C-TPAT Membership Security Model Summary

Report generated by: Carlos Farfan

Report generated at: Wed Sep 02 19:00:21 EDT 2020

C-TPAT Membership Security Model Summary

Business Type Information

Security Model Name	KIA MOTORS MEXICO SA DE CV				
Business Type	Foreign Manufacturer	**Status**	Validated	**CTPAT Account #**	05151486

Business Entity Information

Foreign Manufacturer
MID
MXKIAMOT777NUE
Dun and Bradstreet Number

Addresses

Primary Address	Secondary	Mailing	Address Type	Address Line 1	Address Line 2	City	Postal Code	Country	State
Y	N	Y	Headquarters	Av. Paseo de la Reforma No. 250	Capital Reforma Torre B Piso 16 Col. Juarez	Mexico D.F.	06600	Mexico	Districto Federal
N	Y	Y	Warehouse	Boulevard Kia No. 777		Pesqueria	66679	Mexico	Nuevo Leon
N	Y	Y	Main Office	Boulevard Kia No. 777		Pesqueria	66679	Mexico	Nuevo Leon

Contacts

Primary Contact	Officer	Employee	Consultant	User Email	Last Name	First Name	Initial	Title	Phone Number
N	N	N	Y	cfarfan@aes.org.co	Farfan	Carlos		Excecutive President	+5724899191
N	N	N	Y	aarizpe@aes.org.co	Arizpe	Alicia		Mexico Director	+5218111833506
Y	Y	N	N	fernando.rangel@kia-mexico.com	Rangel	Fernando		GA&S Manager	+52815998 6036

International

Mutual Recognition Agreement	Agreed
Mutual Recognition Programs	
Canada	

Security Profile

Upper Management Responsibility : Corporate Wide Security Measures

Have representatives from all of the relevant departments been incorporated into a cross-functional team to build a robust Supply Chain Security Program? Have these new security measures been incorporated into existing company procedures to create a more sustainable structure that emphasizes that supply chain security is everyone’s responsibility?

Partner Response:

Currently, we have a supply chain security committee, in this committee we see relevant security issues, the last meeting was held on January 9, 2020.

Team departments

-Security~ Responsible of physical security and assets protection, also CTPAT certification

-Human Resources~ Responsible of the hiring employees and the application of sanctions

-Purchasing~ Responsible for the selection of new suppliers,in addition to the contractual structure and audits

-IT~ Responsible for information security, network administrators and new technologies, employees and suppliers awareness

-Logistic & customs~ Responsible for the imports, procedures nd legal compliance

-Exports~ Responsible of exports, logistic and transportation

SCSS Comment :

none

Upper Management Responsibility : Audit Program

Is the supply chain security program designed with, supported by, and implemented by an appropriate written review component? The purpose of this review component is to document that a system is in place whereby personnel are held accountable for their responsibilities and all security procedures outlined by the security program are being carried out as designed. This is a requirement.

Partner Response:

The security department is in charge of make the internal and supplier audits. We have an annual work plan related to supply chain security. In this plan the internal audit is contemplated on November, 2020

I attach the 2019 internal audit evidence

SCSS Comment :

none

Upper Management Responsibility : Updating Audit Program

Is the review plan updated as needed based on pertinent changes in your organization’s operations and level of risk? This is a requirement.

Partner Response:

The frequency of the internal audit is annual, and we use the minimum security criteria established by the program.

The update of the internal audit program is carried out the first months of the year

SCSS Comment :

none

Upper Management Responsibility : Updates to Management

The role of a company’s upper management in CTPAT is to provide support and oversight to ensure the creation and maintenance of the company’s Supply Chain Security Program. To this end, do the CTPAT point(s) of contact (POC) provide regular updates regarding the progress or outcomes of any audits, exercises, or validations?

Partner Response:

We continually keep our senior management informed of planned and executed supply chain security activities

Some examples:

-Internal Audits
-Annual Program

SCSS Comment :

none

Upper Management Responsibility : POC Requirements

Are the POCs knowledgeable about CTPAT’s program requirements? This is a requirement.

Partner Response:

KMM is a company that exports 80% of its products to the United States, for us it is very important to comply with the minimum security criteria established by the program,

Every year the security team is trained through external consultants in various topics of C-TPAT, we also learn important news through the C-TPAT portal, follow CBP accounts on social networks, etc.

SCSS Comment :

none

Upper Management Responsibility : Statement of Support

In promoting a culture of security, is commitment to supply chain security and the CTPAT program demonstrated through a statement of support? Is the statement signed by a senior company official and displayed in appropriate company locations?

Partner Response:

KMM has a supply chain security policy, which is endorsed by senior management (President)

This policy is reviewed every year

SCSS Comment :

none

Risk Assessment : Conduct Risk Assessment

Is the amount of risk in supply chains documented? Has an overall risk assessment (RA) been conducted to identify where security vulnerabilities may exist? Does the RA identify threats, assess risks, and incorporate sustainable measures to mitigate vulnerabilities. Are CTPAT requirements specific to the role in supply chain taken into account? These are requirements.

Partner Response:

The risk assessment process takes the C-TPAT / AEO standard to determine the controls that KMM must implement to detect a specific risk scenario before happening.

SCSS Comment :

none

Risk Assessment : Map Supply Chain

Does the international portion of the risk assessment document or map the movement of cargo throughout the supply chain from the point of origin to the distribution center? Does the mapping include all business partners involved both directly and indirectly in the exportation/movement of the goods? As applicable, does mapping include documenting how cargo moves in and out of transport facilities/cargo hubs and noting if the cargo is “at rest” at one of these locations for an extended period of time? Cargo is more vulnerable when “at rest,” waiting to move to the next leg of its journey.

Partner Response:

We have international mapping in the supply chain, origin and destination

SCSS Comment :

none

Risk Assessment : Annual Review of RA

Are risk assessments reviewed annually, or more frequently as risk factors dictate? This is a requirement.

Partner Response:

The risk analysis is reviewed annually, and documented in the "Document Approval Cover Page" format

SCSS Comment :

none

Risk Assessment : Business Resumption

Are written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption?

Partner Response:

We have procedures related to business continuity plan related to the supply chain.

SCSS Comment :

none

Business Partners : Written Screening Process

Is a written, risk based process in place for screening new business partners and for monitoring current partners? This is a requirement.

Partner Response:

KMM conducts the selection of commercial partners in its Korea headquarters. A Hyundai Group company, Hyundai Mobis, located in the same industrial complex where the KMM plant is located, manufactures parts and inputs. This company is in the CTPAT and AEO certification process; additionally, the logistics supplier has been selected in Korea, being also part of the Hyundai Group (Hyundai Glovis).

Commercial partners who provide services to KMM are selected in Mexico, including transporters, customs agents, security, personnel outsourcing, and port control. Procedure COP16-P01 is used for these processes and additional security requirements are included in the KMM Supply Chain Security Guideline. Commercial partners are assessed in compliance with KIA Code of Ethics and Conduct. The Corporation has also set forth a Code of Ethics and Conduct for corporate purchases, as well as documents to determine compliance policies regarding gifts, ethical businesses, and fair trade regulations. http://pr.kia.com/en/company/about-kia/corporate-social-responsibility/trust-management.do

SCSS Comment :

none

Business Partners : MRA

Does the business partner screening process take into account whether a partner is a CTPAT Member or a member in an approved Authorized Economic Operator (AEO) program with a Mutual Recognition Arrangement (MRA) with the United States (or an approved MRA)? Certification in either CTPAT or an approved AEO is acceptable proof for meeting program requirements for business partners. Is evidence of the certification obtained and are business partners continuously monitored to ensure they maintain their certification? These are requirements.

Partner Response:

Every commercial partner is assigned a datasheet containing basic corporate data, contact information, and standards (C-TPAT/ AEO). There is also a list of critical commercial partners with their respective SVI Number and other relevant identification data. Commercial partners who have a C-TPAT certification do not require annual audits, but their facilities are visited on a yearly basis to review the process critical aspects and to guarantee the integrity of processes related to KMM. C-TPAT certified Commercial Partners, as well as those without this certification must fill out the C-TPAT Security Questionnaire. Additionally, it is reviewed on a yearly basis, to see whether they are included in the UN or OFAC restrictive /sanctions lists.

