SECURITY REQUIREMENTS
FOR
JAMAICA CUSTOMS AGENCY'S (JCA)
AUTHORIZED ECONOMIC OPERATORS (AEO)

ENGAGED IN IMPORTATION, EXPORTATION & MANUFACTURING

1. MANAGEMENT AND ADMINISTRATION O F T H E SECURITY CONTROL SYSTEM

THE AEO MUST:

1.1 Document, implement, publish and distribute security policies which aid in the prevention of illegal and criminal activities. The policies must have clear and measurable objectives to ensure compliance. Illegal and criminal activities include, but are not limited to, drug trafficking, terrorism, smuggling and theft.

1.2 Charge Senior Management with the responsibility of ensuring compliance with security policies (referenced in 1.1).

1.2.1 Have a designated Manager who is documented as being responsible for all security requirements of the AEO Programme.

1.3 Document and implement a Risk Management system (as detailed in 2 – 9) incorporating business partner security, container and conveyance security, physical security, physical access control, personnel security,

information technology security, training, and security of raw and packaging materials (where applicable).

1.4 Identify and document the processes (pictorial representations may be used) that the organization uses in the conduct of its business. These processes should identify inputs, outputs, and indicators measuring compliance and responsible use of the processes.

1.5 Have the designated AEO Officer for the company or if the internal audit team conduct an audit on the compliance of AEO requirement, this person should be trained in the AEO Program and its requriments.

1.5.1 Conduct a minimum of one (1) annual internal audit to assess compliance with minimum AEO security requirements and to identify and implement corrective actions and improvements where required. These audits shall be submitted to the Commissioner of Customs. This audit report must be submitted no later than three (3) months after the anniversary date of receiving the AEO status.

1.6 Have an organized and updated system that covers all administrative and financial activities of the organization: general accounting, banking, accounts receivable, accounts payable, billing, inventory, payroll, production, purchasing, sales, etc.

1.7 Have documented job descriptions for personnel employed in areas of importation and exportation.

2. BUSINESS PARTNER SECURITY

Business partners are considered to be persons/entities contracted or subcontracted to perform a service, or provide goods, whose action can affect the security of the supply chain. These include: air and sea carriers, importers, exporters, Customs Brokers,

freight consolidators/forwarders, Shipping Agents, port facilities, airports, suppliers and haulage contractors.

THE AEO MUST:

2.1 Have written and verifiable processes for the selection of business partners (as defined in 2).

2.2 Maintain and update (at least) the following information for their business partners:

1. (a) Individual – name or trading name

(b) Corporate Entity - the legal and trading name (if applicable) of the organization

2. Unique identification number, such as a tax registration number
3. Business Address
4. Business background (inclusive of their economic activity)

2.3 Document (certificate number, if applicable) which of their business partners have any of the following security certification: C-TPAT, BASC, AEO, ISO 28000, PIP, NEEC, MCME.

2.4 Check that their business partners who are certified by a security program other than those listed in 2.3, or who have no form of security certification, meet the minimum security requirements of the AEO Programme. This can be verified by administering the Business Partner

Security Questionnaire (available on the JCA website). This questionnaire is to be re-administered to business partners in this category whenever the AEO status is being renewed

2.4.1 If the AEO identifies weaknesses in their business partners in this regard, they should ask that the weaknesses be corrected.

Please note, if the business partner has security certification as listed in 2.3 or meets the minimum security requirements as outlined in 2.4, then 3.1 & 3.2 do not apply

3. CONTAINER AND CONVEYANCE SECURITY

Container and conveyance integrity must be maintained to protect against the introduction of unauthorized material and/or persons. At the point of stuffing, procedures must be in place to properly seal and maintain the integrity of the shipping containers. A high security seal must be affixed to all loaded containers bound for Jamaica and outbound from Jamaica.

3.1 and 3.2 are applicable to exporters who also import.

THE AEO MUST:

Container and Conveyance Inspection

3.1 Request a Container Inspection Report, duly signed by the inspecting officer from their overseas supplier/consolidator for each container prior to loading. This report must incorporate the seven-point inspection process outlined in 3.2. including the names of the personnel off-loading the container

3.2 Have documented and implemented procedures in order to verify the physical integrity of the container. This should include the reliability of the locking mechanisms of the doors after unloading and prior to returning the empty container to the port. A seven- point inspection process is required for all containers:

1. Front wall
2. Left side
3. Right side
4. Floor
5. Ceiling/Roof
6. Inside/outside doors
7. Outside/Undercarriage

Reefer:

