed by both safety officers/electrician personnel
9.9.4. Any abnormalities found upon opening and closing shall be reported to assistant EHSS manager and supervisor via incident report for investigation
9.9.5. Investigation report shall be kept by security officer at least 1 year

9.10. **Gate and Gate Houses:**

9.10.1. Gates through which the vehicles and/or personnel enter or exit must be manned by authorized security personnel and/or monitored 24 hours a day including non-working days. The number of gates should be kept to the minimum necessary for proper access and safety.

9.11. Physical security checks shall be done on a weekly basis by Security personnel
9.12. Identified issues found during weekly physical security inspection should be reported to security officer via incident report for investigation
9.13. All issues found during weekly physical inspection must have corrective action and should be monitored and verify until closure
9.14. Weekly inspection records and investigation report must be kept by security officer at least 1 year

9.15. List of Employees Access Privilege

9.15.1. Security officer shall give an up-to-date list of employee's privilege, key personnel (All areas pass) and approving signatories to Security SIC/Head guard for any changes And to department heads to identify non-organic personnel to the ff. Sensitive areas but Not limited to:
9.15.1.1.. Finish goods storage
9.15.1.2. Shipping and receiving areas
9.15.1.3. Shipping office
9.15.1.4. HR office
9.15.1.5. IT server/room
9.15.1.6. Inspection room
9.15.1.7. Logistics warehouse/office
9.15.1.8. PPIC
9.15.1.9. MD room
9.15.1.10. QC office
9.15.1.11. Loading/dispatch area
9.15.1.12. Washlab
9.15.2. List of employees should be posted at entrance to every sensitive areas for verification Purposes of non-organic person wish to entry
9.15.3. Copy of list of employees at guard house and posted to sensitive areas must have an Approval by department heads and assistant EHSS manager/supervisor
9.15.4. Security officer should also kept copy of list of employee's access privilege to sensitive Areas

9.16. **Internal/External Communication**:

9.16.1. EHSS Department must ensure that important Telephone numbers of internal security, Factory manager, HR manager, assistant EHSS manager/supervisor and Security officer must be posted conspicuously inside the offices of the facility and external telephone numbers of external security forces should be posted at guard station.

9.16.2. List of Telephone Numbers must also indicate the name/designation of person to contact when reporting a specific case or situation.

9.16.3. Upon detection of any unlawful activity and/or suspicious acts or activities, the concerned employee must inform the factory security personnel, Factory manager, HR manager, assistant EHSS manager/supervisor

9.16.4. Internal security must record at Daily Occurrence Book (DOB) of every incident/report regarding unlawful activity and/or suspicious act. Incident report must contain the following information:

9.16.4.1. Date and Time the incident is reported

9.16.4.2. Person Contacted or person to whom the incident was reported to

9.16.4.3. Nature of the incident/specific case or situation

9.16.4.4. Action taken by the concerned person

9.16.4.5. Name and designation of the person who reported the incident

9.16.5. If the situation is beyond what the internal security can handle, then internal security must ask for reinforcement from external security force or local law enforcement.

9.16.6. All reported unlawful activity and or suspicious act or activities should be investigated by the factory manager, HR manager and assistant EHSS manager/supervisor

9.16.7. Security Department and EHSS department must kept record of incident report

9.16.8. Incident report must be kept at least 1 year

10. Physical Access Control

10.1. Employees Access Control

10.1.1. All employees must wear company ID and uniform upon entering and within the facility at all Times.

10.1.2. All employees' company ID shall have the following information:

10.2.2.1. Employee Photo

10.2.2.2. Employee Name

10.2.2.3. Section/Department

10.2.2.4. Employee Signature

10.1.3. All employees company ID are reviewed on an annual basis thru system generated Master list by HR department

10.1.4. Consolidated company ID'S subject for replacement should be in place

10.1.5. Record of ID replacement should be available

10.1.6. All employees (including factory management, adidas Group personnel who are Deployed to work on that particular site on a daily basis), are subject to a standard Entry-exit control measures

10.1.7. Adidas staff who work on-site must also wear their own adidas staff card at all time in The facility

10.2. **Access to Sensitive Areas**

10.2.1. Organic personnel or personnel assigned in sensitive areas should have issued a color Coded access pass and must be replaced as needed

10.2.2. It must be worn at all times inside the premises

10.2.2. Other employees and non-organic personnel shall secure corresponding access pass at The security guard station prior going to sensitive areas