SCSS Comment :

none

Business Partners : Partners Must Meet Criteria

Where a CTPAT Member outsources or contracts elements of its supply chain, is due diligence exercised (via visits, questionnaires, etc.) to ensure these business partners have security measures in place that meet or exceed CTPAT’s Minimum Security Criteria (MSC). This is a requirement.

Partner Response:

KMM encourages its business partners to certify CTPAT . Similarly, sends a C-TPAT security questionnaire that includes all safety requirements, also requests a letter of commitment to implementation and maintenance of C-TPAT Security Requirements and annually verifies that C- TPAT requirements are met.

Commercial Partners datasheets indicate whether they are C-TPAT, or if they have any other AEO – Authorized Economic Operator type of certification. KMM encourages its eligible Commercial Partners to get their C-TPAT or NEEC certifications. Those who are not eligible are encouraged by KMM to become part of the PVP which annually verifies that they comply with the minimum security requirements.

SCSS Comment :

none

Business Partners : Correcting Weaknesses

If weaknesses are identified during business partners' security assessments, are they addressed as soon as possible and are corrections implemented in a timely manner? Is it confirmed that deficiencies have been mitigated via documentary evidence? These are requirements.

Partner Response:

When we detect any finding in the supplier evaluations, the finding is documented, corrective actions are requested and a commitment date is set. Subsequently it is audited that they have fulfilled

SCSS Comment :

none

Business Partners : Update Partner Assessments

To ensure that business partners continue to comply with CTPAT's security criteria, are security assessments of business partners updated on a regular basis, or as circumstances/risks dictate?

Partner Response:

Audits to business partners are performed annually, subsequently a visit is made to verify compliance or closure of the findings

SCSS Comment :

none

Business Partners : Subcontracted Carriers

For inbound shipments to the United States, if subcontracting transportation services to another highway carrier, is a CTPAT certified highway carrier used or a highway carrier that works directly for the member as delineated through a written contract? Does the contract stipulate adherence to all minimum security criteria MSC) requirements? These are requirements.

Partner Response:

The carriers that we hire to ship our product have the C-TPAT certification. The contractual party also specifies the commitment they must have with the security program

SCSS Comment :

none

Business Partners : Forced Labor

Is a documented social compliance program in place that, at a minimum, addresses how the company ensures goods imported into the United States were not mined, produced or manufactured, wholly or in part, with prohibited forms of labor, e.g., forced, imprisoned, indentured, or indentured child labor?

Partner Response:

KMM is certified as a socially responsible company (ESR)

KMM establishes as main standards in its organizational culture, ethics, morals, and everything that refers to values.

SCSS Comment :

none

Procedural Security : Information

Are procedures in place to ensure that all information used in the clearing of merchandise/cargo is legible, complete, accurate, protected against the exchange, loss, or introduction of erroneous information, and reported on time? This is a requirement.

Partner Response:

For vehicle storage, shipping, and transit to railroad terminals, the border, or maritime ports, transport companies offer traceability and registries generated in the VPC by Glovis. Carrier procedures include the description of tools used to know the exact position of the trailer at a given time. Vehicle routes and transit times are also identified, as well as inspection time and places. In addition, transporters have in place emergency plans in case there is an unexpected stop during the transportation process (roadblocks, route changes, mechanical failures, accidents, etc.) Hyundai Glovis, as the logistical operator, guarantees the performance and compliance with the placement of seals in three (3) levels and Automax, to ensure the integrity of each seal, once secured to the railcar. Documents are duly filled out with the seal serial numbers to comply with C-TPAT norms and requirements. Internally, before being shipped, vehicles are stored at VPC yard until the SAP system programs their shipment. Before taking a vehicle to PDI (Pre- Delivery Inspection), a brief inspection is performed to detect damages, missing parts, or exceeding parts. Once at PDI, a detailed inspection is performed to each vehicle, opening every compartment to make sure unauthorized elements are not present. This activity is registered by IQIS (Internal Quality System) and SAP. Finally, vehicles are sorted by programmed destination in a tender area to be loaded in the trailer

SCSS Comment :

none

Procedural Security : Weight, and Piece Count

Are the weight and piece count accurate? This is a requirement.

Partner Response:

At this vehicle-processing center, an exhaustive vehicle control takes place in terms of Quality and Security. Every activity performed at the VPC by personnel of the company contracted for this last phase of the vehicle manufacturing process is registered at the RPs (Reporting Points). RPs are constantly monitored by SAP systems, the main ones being: A vehicle becomes an inventory unit through a VIN scanning process, once it leaves the KMM production line and goes into VPC. The vehicle is externally inspected there and added to VPC inventory. The security officer verifies each vehicle, before it is loaded, against the transporter shipment documents (VIN vs. document).

SCSS Comment :

none

Procedural Security : Shipping Documents, Timely Filing

Does the shipper or its agent ensure that bill of ladings (BOLs) and/or manifests accurately reflect the information provided to the carrier, and do carriers exercise due diligence to ensure these documents are accurate? Are BOLs and manifests filed with CBP in a timely manner? Does BOL information filed with CBP show the first foreign location/facility where the carrier takes possession of the cargo destined for the United States? These are requirements.

Partner Response:

Before release each vehicle , the VIN is checked against the invoice , to ensure that the product leaving the plant is the one that really corresponds to the invoice. This process is also registered in SAP. All SAP system activities are in constant communication with VELES system, used by the Hyundai Glovis supplier, which is only accessible by authorized personnel. Shipping information is sent through the SAP system to internal users (Hyundai Glovis) and are e-mailed to commercial partners (customs agents and transporters).

SCSS Comment :

none

Procedural Security : Storing Forms

If paper is used, are forms and other import/export related documentation secured to prevent unauthorized use.

Partner Response:

KMM uses certain types of paper documents, including manifests, purchase orders, referrals, contracts, and bills of lading. To ensure the security of the documents we keep them in locked drawers, each department is responsible for maintaining control of their documents. The security team is responsible for carrying out "clean desk" security audits in which they check that the PCs are turned off, the drawers are locked and that there are no confidential documents on the work table, all this to comply with the security standards of C-TPAT / OAS / ISO27001

SCSS Comment :

none

Procedural Security : Staging Cargo Overnight

When cargo is staged overnight, or for an extended period of time, are measures taken to secure the cargo from unauthorized access? This is a requirement.

Partner Response:

When loading the units, there is always one person for transport, the loader and one security person. The security person is responsible for checking that what is shown on the manifest is what is being loaded. At the end of the loading, evidence is taken of the sealing (in the case of wagons). It is important to mention that all loading areas are monitored by CCTV 24 hours a day and all the vehicles are inspected by security guards and K9 units.

SCSS Comment :

none

Procedural Security : Supervise Stuffing

Is the loading/stuffing of cargo into containers/IIT supervised by a security officer/manager or other designated personnel?

Partner Response:

All loads are supervised by the security department of Hyundai Glovis

When loading the units, Hyundai Glovis' security department documents through a cargo inspection form

SCSS Comment :

none

Procedural Security : Reconciliation of Cargo and Documents

Is arriving cargo reconciled against information on the cargo manifest? Is departing cargo verified against purchase or delivery orders?

Partner Response:

We do not have unit reconciliation, the vehicles we produce in the plant are the ones that are shipped only.

SCSS Comment :

none

Procedural Security : Investigate Anomalies

Are all shortages, overages, and other significant discrepancies or anomalies investigated and resolved, as appropriate? This is a requirement.

Partner Response:

VPC performs a final vehicle inspection to make sure it is complete, without missing parts or elements that should not be in it. GLOVIS Company, specialized in vehicle management, conducts this inspection. The inspection process is filmed and personnel who work in this area are not allowed to have anything in their pockets. In case there is a suspicious activity such as missing parts, or elements that should not be in the car, GLOVIS personnel immediately notify KMM personnel in order to report this to the authorities, if required, as well as KMM accountable personnel to conduct the respective analysis, find out the causes, and adopt appropriate corrective measures.

SCSS Comment :

none

Procedural Security : Challenging

Are procedures in place to identify, challenge, and address unauthorized/unidentified persons? Do personnel know the protocol to challenge an unknown/unauthorized person, how to respond the situation and are they familiar with the procedure for removing an unauthorized individual from the premises? These are requirements.