1. Inspection of the evaporator area.
2. Area of the condenser.
3. Control box

4. Area Compressor

3.2.1 When exporting – Inspect the tractor head and chassis and complete the Inspection Check List. The inspection checklist must be duly signed by the inspecting officer. It must contain the following:

1. The fifth wheel area - inspect the natural compartment / skid plate
2. Exterior - front / side
3. Rear - bumpers / doors
4. Front wall
5. Left side
6. Right side
7. Floor
8. Ceiling Indoor / Outdoor
9. Inside (including the Sleeper)/outside
10. Exterior / Bottom section

Container Seals

3.3 Submit a written request to their suppliers/consolidator for high security seals to be affixed to all their imported and exported containers. All seals must meet or exceed the current PAS ISO 17712 standards for high security seals.

3.4 Document, implement and maintain procedures to recognize and report to the shipping line or agent and the Jamaica Customs Agency (JCA), whenever the seals, containers and / or other cargo units have been violated. Similarly, the importer must report to the

JCA prior to the landing or opening of the container if the supplier(s)/consolidator neglect to use seals meeting the required standard.

3.4.1 Document, implement and maintain procedures governing the use, distribution and storage of seals. Only designated employees should handle and distribute seals.

3.5. Notify the JCA immediately through the AEO Account Officer when the goods are found to be contaminated or damaged

Container Storage

3.6 Store containers and other cargo units (loaded and empty) in a secure area to prevent access and/or tampering.

3.7 Have procedures for reporting and neutralizing unauthorized entry into containers, trailers, and areas for the storage of containers and trailers.

3.8 Perform and document periodic inspections of storage areas for containers and other cargo units (full and empty) to detect suspicious or irregular activities (refer to 8.1).

4. PHYSICAL SECURITY

THE AEO MUST:

Fencing

4.1 Have perimeter fencing that encloses the cargo handling areas and storage facilities. The fencing must be appropriate for protecting the cargo.

4.2 Inspect perimeter fencing at least once per week to verify their integrity and address any damages. There must be documentary record of the inspections, duly signed by the person who conducted the inspection.

Finished goods imported for export under bonded facility

4.3 Have designated areas within the cargo handling area to separate and store goods intended for local consumption and goods intended for export.

Entrances and Exits

4.4 Monitor entrances and exits for vehicles and personnel. A log must be used to capture information such as the driver's/visitor's name; license plate number; and the number from valid photo identification. This log must be kept for a minimum of three (3) years.

Building structure

4.5 Secure their building structures with the necessary physical features that will serve to reduce the possibility of illegal entry.

4.6 Perform annual inspections and conduct repairs as circumstances dictate in order to maintain the integrity of their building structures.

Control of locks and keys

4.7 Secure all windows, doors, interior and exterior gates with locks. Management or security personnel must control the issuance of all locks and keys using appropriate logs. This log must be kept for a minimum of three (3) years.

Security System

4.8 Either have their own security service staffed by persons registered with the Private Security Regulation Authority (PSRA) or contract a security company registered with the PSRA. The security personnel should be prepared to offer timely 24-hour response service in the event of any unforeseen threat to the company's operations.

4.9 Have a map showing the location of sensitive areas (relating to the importation, manufacturing and exportation of cargo, as applicable) of the facility.

4.10 Use alarm systems and video surveillance cameras to monitor premises (especially the sensitive areas as defined in 4.9) and aid in deterring unauthorized access to the areas of cargo handling and storage. The recordings must be stored for a minimum of 30 days (1 month). Storage can be in the form of DVDs etc.

4.10.1 For the buildings at the location, cameras must be installed to monitor all exterior sections of the building including offloading and loading areas, entrances, exits and interior sensitive zones. For warehouses, cameras must be installed to ensure all access areas are monitored. Cameras must also be positioned to capture all activities inside the container.

4.11 Document, implement and maintain contingency and emergency procedures to be used in the event of natural disasters, pandemics, civil unrest, container contamination (in any form), corruption and terrorist acts to ensure continuity and security in the international supply chain

4.12 Conduct drills including fire drills at least once per year to test contingency and emergency procedures outlined in 4.11.

THE AEO MUST:

Lighting

4.13 Have adequate lighting inside and outside the facility at all times. Special attention must be paid to the following areas: entrances and exits, areas of cargo handling and storage, perimeter fencing and parking areas.

4.14 Have an emergency electrical power supply system (such as generators or inverters) to restore power to sensitive areas (refer to 4.9) in the event of a possible loss of electricity. Alarm systems and surveillance video cameras must be connected to the emergency power supply system.