10.2.3. Other employees and non-organic personnel must log in/out to unauthorized access Logbook

10.2.4. Access pass adopts a color-coding scheme to identify areas to access.

- 10.2.4.1. Visitors pass (all areas but with management Representative except for PISP
- 10.2.4.2. Green : warehouse access only
- 10.2.4.3. White : all area pass
- 10.2.4.4. Yellow : logistics access only
- 10.2.4.5. Admin access only (include applicants, suppliers, sub- contractors and contractors)
- 10.2.4.6. Pink: for factories with ATM machines
- 10.2.4.7. Orange for inspection

10.2.5. Monthly inventory of access pass should be conducted by the security personnel

10.2.6. Cases of lost or misplace access pass , concerned employee is required to report such incident within 24 hours to the EHSS Department for immediate action

10.2.7. EHSS department shall conduct investigation upon receiving the report with corrective action

10.2.8. In case lost or misplace access pass are not retrieved, Security officer shall immediately update the master list To prevent unauthorized usage and access to any areas

10.2.9. Employees who lost issued access pass shall be issued NTE or notice to explain by HR IR

10.2.10. Sanction will be based on CCD or escalation policy

10.2.11. Access pass must have affixed signature by HR manager/Assistant EHSS manager/ Supervisor with control number.

10.2. Challenging and Removing Unauthorized Persons

10.3.1. The facility through the assistant EHSS manager/supervisor and EHSS manager shall Established security guard policies and procedures that clearly list the security guards' Duties and responsibilities and conduct annual review if policy is being followed

10.3.2. Any person inside the company premises noticed to be not wearing the proper ID shall Be immediately identified by the factory security and will be requested to present their Identification card.

10.3.3. In the event that this person has an unauthorized entry to the factory, factory security Personnel shall take custody of this person and take the appropriate action for this Violation.

10.3.4. Any personnel who express intentions to enter factory premises are duly verified Through the presentation of valid identification card and with the confirmation of the Person whom the former wishes to transact business with. The absence of both Requirements, above-Mentioned person shall not be admitted to the company Premises

10.2.8. Any employee who have identified unauthorized personnel in the facility or on restricted area where issued pass prohibits entry level of the badge, the employee shall challenge

the unauthorized personnel by asking for his identification and address the latter's concerns on the area.

10.2.9. An employee who has identified such unauthorized entry shall immediately report the unauthorized personnel to the security office and/or Factory Management for investigation.

10.3. Issuance, Removal and Charging of Access Devices

10.4.1. Issuance of company access devices but not limited to mobile phone, tablets, note book computer as well as the IT devices e.g. hardware and software shall be monitored by the EHSS Department through assets custodian and IT department and shall be returned / surrendered to the latter upon separation of employment.

10.4.2. A terminated/separated employee shall not be issued an exit clearance if all issued access devices has not been properly endorsed.

10.4.3. All issued company access devices and IT device are documented by the properties custodian and IT department and shall be removed when an employee has been separated from employment.

10.4.4. IT access like password shall be deactivated by the IT In-Charge upon separation of employment after asking the confirmation from the department heads. IT In-Charge shall immediately terminate link and access of the employee to any IT programs.

10.4.5. All issued company and PEZA ID shall be surrendered to the HR Associate (Recruitment) upon processing for exit clearance.

10.4.6. Cases of lost company access devices and IT device, concerned employee is required to report such incident within 24 hours to the EHSS Department for immediate action. The employee shall further furnish the department with an affidavit of loss to support the incident.

10.4.7. Cases of lost or stolen company access devices and IT device, concerned employee is required to report such incident within 24 hours to the EHSS Department for immediate action

10.4.8. EHSS department shall conduct investigation upon receiving the report with corrective action

10.4.9. In case lost or stolen company access devices and IT device are not retrieved, properties custodian and IT department shall immediately change the device. Security personnel shall immediately monitor any anomalous activity surrounding the area where the device is located

10.4.10. Employees who lost issued company access devices and IT device shall be issued NTE or notice to explain by HR IR

10.4.11. Sanction will be based on CCD or escalation policy

10.5. Visitors Access Control

10.5.1. Visitors, applicants, sub/ contractors, Couriers, Suppliers are required to present valid ID/government issued ID's in the guard station. Upon verification by the security personnel, he/she shall issue a security access pass. The issued security access pass shall be worn at all times inside the company premises.

10.5.2. Security guards are to verify with the HR or EHSS Department if the visitors, applicants, sub/contractors had an appointment. Upon verification by the security personnel, security personnel logs information of the visitors in the visitors logbook

10.5.3. Visitor's transactions are logged in the visitors Logbook containing the date, the name of

visitor, Identification Card presented, purpose of the visit, specific person/department to be visited, ID pass number, the time in/out and signature of the visitor, purpose and will then store the visitor's logbook away from public and unauthorized viewing

10.5.4. Visitors are escorted to their destinations where applicable upon due verification and confirmation with the person's they wished to transact business with.