Partner Response:

At KMM we have 2 procedures that refer to the identification and removal of unauthorized persons from the facilities.

-Prevetive patrolllings procedure

-Supply chain contingency plan

SCSS Comment :

none

Procedural Security : Written Reporting Procedures

Are written procedures in place for reporting an incident to include a description of the facility's internal escalation process? Is a notification protocol in place to report any suspicious activities or security incidents that may affect the security of the member's supply chain? As applicable, are incidents reported to the SCSS, the closest port of entry, any pertinent law enforcement agencies, and business partners that may be part of the affected supply chain? Do notification procedures include the accurate contact information that lists the name(s) and phone number(s) of personnel requiring notification, as well as for law enforcement agencies? These are requirements.

Partner Response:

If suspicious activity is detected, the security officer , according to the procedure of reporting suspicious transactions , communicate with CBP and AEO -
SAT personnel.

SCSS Comment :

none

Procedural Security : Notifying CBP

Are notifications to CBP made as soon as feasibly possible and in advance of any conveyance or IIT crossing the border?

Partner Response:

The process for notifying CBP in case of some event or incident is documented in the supply chain contingency plan

SCSS Comment :

none

Procedural Security : Review of Reporting Procedures

Are procedures periodically reviewed to ensure contact information is accurate? This is a requirement.

Partner Response:

We don't have a process as such

We have a list of security contacts and this is updated whenever we are informed of any changes

SCSS Comment :

none

Procedural Security : Anonymous Reporting

Has a mechanism been established to report security related issues anonymously? When an allegation is received, is it investigated, and if applicable, are corrective actions taken?

Partner Response:

KMM has an email for anonymous complaints kmmdenuncia@kia-mexico.com

SCSS Comment :

none

Procedural Security : Internal Investigations

Are internal investigations performed immediately after an incident? Is the investigation documented? This is a requirement.

Partner Response:

Any type of security incident is recorded, analyzed, followed up and corrective actions are taken.

We also have an incident management procedure

SCSS Comment :

none

Conveyance and IIT : Secure Storage IIT

Are conveyances and Instruments of International Traffic (IIT) stored in a secure area to prevent unauthorized access, which could result in an alteration to the structure of an Instruments of International Traffic or (as applicable) allow the seal/doors to be compromised? This is a requirement.

Partner Response:

All transports and international traffic instruments are protected within the facilities, our security filters include:
-Perimetral fence
-Access gates with padlock
-CCTV cameras (Thermal, PTZ, Bullet)
-Security guards at the accesses 24/7
-Monitoring cameras 24/7
-Extra security company (Hyundai Glovis)
-Lighting in the loading yards and perimeter

SCSS Comment :

none

Conveyance and IIT : Written Inspection Procedures.

Are written procedures in place for both security and agricultural inspections of IIT? This is a requirement.

Partner Response:

We have a documented procedure called "Inspection of cargo vehicles", in which the inspection process is explained, in recent months an update of the procedure was carried out, attaching information on the agricultural safety inspection

SCSS Comment :

none

Conveyance and IIT : Inspections

Prior to loading/stuffing/packing, do all conveyances and empty IIT undergo CTPAT approved security and agricultural inspections to ensure their structures have not been modified to conceal contraband or have not been contaminated with visible agricultural pests? Is a seven-point inspection on all empty containers and unit load devices (ULD), and an eight-point inspection on all empty refrigerated containers and ULDs conducted prior to loading/stuffing to include: 1. Front wall; 2. Left side; 3. Right side; 4. Floor; 5. Ceiling/Roof; 6. Inside/outside doors, including the reliability of the locking mechanisms of the doors; 7. Outside/Undercarriage; 8. Fan housing on refrigerated containers? Do these systematic inspections include: Tractors: 1. Bumper/tires/rims; 2. Doors, tool compartments and locking mechanisms; 3. Battery box; 4. Air breather; 5. Fuel tanks; 6. Interior cab compartments/sleeper; 7. Faring/roof? Trailers: 1. Fifth wheel area - check natural compartment/skid plate; 2. Exterior - front/sides; 3. Rear - bumper/doors; 4. Front wall; 5. Left side; 6. Right side; 7. Floor; 8. Ceiling/roof; 9. Inside/outside doors and locking mechanisms; 10. Outside/Undercarriage? These are requirements.

Partner Response:

At Kmm we have two types of cargo units: motherships and wagons, both units are inspected upon entering the facilities, the first inspection is carried out by a security officer and reviews the applicable checklist points, the second inspection is carried out by K9 handlers.

SCSS Comment :

none

Conveyance and IIT : Hardware

Are conveyances and IIT (as appropriate) equipped with external hardware that can reasonably withstand attempts to remove it? Are the doors, handles, rods, hasps, rivets, brackets, and all other parts of a container's locking mechanism fully inspected to detect tampering and any hardware inconsistencies prior to the attachment of any sealing device? These are requirements.

Partner Response:

All transports contracted by our supplier Hyundai Glovis have a satellite tracking system (Transportes Cuauthemoc, Kansas City)

Among the points to inspect the load units are the wagon doors, hinges, handles, supports, etc. are checked.

SCSS Comment :

none

Conveyance and IIT : Clean if Pests Found

If visible pest contamination is found during the conveyance/IIT inspection, is washing/vacuuming carried out to remove such contamination? Is documentation retained for one year to demonstrate compliance with these inspection requirements? These are requirements.

Partner Response:

We have a procedure for "inspection of cargo vehicles", if we find any type of contamination by pests or weeds, we return the cargo unit and access is not allowed until it returns decontaminated.

SCSS Comment :

none

Conveyance and IIT : Inspections at Yards

Are inspections of conveyances and IIT systematic and are they conducted at conveyance storage yards? Where feasible, are inspections conducted upon entering and departing the storage yards and at the point of loading/stuffing? These are requirements.

Partner Response:

Inspections of cargo units are carried out when entering and leaving the KMM facilities, in both situations physical inspections are carried out with a security officer and with the K9 units.

These inspections are carried out in different places, depending on the type of load unit. For example, in "Nodrizas", inspections are carried out when entering and leaving the premises. In the case of wagons, inspections are carried out once while inside the facilities on the internal tracks.

SCSS Comment :

none

Conveyance and IIT : Inspections in Secure Area

Are security inspections performed in an area of controlled access and, if available, monitored via a CCTV system?

Partner Response:

All cargo unit security inspections are conducted within a private and controlled area. All inspection operations are documented in CCTv

SCSS Comment :

none

Conveyance and IIT : Checklist

Is the inspection of all conveyances and IIT recorded on a checklist? Are the following elements documented on the checklist: container/trailer/instruments of international traffic number, date of inspection, time of inspection, name of employee conducting the inspection, and specific areas of the instruments of international traffic that were inspected?

Partner Response:

We have security inspections of the cargo units, these are documented in an inspection check list which contains the following items:

- Carrier line
- Name of the driver
- Economic numbers
- Plates
- Name of the K9 handler
- Inspection Date
- Inspection time
- Name and signature of the driver
- Name and signature of the security officer

SCSS Comment :

none

Conveyance and IIT : Supervisor’s Signature

If the inspections are supervised, does the supervisor should also sign the checklist?

Partner Response:

Inspections are supervised by the control and monitoring center only.
In this area, a CCTV inspection checklist is carried out in which the monitored activities are documented.

On the other hand, the security supervisor attends a supervision tour sporadically

SCSS Comment :

none

Conveyance and IIT : Checklist & Shipping Docs

Is the completed container/IIT inspection sheet part of the shipping documentation packet? Does the consignee receive the complete shipping documentation packet prior to receiving the merchandise?

Partner Response:

The inspection check list has 2 sheets, after filling and signing, a sheet is delivered to the driver of the cargo unit

SCSS Comment :

none

Conveyance and IIT : Management Surprise Inspections

Based on risk, does management conduct random searches of conveyances after the transportation staff have conducted conveyance/IIT inspections? Are searches of the conveyance done periodically, with a higher frequency based on risk? Are the searches conducted at random without warning, so they will not become predictable?

Partner Response:

Currently we do not carry out this type of surprise inspections, we are working on a plan to meet this criterion.