Parking and Lockers

4.15 Prohibit the parking of vehicles of employees and visitors within the cargo handling areas and adjacent areas while such operations are taking place.

4.16 Manage areas designated for employee s' lockers, ensuring that these areas are away from the cargo handling areas.

5. PHYSICAL ACCESS CONTROLS

THE AEO MUST:

5.1 Have an identification system for employees if they employ in excess of nineteen (19) persons. This system must include an identification card with a picture which must be presented upon arrival.

5.2 Document procedures for delivery, removal and changing of access devices to employees (e.g. keys, key cards, etc.).

5.3 Require visitors going to the sensitive areas (refer to 4.9) of the organization to submit valid photo identification upon arrival, and record essential information from the ID.

5.4 Issue visitors going to the sensitive areas (refer to 4.9) of the organization with the organization's temporary visitor pass, which must be visibly displayed for the duration of the visit (This requirement does not apply to organizations employing less than 20 persons).

5.4.1 Control the issuance and return of visitors' passes. This includes having procedures in place to address lost or unreturned passes.

5.5 Have a record of all visitors going to the sensitive areas (refer to 4.9) of the organization. These records must include their arrival and departure times, as well as the name of the employee they are visiting.

THE AEO MUST:

5.6 Escort visitors and unauthorized staff going to the sensitive areas (refer to 4.9) of the organization during their visit.

5.7 Have documented and implemented procedures on how to identify, challenge and address unauthorized or unidentified people within the facility, including unauthorized staff members.

6. PERSONNEL SECURITY

THE AEO MUST:

6.1 Document, implement and maintain procedures for the selection of employees (a recruitment policy).

6.2 Verify the information on the employment application, such as criminal record, personal and employment references, etc., in keeping with appropriate national legislation for candidates with employment opportunity.

6.3 Have updated employment history for all personnel, including photograph, address, phone number(s), next of kin information, and other relevant personal data.

6.4 Identify and update the critical positions that could compromise the security of the supply chain. Critical positions encompass all employees working in the sensitive areas (refer to 4.9) of the organization, along with the management team.

6.5 Have a manual of conduct and code of ethics that stipulates the administrative sanctions for breaches of the security measures and other behaviours that affect safety. This manual must be communicated and made available to all staff.

6.6 Have a policy in place to control the supply (delivery and return) of uniforms and company identification, and make reasonable effort (documented) to ensure that these supplies are returned upon the employee's separation from the company.

6.7 Have a policy governing the separation whether (voluntary, involuntary or abandonment) of employees from the organization.

6.8 Have procedures in place to refer staff to appropriate institutions in cases of substance abuse.

7. INFORMATION TECHNOLOGY SECURITY

THE AEO MUST:

Control and data protection

7.1 Assign individual accounts to employees. These accounts must require a change of password every three (3) months (minimum).

7.2 Have Information Technology policies documented and these must be communicated to employees through training.

7.3 Have a back-up of trade-sensitive information for at least the last three (3) years of operation. A copy must be stored securely offsite.

7.4 Have a system in place to identify abuse of computer systems and detect improper access, tampering or the altering of business data.

7.5 Apply disciplinary measures to all violators of the system.

7.6 Comply with the laws governing Intellectual Property Rights (IPR) and Copyrights.

8. SECURITY TRAINING AND AWARENESS OF THREATS

THE AEO MUST:

8.1 Train employees in the procedures established by the company to address and report suspicious activities to the management team and the Jamaica Customs Agency.

Documented training sessions

- Company established procedures for addressing & reporting suspicious activities to the management team and the JCA:
  i. Maintaining Cargo Integrity
  ii. Access Controls
  iii. Recognizing internal conspiracies

8.2 Provide specific training to assist employees in maintaining cargo integrity, access controls, and recognizing internal conspiracies.

8.3 Implement a threat awareness program to equip employees with the knowledge of how to prevent, recognize and react to any threat of smuggling, hostage taking, bomb threat, criminal activities and terrorism.

9. CONTROL OF RAW MATERIALS AND PACKAGING MATERIALS

(Applicable to manufacturers only)

THE AEO MUST:

9.1 Use the necessary documentation (such as requisitions, returns, inputs, outputs, and authorized signatures) for the control of raw materials and packaging materials. These documents must be maintained for at least three (3) years.

9.2 Control access to areas where raw materials and packaging materials are stored.

10. PROCEDURAL SECURITY

10.1 Implement procedures to verify the accuracy of Customs Declarations.

10.2 Procedures in place on how documented procedures are updated and who is responsible for updating these procedures.