10.5.5. All visitors, applicants, sub/ contractors, Couriers are subject to a standard entry-exit control measures, including visitor escorts, baggage checks, and vehicle searches. Exceptions are only allowed for VIP visitors

10.5.6. All visitors, applicants, sub/ contractors, Couriers, suppliers shall be check via metal detector to check if no fire arms brought inside the facility

10.6. Vehicles

10.6.1. Vehicles entering/ exiting the factory premises will be inspected with 7 points inspection Vehicle driver should stay at guard station

10.6.2. Vehicle should be logged in vehicle logbook containing date, time in/out, Driver Name, truck number/plate number and assigned security guard who conduct inspection

10.7. Control of Access to mails and parcel

10.7.1. All deliveries except for cartons will only be up to the guard station.

10.7.2. Guard on duty shall screen all mails and packages before endorsing it to the receptionist.

10.7.3. All received mails and packages shall be recorded in mails and packages logbook by the security personnel

10.7.4. Responsible person to conduct inspection of mails and parcel must be trained

10.7.5. Training record shall be kept by security officer

10.7.6. Receptionist calls the mail addressee to claim his/her mail/package and record to receiving logbook

10.8. List of logbooks maintained in the guard station:

10.8.1. Visitors Logbook

10.8.2. Lost ID monitoring Logbook

10.8.3. Contractor's Logbook

10.8.4. Daily Occurrence Book

10.8.5. Suppliers Logbook

10.8.6. SCI Incoming Employees Logbook

10.8.7. Key Borrowers Logbook

10.8.8. Key Inventory Logbook

10.8.9. Opening/Closing Monitoring Logbook

10.8.10. Mail and Packages Logbook

10.8.11. Keeping of books shall be in 1 year by the security SIC/Head guard

11. Personnel Security

11.1. General Requirements

11.2. Pre-employment Verification

11.2.1. Background checking of prospective employees
11.2.2. NBI clearance
11.2.3. PSA/NSO authenticated birth certificate

11.3. Periodic Checks and Reinvestigation

11.3.1. Updated list of employees in sensitive positions should be available and reviewed in annual basis or as need arises by the security officer
11.3.2. List of employees in sensitive positions shall be prepared by security officer, noted by assistant EHSS manager/supervisor and approved by factory manager
11.3.3. Annual check and background investigation shall be performed to all employees in sensitive positions
11.3.4. All employees in sensitive positions shall renew their NBI clearance one (1) month prior the expiry date annually
11.3.5. Sensitive positions include staff working directly with cargo or its documentation as well as personnel involved in controlling access to sensitive areas or equipment. Such positions include but not limited to, Managers of (factory, production HR, PPIC, QC, Supply, TSD), assistant EHSS managers/Supervisor, supervisors of (shipping, HR, FG, Warehouse), team leaders for (Shipping, FG, Warehouse), Associates of (Shipping, FG), Processor, IT support, IT Engineer, Sr. programmer, Programmer, system administrator, network engineer, Hr. IR, Hr. Recruitment, FG (clerk, HED, Sipping associates, Electricians, building engineers, safety officers, technicians, and utility),CWH (safety officers), EHSS security officers, factory (logistics personnel, scanner, clerk, packer), Security Guards, Seal in-charge and CPRD drivers as they all are allowed access to certain areas where finish product stored
11.3.6. Annual update of all employees' information shall be conducted regardless of sensitivity of the position
11.3.7. NBI clearance and background investigation shall be kept by security officer and annual update of employees information shall be kept by HR department at least 1 year

11.4. Personnel Termination Procedure

11.4.1. The company abides by the provision of the Labor Code of the Philippines regarding employee separation.
11.4.2. All moves for separation should be forwarded to the HRD for initial action.
Separation may be in the form of:
11.4.3. Termination of just cause or gross violation of existing company rules and regulations may be effected immediately after due process has been observed.
11.4.4. When the decision to terminate has been rendered, the HRD Manager shall serve the Termination Notice to the Employee.
11.4.5. If the employee refuses to sign, HRD manager shall indicate "refused to sign" and shall have it attested by a witness. In such cases, the refusal to sign does not mean the sanction is suspended
11.4.6. A copy of the Termination Notice shall be sent to the employees last known address by registered mail. The process of sending the notice to the employee shall be observed 3 times, while for AWOL (4 times and Last notice will be the termination notice) in case that the first and second attempt fails to reach the employee.
11.4.7. Shall the employee accepts the Termination, the HRD Manager, then discuss to the employee the procedure on how employee shall process his exit clearance and availment of benefits.