The company that provides us with transportation services (Kansas City) has this type of random inspections documented

SCSS Comment :

none

Conveyance and IIT : Location of Management Searches

Are inspections conducted at various locations where the conveyance is susceptible: the carrier yard, after the truck has been loaded, and en route to the United States border?

Partner Response:

Currently we do not carry out this type of surprise inspections, we are working on a plan to meet this criterion.

The company that provides us with transportation services (Kansas City) has this type of random inspections documented

SCSS Comment :

none

Conveyance and IIT : Written Seal Procedures

Are written high security seal procedures in place that describe how seals are issued and controlled at the facility and during transit? Are procedures in place that provide the steps to take if a seal is found to be altered, tampered with, or has the incorrect seal number to include documentation of the event, communication protocols to partners, and investigation of the incident? Are the findings from the investigation documented, and any corrective actions implemented as quickly as possible? Do written seal controls include the following elements? Controlling access to seals: management of seals is restricted to authorized personnel, secure storage, inventory, distribution, & tracking (seal log), recording the receipt of new seals, issuance of seals recorded in log, track seals via the log, and only trained, authorized personnel may affix seals to instruments of international traffic (IIT). Controlling seals in transit: when picking up sealed IIT (or after stopping), verify the seal is intact with no signs of tampering, confirm the seal number matches what is noted on the shipping documents, Seals broken in transit: if load examined--record replacement seal number, the driver must immediately notify dispatch when a seal is broken, indicate who broke it, and provide the new seal number; the carrier must immediately notify the shipper, broker, and importer of the seal change, and the replacement seal number; and the shipper must note the replacement seal number in the seal log. Seal discrepancies: hold any seal discovered to be altered or tampered with to aid in the investigation, Investigate the discrepancy, follow-up with corrective measures (if warranted), and as applicable, report compromised seals to CBP and the appropriate foreign government to aid in the investigation. These are requirements.

Partner Response:

Exports are conducted in two (2) types of transportation units. Vehicles, using trailers and containers on platforms. For containers, Glovis Mexico team is in charge of filling them with empty collapsible plastic crates. These containers are sealed with a high-security seal; a packing list is created with the information of the contents which will be uploaded into the GCS system to be able to create the commercial invoice. The Glovis Forwarding team is in charge of programming the collection of the containers at the KMM facilities and trace it until it arrives at the supplier facilities. Containers are shipped from the facilities to the railroad terminal on a truck platform and from the railroad terminal to the port by train. Once at the port, they are loaded into a ship that takes them back to the port in Korea. KMM logistics team is in charge of coordinating the export and gathering the required paperwork. For vehicles transported by trailer, and then by train, security seals are placed to the rail cars, in the train terminals; these seals are managed and controlled by the railroad transporter. Security seals that comply with ISO 17712 Standard are used. These are managed and controlled according to C-TPAT requirements.

SCSS Comment :

none

Conveyance and IIT : Annual Review

Are procedures reviewed at least once a year and updated as necessary? This is a requirement.

Partner Response:

All security policies and procedures including the security management system in the supply chain are reviewed annually and documented in a change history. This according to the document control procedure

SCSS Comment :

none

Conveyance and IIT : Local Level, Procedures

Are written procedures maintained at the local, operating level so that they are easily accessible? This is a requirement.

Partner Response:

All procedures related to security operations are found in security folders located in all the access booths where security personnel are working.

SCSS Comment :

none

Conveyance and IIT : ISO Seals

Are all CTPAT shipments that can be sealed secured immediately after loading/stuffing/packing by the responsible party (e.g. the shipper or packer acting on the shippers behalf) with a high security seal that meets or exceeds the most current International Standardization Organization (ISO) 17712 standard for high security seals? Qualifying cable and bolt seals are both acceptable. Are seals securely and properly affixed to IIT that are transporting CTPAT members' cargo to/from the United States? There are requirements.

Partner Response:

After loading the vehicles in the wagons, the security seals are placed, relevant information is documented such as the loading time, the economic number of the wagon, the seal numbers placed, the signatures of the people who are present at the Time of sealing (In the load there are always 3 different companies checking the load; Glovis Security, Glovis Operations, Rail Assist, Fast Automotive). The seals we use comply with ISO 17712 certification

SCSS Comment :

none

Conveyance and IIT : VVTT

Is CTPAT's seal verification process followed to ensure all high security seals (bolt/cable) have been affixed properly to IIT, and are operating as designed? The procedure is known as the VVTT process: V – View seal and container locking mechanisms; ensure they are OK; V – Verify seal number against shipment documents for accuracy; T – Tug on seal to make sure it is affixed properly; T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose. This is a requirement.

Partner Response:

After the wagon sealing, the Hyundai Glovis security officer performs the VVTT operation to ensure that the seals are properly placed.

When the loaded wagons are transferred to the final line, a second VVTT inspection is carried out, this is carried out by a KMM security officer and is carried out on a random basis

SCSS Comment :

none

Conveyance and IIT : Document ISO Compliance

Is it documented that the high security seals either meet or exceed the most current ISO 17712 standard? This is a requirement.

Partner Response:

All security seals comply with ISO 17712 standard

SCSS Comment :

none

Conveyance and IIT : Digital Photos

As documented evidence of the properly installed seal, are digital photographs taken at the point of stuffing?

Partner Response:

We have graphical evidence of all sealed cargo units

SCSS Comment :

none

Conveyance and IIT : Forward Photos

To the extent feasible, are these *images electronically forwarded to the destination for verification purposes? *photographs taken at the point of stuffing.

Partner Response:

Hyundai Glovis and Rail Assist are the companies in charge of taking graphic evidence of the sealing. These photos are only shared in case of any type of security incident

SCSS Comment :

none

Conveyance and IIT : BOL & Seal Number

Are seal numbers electronically printed on the bill of lading or other shipping documents?

Partner Response:

All security seals are registered on the shipping documents

SCSS Comment :

none

Conveyance and IIT : Transmit Seal Numbers to Consignee

Are seal numbers assigned to specific shipments transmitted to the consignee prior to departure?

Partner Response:

The information where the security seals are documented are sent once the load unit has left

SCSS Comment :

none

Conveyance and IIT : Seal Audits

If an inventory of seals is maintained, does company management or a security supervisor conduct audits of seals that includes periodic inventory of stored seals and reconciliation against seal inventory logs and shipping documents? Are all audits documented? As part of the overall seal audit process, do dock supervisors and/or warehouse managers periodically verify seal numbers used on conveyances and IIT? These are requirements.

Partner Response:

Hyundai Glovis is the company in charge of safeguarding security seals, they have an updated inventory. The seal audit is carried out by the transport company "Kansas City" on a random basis and as a second security filter, KMM performs a seal audit within the internal audit times.

SCSS Comment :

none

Conveyance and IIT : Members Tracking Conveyances

Is there a mechanism in place to work with transportation providers to track conveyances from origin to final destination point? Are specific requirements for tracking, reporting, and sharing of data incorporated within terms of service agreements with service providers?

Partner Response:

The Hyundai Glovis company is in charge of hiring the transport companies and tracking shipments, this company has a procedure called "Tracking shipments". As a requirement to be a business partner, the company requires the transport company to have a satellite tracking system and a mirror account is requested.

SCSS Comment :

none

Conveyance and IIT : Access to GPS

Is there a mechanism in place to access the carrier’s GPS fleet monitoring system to track the movement of shipments?

Partner Response:

As a requirement to be a business partner, the company requires the transport company to have a satellite tracking system and a mirror account is requested.

SCSS Comment :

none

Conveyance and IIT : Notify Partners of Threat

If a credible (or detected) threat to the security of a shipment or conveyance is discovered, are business partners in the supply chain that may be affected and any law enforcement agencies alerted (as soon as feasibly possible), as appropriate. This is a requirement.

Partner Response:

Within the documented procedure "shipment tracking" the process to follow in case of detecting an incident during shipment is described.
In summary, the transport company gives immediate notice to its client and this notifies the other business partners involved and the corresponding authorities.

SCSS Comment :

none

Conveyance and IIT : No Stop Policy

For land border shipments that are in proximity to the United States border, is a “no-stop” policy implemented with regard to unscheduled stops?

Partner Response:

This policy or procedure is not available, we will be working to apply it as soon as possible.

SCSS Comment :

none

Conveyance and IIT : Pre-border Inspection

In areas of high risk, and immediately prior to arrival at the border crossing, is a “last chance,” verification process incorporated for U.S. bound shipments for checking conveyances/IIT for signs of tampering to include visual inspections of conveyances and the VVTT seal verification process? Do properly trained individuals conduct the inspections? V – View seal and container locking mechanisms; ensure they are OK; V – Verify seal number against shipment documents for accuracy; T – Tug on seal to make sure it is affixed properly; T – Twist and turn the bolt seal to make sure its components do not unscrew, separate from one another, or any part of the seal becomes loose.

Partner Response:

The transport company performs this type of verification before the border crossing, Hyundai Glovis as a client audits that this process is carried out.

For our part, KMM will be developing a plan to jointly with Hyundai Glovis and Kansas City to carry out this audit.

SCSS Comment :

none

Agricultural Procedures : Written procedures

In accordance with the applicable business model, are there written procedures in place that are designed to prevent visible pest contamination to include compliance with Wood Packaging Materials (WPM) regulations? Do measures regarding WPM meet the International Plant Protection Convention’s (IPPC) International Standards for Phytosanitary Measures No. 15 (ISPM 15)? This is a requirement.

Partner Response:

Our product is loaded in "mother" freight vehicles and wagons. We do not use wood in any of the transports . However, all our shipping areas are in paved areas and are fumigated once a month.

SCSS Comment :

none

Agricultural Procedures : Implement Pest Prevention

Are visible pest prevention measures adhered to throughout the supply chain? This is a requirement.

Partner Response:

The supplier audit plan included an inspection focused on the prevention of insect pests and weeds, especially in shipping areas.

SCSS Comment :

none

Agricultural Procedures : Cargo Staging Areas Pest Inspection

Are cargo staging areas, and the immediate surrounding areas, inspected on a regular basis to ensure these areas remain free of visible pest contamination? This is a requirement.

Partner Response:

Cargo vehicles are inspected by the security departments of KMM and Hyundai Glovis before being loaded. This inspection checks for the presence of visible pests or any type of weeds. If any deviations are detected, an incident report is made and followed up.

SCSS Comment :

none

Physical Security : Physical Deterrents

Are there physical barriers and/or deterrents in place to prevent unauthorized access to offices, trailer yards, cargo handling and storage facilities? This is a requirement.

Partner Response:

A 2.5 meters high perimeter fence was installed surrounding the rail operations yard and 3 access gates to control the access to that area. 3 fix security guards and 1 patroles were assignated to protect the rail operation yard.

Storage areas of the vehicles is enclosed with perimeter fencing and controlled with a CCTV system . The import container yard also is enclosed with perimeter fencing and controlled with a CCTV system.

We have K9 agents in all the vehicle entrance:

-Logistic Gate 1 - 2 K9
-Logistic Gate 2 - 2 K9
-Logistic Gate 3 - 2 K9
-Logistic Gate 4 - 1 K9
-Logistic Gate 5 - 1 K9
-Rail Road - 2 K9

SCSS Comment :

none

Physical Security : Perimeter Fencing

Does perimeter fencing enclose the areas around cargo handling and storage facilities?

Partner Response:

The production areas are independent and are kept closed . Storage areas for vehicles not separate domestic or export products; all vehicles are handled as if they were products export. The VPC (Vehicle Process Center) where vehicles are stored , is a restricted area and enter only employees working in this area , who are identified with different uniform than those of other areas

SCSS Comment :

none

Physical Security : Interior Fencing

If a facility handles cargo, is interior fencing used to secure cargo and cargo handling areas? Based on risk, does additional interior fencing segregate various types of cargo such as domestic, international, high value, and/or hazardous materials?

Partner Response:

We have 2 exclusive yards for the storage areas and 2 exclusive yards for the cargo areas, both separated by more than 300 meters and with a dividing fence. In one yard, cargo is loaded in "Nodrizas" and in the other one in railroad wagons

SCSS Comment :

none

Physical Security : Inspecting Fencing

Is fencing regularly inspected for integrity and damage by designated personnel?

Partner Response:

We have a perimeter fence in all installations which is checked every day by a security officer who is in charge of the perimeter patrolling. If any anomaly is detected, a report is made and then sent to the facilities department for repair.

SCSS Comment :

none

Physical Security : Repairing Fencing

If damage is found in the fencing, are repairs made as soon as possible?

Partner Response:

Damages detected in our perimeter fence are immediately reported and repaired

SCSS Comment :

none

Physical Security : Gates

Are gates where vehicles and/or personnel enter or exit (as well as other points of ingress/egress) manned or monitored? This is a requirement.

Partner Response:

We have 11 accesses to the facilities:

Pedestrian
-EG1
-EG2
-EG3

In all the accesses we have security guards, physical controls (turnstiles, card reader), metal detector arches, surveillance cameras and presence of K9 agents

-Visitors Gate

In this access we have security guards, physical controls (turnstiles, card reader), metal detector arches, surveillance cameras and temporary presence of K9 agents

Vehicles
-LG1
-LG2
-LG3
-LG4
-LG5

In these access we have security guards, physical controls (vehicle barriers), surveillance cameras and presence of K9 agents

-Rail Road 1
-Rail Road 2

In these accesses we have 2 watch towers, access gates, security guards, surveillance cameras (Railroad crossing)

SCSS Comment :

none

Physical Security : Parking

Are private passenger vehicles prohibited from parking in or adjacent to cargo handling and storage areas, and conveyances?

Partner Response:

Parking lots are outside of the facilities. Employee vehicles are not allowed in the facilities.
Only the CEOs, and Directors vehicles are allowed in the facilities in a pre-assigned parking space, away from loading operations. Access to parking areas is controlled by vehicle control bars activated by employees identification badges.

SCSS Comment :

none

Physical Security : Lighting

Is adequate lighting provided inside and outside the facility including, as appropriate, the following areas: entrances and exits, cargo handling and storage areas, fence lines, and parking areas? This is a requirement.

Partner Response:

Every entrances, production areas, warehouses, cargo management, parking lot, perimeter areas and office areas have suitable lighting to allow adequate surveillance and security tasks. Lighting has a maintenance program in place and frequent inspections are made to avoid any fault that might take place.

SCSS Comment :

none

Physical Security : Security Technology

Is Security Technology utilized to monitor the premises and prevent unauthorized access to sensitive areas?

Partner Response:

A closed circuit television (CCTV) system is in operation. At the current implementation stage, there are 458 cameras covering the following areas: - Utility Center - Stamping - Welding - Painting - Assembly - Perimeter - Parking lots - Main gate - Employee gates - VCP Area Indoor-Outdoor, Rail Road Area. CCTV cameras have night-vision function and outdoor cameras have 43x and 33x zooms. CCTV recordings are stored in the KMM servers; storage capacity is approximately 900 TB (2 months). Additionally, the VPC area has an extra CCTV system to register the quality control and security processes performed before shipping vehicles out of the plant. Our CCTV management procedure includes operation mode, replacement, maintenance, and registry retention time (recording time).

SCSS Comment :

none

Physical Security : Recommend cameras

Do cameras monitor the facility’s premises and sensitive areas to deter unauthorized access?

Partner Response:

The perimeter fence and others critical areas are constantly inspected during the day and night shifts by an assigned security officer. Monthly inspections are conducted by the Security Personnel, including perimeter fences , lighting system, entrances, CCTV system and in general all security systems. According to the critical areas matrix, they control to be made in each defined , including frequently inspections.

SCSS Comment :

none

Physical Security : Recommend alarms

Are alarms used to alert unauthorized access into sensitive areas?

Partner Response:

We have an audible alarm system at all security entrances in case of any security incident.

In addition, our "Genetek" access system informs us if someone tries to enter an unauthorized area.

The entire alarm system is constantly monitored by our control and monitoring center

SCSS Comment :

none

Physical Security : Written Procedures, Cameras and Alarms

If relying on security technology for physical security, are there written policies and procedures governing the use, maintenance, and protection of this technology? At a minimum, do these policies and procedures stipulate: How access to the locations where the technology is controlled/managed or where its hardware (control panels, video recording units, etc.) is kept, is limited to authorized personnel? The procedures that have been implemented to test/inspect the technology on a regular basis? That the inspections include verifications that all of the equipment is working properly, and if applicable, that the equipment is positioned correctly? That the results of the inspections and performance testing is documented? That if corrective actions are necessary, these are to be implemented as soon as possible and that the corrective actions taken are documented? That the documented results of these inspections be maintained for a sufficient time for audit purposes? These are requirements.