11.4.8. Authorized cause due to retrenchment to prevent losses, closure or cessation of operation and when employee is suffering from a disease not curable within The period of 6 months and his/her continued employment is prejudicial to His/her health or to the health of his/her co-employees.

11.4.9. Resignation of the employee by serving at least 15 days' notice.

11.4.10. An exit clearance form shall bear the flow of which the employee needs to declare And submit issued items, supplies and access.

11.4.11. Issued supplies shall be returned to the property custodian while IT access be Cleared by the IT Department. Issued identification badges, keys and files must be Endorsed to the HR Supervisor.

11.4.12. HR Supervisor shall verify that all items on the exit clearance are properly Accomplished before final clearance is issued to the employees

11.4.13. The separated employee's name, photo, date and reason of separation shall be Endorsed to the security personnel every month to aid them in controlling access to the Factory and must be kept in high confidentiality.

11.4.14. Should a separated employee wish to enter the factory premise, the following items? Shall be observed:

11.4.15. They are required to present valid ID at the guard station. Upon verification by the Security personnel, he/she shall issue a security ID. The issued security ID shall be Worn at all times inside the company premise.

11.4.16. Transactions are logged in the Visitor's Logbook including the time in / out and Purpose of the visit.

11.4.17. Once confirmed by the HR Manager or his/her authorized representative, the Separated employee is escorted to the HRD office and discuss what they wish to Transact.

11.4.18. Security guards must ensure the completeness of the visitor(s) logged information And will then store the visitor's logbook away from public and unauthorized Viewing

11.4.19. Once confirmed by the HR Manager or his/her authorized representative, the Separated employee is escorted to the HRD office and discuss what they wish to Transact.

11.5. Employees Code of Conduct

11.5.1. All employees must receive copy for the outline of behaviors that are prohibited Stating policy of disciplinary actions for violations

11.5.2. Proof/acknowledgement receipt must be kept to employees individual 201 file by HR Department

11.6. Lost Identification Badges

11.6.1. An employee who has lost his/her Company ID shall report immediately to HRD through the HR Associate – IR

11.6.2. HR Associate - IR will give an incident memo to the employee concerned to write his/her explanation and such employee will process/submit an Affidavit of Loss to HRD so that a referral slip will be given to process a new ID.

11.6.3. HR Associate - IR will give the Security Personnel a list of employees who lost their company ID for identification, verification and monitoring of entry/exit every occurrence.

11.6.4. If security personnel recognizes and confirm employees had no/lost their company ID's, security personnel will immediately notify to HR department
11.6.5. Employees having lost company ID shall log in/out every day to lost ID monitoring logbook while waiting of ID replacement for recording and monitoring purposes.

12. Education Training and Awareness

12.1. EHSS Department in coordination with training department shall conduct an annual orientation and training to all its security guards, canteen personnel, contractor's/sub-contractors personnel and all employees in the facility for CTPAT policy and procedures.
12.2. Security officer through the department heads shall ensure internal procedures to the following special activity/process is in place;
12.2.1. Logistics
12.2.2. Loading/Unloading
12.2.3. 7 and 17 points inspection
12.2.4. Shipping
12.2.5. Receiving of mails and packages
12.2.6. Cargo handling
12.2.7. Ho to affix Seals
12.2.8. IT/Cyber Security
12.3. Security officer in coordination with the department heads and training department shall conduct annual special training to the following special activity/processes;
12.3.1. Logistics
12.3.2. Loading/Unloading
12.3.3. 7 and 17 points inspection
12.3.4. Pest Contamination inspection
12.3.5. Shipping
12.3.6. Receiving of mails and packages
12.3.7. Cargo handling
12.3.8. How to Seals
12.3.9. IT/Cyber Security
12.4. All Security Guards and Canteen personnel shall undergo CTPAT Security and Threat Awareness training prior to Deployment.
12.5. All newly hired employees shall undergo CTPAT procedures orientation on their first day of work
12.6. Training department in coordination to the responsible person who conduct the training shall conduct evaluation for training effectiveness at least twice a year
12.7. Documented CTPAT procedures shall publicized throughout the facility such as posters and bulletin boards
12.8. Training record e.g. system generated attendance and documents of training effectiveness must be kept by Security officer at least 1 year

1. FLOW CHART

1.1. n/a

2. FORMS

2.1. n/a

3. REFERENCES

3.1. None

4. ADMINISTRATION AND REVIEW:

4.1. SCI-Cebu shall implement this policy through the Human Resources Department.