Partner Response:

We have a procedure for CCTv operations and access controls. This describes the functionality of the system.

We have a preventive-corrective maintenance policy that covers all of our equipments (cameras, controllers, IDfs, UPS, turnstiles, readers, vehicle barriers, metal detector archs, etc.)

SCSS Comment :

none

Physical Security : Annual Policy Review

Are security technology policies and procedures reviewed and updated annually, or more frequently, as risk or circumstances dictate? This is a requirement.

Partner Response:

All security policies and procedures are within the management of ISO 9001:2015, for which revisions are made annually.

The CCTv & access control maintenance policy is also renewed annually

SCSS Comment :

none

Physical Security : 3rd Party Monitoring, Written Procedures

If a third party central monitoring station (off-site) is utilized, does the CTPAT Member have written procedures stipulating critical systems functionality and authentication protocols such as (but not limited to) security code changes, adding or subtracting authorized personnel, password revisions(s), and systems access or denial(s)?

Partner Response:

We have our own control and monitoring center, monitored by security personnel hired by us.

SCSS Comment :

none

Physical Security : Use Licensed Resources

Are licensed/certified resources utilized when considering the design and installation of security technology?

Partner Response:

We have licenses granted by the company "GENETEK" for CCTv equipments

SCSS Comment :

none

Physical Security : Secure Equipment

Is all security technology infrastructure physically secured from unauthorized access? This is a requirement.

Partner Response:

For the physical infrastructure part: all our equipments are located at height (+ 6mts), and in locked drawers

For the network part: our network, is a separate network from KMM's internal network (underground), we have some users for daily operation and only 2 administrator users. All protected with passwords that expire every 60 days.

SCSS Comment :

none

Physical Security : Alternate Power Source

Are security technology systems configured with an alternative power source that will allow the systems to continue to operate in the event of an unexpected loss of direct power?

Partner Response:

We have a complete system of power supplies (UPS) that cover all CCTv equipments, the average duration is 1.5 hours.

SCSS Comment :

none

Physical Security : Alarm Notification

If camera systems are deployed, do cameras have an alarm/notification feature, which would signal a “failure to operate/record” condition?

Partner Response:

Among the benefits offered by "Genetek" system we have a customizable dashboard where we can see the cameras we have vs. those that are not working

SCSS Comment :

none

Physical Security : Positioning Cameras

If camera systems are deployed, are cameras positioned to cover key areas of facilities that pertain to the import/export process? This is a requirement.

Partner Response:

We have different types of cameras and cover all critical areas previously identified.
The loading and receiving areas, entrances and exits to the facilities are totally covered

SCSS Comment :

none

Physical Security : Picture Quality

Are cameras programmed to record at the highest picture quality setting reasonably available, and be set to record on a 24/7 basis?

Partner Response:

The cameras we have are recording 24/7 with an acceptable image quality to be able to follow up on an incident or investigation.

SCSS Comment :

none

Physical Security : Maintain Footage

If cameras are being used, are recordings of footage covering key import/export processes maintained for a sufficient time for a monitored shipment to allow an investigation to be completed?

Partner Response:

All our cameras have a recording time of 2 months

SCSS Comment :

none

Physical Security : Audit Footage

If camera systems are deployed, are periodic, random reviews of the camera footage conducted (by management, security, or other designated personnel) to verify that cargo security procedures are being properly followed in accordance with law? Are results of the reviews summarized in writing to include any corrective actions taken? Are the results maintained for a sufficient time for audit purposes?

Partner Response:

We have a security specialist who is responsible for randomly monitoring the security cameras, in addition to reviewing the preventive-corrective maintenance activities

SCSS Comment :

none

Access Controls : ID badges

Are there written procedures governing how identification badges and access devices are granted, changed, and removed? This is a requirement.

Partner Response:

Electronic card control has been established in the process to assign, manage, and withdraw electronic cards, indicating that the Human Resources Department is responsible for collecting new employee?s data and pictures in order to print their badges. This information is stored securely in a database. Subsequently, the security analyst is accountable for reviewing that information and sending the badge clasps to HHRR so they can be delivered to the new employees. Delivery, change, and withdrawal of electronic access cards is always documented. The security analyst prepares a log with the badges delivered, including the following information: - Employee name - Department - Employee number - IMSS number - Card tag number If required, the security analyst is responsible for providing access control reports and for configuring ID badges to grant or to deny access to the different areas. Each user is responsible for reporting the loss or damage of his/her identification badge and/or access control card. The security analyst is responsible for restoring the badge clasp, following the same procedure. Unassigned cards are stored in a secured cabinet

SCSS Comment :

none

Access Controls : ID system

Where applicable, is a personnel identification system in place for positive identification and access control purposes? This is a requirement.

Partner Response:

All access are controlled , employees enter through a door with electronic access control , visitors enter through another door , which are identified with an official document and contractors enter through the logistics doors. All access are recorded in both the CCTV system and the physical records kept in the security gates.
When entering the trucks by the logistics door, security personnel carried out a review of the vehicle and positively identified to the driver and check if really who is authorized to enter.

SCSS Comment :

none

Access Controls : Restrict Access

Is access to sensitive areas restricted based on job description or assigned duties? This is a requirement.

Partner Response:

We have a security procedure called "personnel access control". This procedure details the different types of security levels we have in the facility. All the doors to these areas are controlled by readers.
Each employee or contractor has access depending on the area where they work.

SCSS Comment :

none

Access Controls : Remove Access

Does removal of access devices take place upon the employee’s separation from the company? This is a requirement.

Partner Response:

Once an employee is terminated by the company, HR department is responsible for remove the access credential.

The database of our access control system is fed by SAP, when the employee is discharged from SAP he is automatically discharged from our access control system.

SCSS Comment :

none

Access Controls : Subject to Search

Are individuals and vehicles subject to search in accordance with local and labor laws?

Partner Response:

All persons and vehicles entering the facility must pass through the security inspection filter. These inspections include the K9 check.

SCSS Comment :

none

Access Controls : Photo ID & Visitor Log

Do visitors, vendors and service providers present photo identification upon arrival? Is a log maintained that records the details of the visit? Does the registration log must include the following: date of the visit, visitor’s name, verification of photo identification (type verified such as license or national ID card)? Frequent, well known visitors such as regular vendors may forego the photo identification, but are they still logged in and out of the facility, including time of arrival, company point of contact and time of departure? These are requirements.

Partner Response:

We have a visitor management system called "autoway", in this system the KMM user registers the visit he is waiting for, filling in the following fields: Visitor's name, reason for the visit, day and time of the visit, which areas he requires access to, etc. The visitor must leave a photo ID and fill out a confidentiality agreement before entering. The visitor cannot enter alone, the KMM user must accompany the visit at all times

SCSS Comment :

none

Access Controls : Visitor ID

In addition, are all visitors and service providers issued temporary identification?

Partner Response:

Visitors are issued a temporary ID on the day of their visit, suppliers and/or contractors are issued an ID for a certain period of time, for this to happen the supplier or contractor must submit certain documentation and permissions authorized by the KMM user

SCSS Comment :

none

Access Controls : Display Temp ID

If temporary identification is used, is it visibly displayed at all times during the visit? This is a requirement.

Partner Response:

All credentials of visitors, suppliers and contractors are visibly displayed

SCSS Comment :

none

Access Controls : Escort Visitors

Are all visitors escorted?

Partner Response:

As part of the visiting process, all KMM users must escort their visit when they enter, during their stay and when they leave the facilities

SCSS Comment :

none

Access Controls : Pick Ups by Appointments

Where operationally feasible, are deliveries and pickups allowed by appointment only?

Partner Response:

All deliveries and shipments are managed by different systems, both processes are scheduled

SCSS Comment :

none

Access Controls : Driver Pickup Details

Prior to arrival, does the carrier notify the facility of the estimated time of arrival for the scheduled pick up, the name of the driver, and truck number?

Partner Response:

No

The transporters, at the moment of arriving at the facilities give us a "delivery note" with information of the load (amount and type of material), where they go, where they come from, information of the driver, etc.

SCSS Comment :

none

Access Controls : Driver Identification

Are drivers delivering or receiving cargo positively identified before cargo is received or released? Do drivers present government-issued photo identification to the facility employee granting access to verify their identity? If presenting a government-issued photo identification is not feasible, the facility employee may accept a recognizable form of photo identification issued by the highway carrier company that employs the driver picking up the load. These are requirements.

Partner Response:

Each time a carrier arrives to drop off or take away material, they are required to present official photo identification, the security guard records the information of the driver and the unit and a security inspection is carried out

SCSS Comment :

none

Access Controls : Cargo Pickup Log

Is a cargo pickup log kept to register drivers and record the details of their conveyances when picking up cargo? When drivers arrive to pick up cargo at a facility, does a facility employee register them in the cargo pickup log? Upon departure, are drivers logged out? Is the cargo log kept secured and are drivers not allowed access to it? These are requirements.

Partner Response:

We have different registers in the security operations, a vehicle register, in which the name of the driver, the data of the unit, the time of entry and exit are registered.

Hyundai Glovis security has cargo records

SCSS Comment :

none

Access Controls : Cargo Pickup Log Details

Does the cargo pickup log have the following items recorded: driver’s name, date, time of arrival, employer, truck number, trailer number, time of departure, and the seal number affixed to the shipment at the time of departure?

Partner Response:

We have the registration of entry and exit of the drivers, this includes the time of entry and exit, driver's name, economic number of the vehicle. On the other hand, we ask for the exit manifest and the cargo, in this document we check the cargo that leaves the facilities and the VIN numbers of the vehicles.

SCSS Comment :

none

Access Controls : Packages

Are arriving packages and mail periodically screened for contraband before being admitted?

Partner Response:

We have a procedure for the reception and delivery of couriers and packages. This describes the process to follow when a package is received. All incoming packages are screened and inspected.

SCSS Comment :

none

Access Controls : Written Guard Policies

If security guards are used, are work instructions for security guards contained in written policies and procedures? This is a requirement.

Partner Response:

We have internal security procedures (e.g., personnel access control, vehicle access control, cargo vehicle inspection, preventive patrollings). The security guards carry out these procedures, it is part of their functions.

Each security company has its own internal policies, and they are focused on KMM processes

SCSS Comment :

none

Access Controls : Management Audits of Guards

Does management periodically verify compliance and appropriateness with these procedures through audits and policy reviews? This is a requirement.

Partner Response:

We have a security specialist strictly focused on daily security operations. Among its functions is the review of compliance with security procedures

SCSS Comment :

none

Personnel Security : Applicant’s Information

What are the written procedures for screening prospective employees and for performing checks on current employees? Is application information, such as employment history and references, verified prior to employment, to the extent possible and allowed under the law? This is a requirement.

Partner Response:

The application of the candidate to be hired by KMM is subject to verification of previous employment, work-related lawsuits, and criminal records. Hiring companies (Prodensa and Reyna Asesores) send an electronic report with all the information. Additionally, a drug screening test is conducted on every new hire. New employees who are rated as high-risk in the Critical Position Matrix are requested to provide a clean criminal history and a socioeconomic study.

SCSS Comment :

none

Personnel Security : Background Checks

In accordance with applicable legal limitations, and the availability of criminal record databases, are employee background screenings conducted? Are results of background checks factored in, as permitted by local statutes, in making hiring decisions? Does employee background screening include verification of the employee’s identity and criminal history that encompass city, state, provincial, and country databases? Background checks are not limited to verification of identity and criminal records. In areas of greater risk, more in depth investigations may be warranted.

Partner Response:

To define controls for new employees, as well as for the rest of personnel, a Critical Position Matrix was established, which includes the evaluation of nine (9) variables to determine the risk level of each position. Additionally, it has been determined that critical positions must provide a clean criminal record once they are hired, with an update every two (2) years thereafter.

SCSS Comment :

none

Personnel Security : Contractors

Based on the sensitivity of the position, do employee vetting requirements extend to temporary workforce and contractors?

Partner Response:

KMM has internal personnel for its operations, with the exception of Hyundai Glovis, KMM's brother company that has operations in warehouse areas.
For their admission it is necessary to present certain documentation as well as a drug test. Because of the type of operations they handle with us, they are classified as critical supplier and are audited on a recurring basis.

SCSS Comment :

none

Personnel Security : Reinvestigations

Once employed, are periodic reinvestigations performed based on cause, and/or the sensitivity of the employee’s position?

Partner Response:

Research is conducted at :
-Newly-hired employees
-Employees who, because of the sensitivity of their position, require annual investigations

SCSS Comment :

none

Personnel Security : Code of Conduct

Is there an Employee Code of Conduct that includes expectations and defines acceptable behaviors? Are employees and contractors required to acknowledge that they have read and understand the Code of Conduct? This is a requirement.

Partner Response:

In KMM we have an internal code of conduct, the main points are:

-Discrimination
-Violence in the workplace
-Harassment
-Drugs, alcohol and weapons
-Employee health and safety
-Information Security
-Security

among other things

SCSS Comment :

none

Education and Training : Overall Training Program

One of the key aspects of a security program is training. Is a security training and awareness program in place and maintained to recognize and foster awareness of the security vulnerabilities to facilities, conveyances, and cargo at each point in the supply chain, which could be exploited by terrorists or contraband smugglers? This is a requirement.

Partner Response:

On a weekly basis, a security course is carried out, in which physical security, information security and official security programs (C-TPAT / OEA) are discussed. The training department is in charge of scheduling the sessions and the security department of giving the course

SCSS Comment :

none

Education and Training : General Security Training

Employees who understand why security measures are in place are more likely to adhere to them. Is security training provided to employees, as required based on their functions and position, on a regular basis? Do newly hired employees receive this training as part of their orientation/job skills training? Is the training program comprehensive and does it cover all of CTPAT's security requirements? This is a requirement.

Partner Response:

The training department together with the security department give courses to new KMM employees, this course has a duration of 2 hours and specific security topics such as physical security, information security, security in the chain are covered supply, etc. At the end of the course, an exam consisting of 12 questions related to the course is applied

SCSS Comment :

none

Education and Training : Sensitive Positions

Do personnel in sensitive positions receive additional specialized training geared toward the responsibilities that the position holds? This is a requirement.

Partner Response:

All KMM staff receive security training, no exceptions. The content is the same for all positions.

SCSS Comment :

none

Education and Training : Refresher Training

Is refresher training conducted periodically, as needed after an incident or security breach, or when there are changes to company procedures? This is a requirement.

Partner Response:

The update course is carried out once a year, in case of any security incident the committee meets to see future actions.

We have an internal communication program in relation to security in the supply chain, security tips and processes relevant to the C-TPAT and ISO 27001 certification are communicated monthly

SCSS Comment :

none

Education and Training : Training Records

Is training evidence retained, such as training logs, sign in sheets (roster), or electronic training records? This is a requirement.

Partner Response:

We have lists of training assistance to contractors, in the case of employees we only have the evidence of the exams and electronic records.

SCSS Comment :

none

Education and Training : Record Details

Do training records include the date of the training, names of attendees, and the topics of the training?

Partner Response:

At KMM we only handle an attendance list format. When training is given to contractors, the name of the training, the name of the instructor, names of the assistants, signatures and the date of the training are recorded.

SCSS Comment :

none

Education and Training : Testing Training

Are measures in place to verify that the training provided met all training objectives?

Partner Response:

At the end of the training, KMM employees are given a knowledge test

SCSS Comment :

none

Education and Training : Inspections

Are drivers and other personnel that conduct security and agricultural inspections of empty conveyances and IIT trained to inspect their conveyances/IIT for both security and agricultural purposes? Does inspection training include the following topics: signs of hidden compartments, concealed contraband in naturally occurring compartments, and signs of pest contamination? These are requirements.

Partner Response:

We only have documented training of security personnel, in relation to inspection methods C-TPAT (Hidden compartments and signs of contamination, including pests and / or weeds)

SCSS Comment :

none

Education and Training : Security Incidents

Are employees trained on how to report security incidents and suspicious activities? This is a requirement.

Partner Response:

Within the security training provided to employees, the issue of reporting suspicious activities or persons is reviewed.

In addition to this, internal communications are constantly sent to all employees reminding them that they can make anonymous complaints to report any type of incident or suspicious activity.

SCSS Comment :

none

Education and Training : Cybersecurity

As applicable based on their functions and/or positions, are employees trained on the company's cybersecurity policies and procedures? Does this include the need for employees to protect passwords/passphrases and computer access? This is a requirement.

Partner Response:

All employees receive annual security training, this includes; physical security, information security, official security programs.

In addition, security policies and procedures are constantly communicated internally, through the communication department.

SCSS Comment :

none

Education and Training : Security Technology

Have employees operating and managing security technology systems received training in their operation and maintenance? Prior experience with similar systems is acceptable. Self-training via operational manuals and other methods is acceptable. This is a requirement.

Partner Response:

The employees who manage the IT department have previous experience in managing systems, applications, databases, SAP, etc.

SCSS Comment :

none

Cybersecurity : Written Cybersecurity Policies

Are comprehensive written cybersecurity policies and/or procedures in place to protect information technology (IT) systems? Does the written IT security policy, at a minimum, cover all of the individual cybersecurity criteria? These are requirements.

Partner Response:

We have an information security management system, supported by procedures and policies such as; The information security policy, asset management, access management, risk management framework, documentary control, acceptable use of assets, security in operations, incident management, etc.

SCSS Comment :

none

Cybersecurity : Annual Review IT Policies

Are cybersecurity policies and procedures reviewed annually, or more frequently, as risk or circumstances dictate? Following the review, are policies and procedures updated if necessary? These are requirements.

Partner Response:

An annual review of documents that are within the management system is carried out, if changes are applied, they are made and the history of the document is modified, as described in the procedure "document control of the ISMS"

SCSS Comment :

none

Cybersecurity : IT Disaster Plan

If a data breach occurs or an event results in the loss of data and/or equipment, do procedures include the recovery (or replacement) of IT systems and/or data? This is a requirement.

Partner Response:

Within the information security management system we have a procedure called "Business continuity and disaster recovery", in addition to other procedures of external origin that are part of KMM's internal process such as the information backup process.

SCSS Comment :

none

Cybersecurity : Information Sharing Policies

Do cybersecurity policies address how information is shared on cybersecurity threats with the government and other business partners?

Partner Response:

Within the information security management system we have a procedure called "asset management" in this procedure, topics such as: types of assets, asset owners, inventories, acceptable use, classification, information management, etc. are documented.

SCSS Comment :

none

Cybersecurity : Social Engineering

Are policies and procedures in place to prevent attacks via social engineering? This is a requirement.

Partner Response:

We have a procedure within the information security management system called "Training and awareness plan", within this procedure issues related to social engineering are reviewed.

As part of our internal training plan, we gave an information security presentation in which we addressed the topic of social engineering.

SCSS Comment :

none

Cybersecurity : Counterfeit Software

Do cybersecurity policies and procedures include measures to prevent the use of counterfeit or improperly licensed technological products?

Partner Response:

KMM uses only authentic products with license officially.
It means KMM doesn't allow to use any improperly software as well as we remove the counterfeit product immediately if it is found.

SCSS Comment :

none

Cybersecurity : Identifying IT Abuse

Is a system in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors? This is a requirement.

Partner Response:

KMM has security software products to prevent and identify unauthorized access to IT system/data such as Symantec, Trendmicro and DRM.
And IDS, IPS and firewall in KMM check and control the unauthorized access from outside to KMM.
Moreover, global security center in Korea also provides a monitoring and managing service to protect secure environment for KMM.

And all IT security policies are saved in the global security management system and KMM storage both.

SCSS Comment :

none

Cybersecurity : IT violations, Disciplinary Actions

Are all violators subject to appropriate disciplinary actions? This is a requirement.

Partner Response:

Disciplinary action for IT policy/procedure violations follows the HR policy based on HQ HR

KMM has an internal code of conduct, every employee signs up when entering

SCSS Comment :

none

Cybersecurity : Security Software

To defend Information Technology (IT) systems against common cybersecurity threats, has sufficient software/hardware been installed for the protection from malware (viruses, spyware, worms, Trojans, etc.) and has an internal/external intrusion detection system been installed (firewalls)? These are requirements.

Partner Response:

PC : Symantec endpoint
Server : Trendmicro
Malware : FireEye, Netshield (It is being managed by global security center in Korea)
Network : Firewall, IDS, IPS

SCSS Comment :

none

Cybersecurity : Updating Security Software

Is security software current and does it receive regular security updates? This is a requirement.

Partner Response:

KMM updates security software according to HeadQuarter guidance. HeadQuarter security team guide the version regularly.

SCSS Comment :

none

Cybersecurity : Test IT Systems

When utilizing network systems, is the security of the IT infrastructure regularly tested? If vulnerabilities are found, are corrective actions implemented as soon as feasible? These are requirements.

Partner Response:

HeadQuarter security team conduct a test for checking security environment regularly.

SCSS Comment :

none

Cybersecurity : Data Backups

Is data backed up once a week or as appropriate? Is all sensitive and confidential data stored in an encrypted format?

Partner Response:

Yes, important data is backed up according to the backup schedule in netbackup solution.

SCSS Comment :

none

Cybersecurity : Regular IT Inventories

Are all media, hardware, or other IT equipment that contains sensitive information regarding the import/export process accounted for through regular inventories? This is a requirement.

Partner Response:

All inventory for media, hardware, IT equipment are being managed by Hyundai Autoever Mexico on behalf of KMM.

Also KMM manages HAEM inventory management regularly. (HAEM send the inventory list every month.)

SCSS Comment :

none

Cybersecurity : Disposal of IT Equipment

When disposed, are they properly sanitized and/or destroyed in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization or other appropriate industry guidelines? This is a requirement.

Partner Response:

When KMM dispose old IT equipment, KMM does format the kind of disk or storage part after detached it from the equipment.

SCSS Comment :

none

Cybersecurity : Personal Devices

If employees are allowed to use personal devices to conduct company work, do all such devices adhere to the company’s cybersecurity policies and procedures to include regular security updates and a method to securely access the company’s network? This is a requirement.

Partner Response:

No, we don’t allow to use personal device for company business.

SCSS Comment :

none

Cybersecurity : Individual Accounts

Do individuals with access to IT systems use individually assigned accounts? This is a requirement.

Partner Response:

Individual account is generated as employee number in the ERP by HR Department.
And the account is applied to AD system for IT.
Also KMM uses Global ID Management system of HeadQuarter.

SCSS Comment :

none

Cybersecurity : Passwords

Is access to IT systems protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication and is user access to IT systems safeguarded? These are requirements.

Partner Response:

All accesses to computer equipment, internal applications, internal systems, printers have a username and password. In addition to the information security management system, we have a password policy

SCSS Comment :

none

Cybersecurity : Restrict IT Access

Is user access restricted based on job description or assigned duties? This is a requirement.

Partner Response:

Only allowed users by firewall and system can access to IT system.
Also KMM use ‘Server Access Control’ system to access to the IT system.

SCSS Comment :

none

Cybersecurity : Review IT Access

Is authorized access reviewed on a regular basis to ensure access to sensitive systems is based on job requirements? This is a requirement.

Partner Response:

The authorization for user is proceeded through KMM electronic approval system. (Cooperation Letter)

SCSS Comment :

none

Cybersecurity : Removing IT Access

Is computer and network access removed upon employee separation? This is a requirement.

Partner Response:

HR department send a group email about resigned employee information to IT and security in order to remove the access permission and proceed resignation process.
Once IT receive the mail, the permission is removed.

SCSS Comment :

none

Cybersecurity : Remote Access

When users are allowed to remotely connect to a network, are secure technologies employed, such as virtual private networks (VPNs), to allow employees to access the company’s intranet securely when located outside of the office? Are procedures in place that are designed to prevent remote access from unauthorized users? These are requirements.

Partner Response:

Yes, employees can access to their own PC in the office through VPN connection.

- VPN Authentication

1) CISCO VPN Authentication
2) RDP

SCSS Comment :

none