

TAPA

FSR 2007

FREIGHT SUPPLIERS MINIMUM SECURITY REQUIREMENTS

Contents

Section 1 - Requirements

1. Scope

- (a) Forward
- (b) Freight Security Requirements
- (c) Other Documents Referenced to FSR
- (d) FSR Applicable Areas
- (e) Resources to Implement the FSR
- (f) Definitions

2. Contract Acceptance

- (a) Suppliers Responsibilities at Acceptance of the Contract

3. Supplier Security Organization

- (a) Supplier Security Representative
- (b) Supplier Loss Investigator

4. Risk Assessment and Audits

- (a) Buyers and Suppliers Responsibilities for Risk Assessments and Audits
- (b) Monitoring Supplier Corrective Action Requirements
- (c) Storage/Warehousing Building Classification Assessment
- (d) Supplier/Buyer Facility Security Audit Schedule

5. Security/Loss Investigations

- (a) Supplier Investigation Responsibilities

6. Waivers

- (a) Waivers
- (b) Waiver Process

7. Supplier Facility and Truck Security

- (a) Procedures
- (b) Supplier Facility Security Requirements (Summary)
- (c) Handling Operations
- (d) High Value Shipments by Truck (Summary)

Section 2 – Specifications

- I. Supplier Facility/Truck Freight Security Requirements

Section 3 – Forms

- FORM 3.1 – REQUEST FOR WAIVER

Section 1 - Requirements

1. Scope

(a) Forward

Technology Asset Protection Association (TAPA) is an association of security professionals and related business partners from high technology and high value companies who have organized for the purpose of addressing the emerging security threats that are common to the high value industry supply chain. A fundamental TAPA objective is to affect positive change in the security practices of the freight transportation and insurance communities as a whole. Major freight service providers are moving toward TAPA-recognized security standards for the care and handling of freight, and are recognizing the inherent value of doing so.

(b) Freight Security Requirements

Freight Security Requirements (FSR) have been established to ensure the safe and secure in-transit storage and warehousing of any TAPA members (Buyers) assets throughout the world. The FSR specifies the minimum acceptable standards for security throughout the supply chain and the methods to be used in maintaining those standards. The FSR outlines the process and specification for Suppliers to attain TAPA certification for their facilities and transit operations. It is the intention of TAPA members to select Suppliers that meet or exceed TAPA certification requirements. The successful implementation of the FSR is dependent upon Suppliers, TAPA Certified Auditors and Buyer working in concert. However, the safe and secure in-transit storage and warehousing of the Buyers assets is the complete responsibility of the Supplier, its agents and sub-contractors, throughout the collection, transit and delivery to the recipient, as specified in a Release. The FSR will be referenced in any contract between the Supplier and Buyer, and into the Supplier's own security program. Unless prior arrangements or agreements have been negotiated and documented between the Supplier and Buyer, failure to implement any part of the FSR shall be construed as a material breach of contract.

(c) Other Documents Referenced to FSR

| Title | Description | Revision date |
|--|---|---------------|
| TAPA Freight Assessment Users Guide | To provide detailed definition and assessment criteria for Buyer & TAPA certified independent assessors. (Not available to Supplier) | Jan 1, 2007 |
| TAPA Pre-Certification Review Planning | Details the process to plan and conduct the pre-certification meeting. This meeting will assist in determining if Supplier facilities & transportation methods meet the minimum-security requirements. For use by Buyer & TAPA certified independent assessors. (Not available to Supplier) | Jan 1, 2007 |

(d) FSR Applicable Areas

The FSR shall apply to all geographical areas, and all such services provided. In geographical areas where English is not the first language, where necessary and applicable it is the joint responsibility of the Buyer and Supplier to ensure that the translation accurately reflects the intentions of the Buyer and to ensure that every relevant employee has been trained to implement the FSR.

(e) Resources to Implement the FSR

The resources to meet the requirements of the FSR shall be the responsibility of the Supplier and at Supplier's own expense, unless as negotiated by or otherwise agreed to by Buyer and Supplier.

(f) Definitions

| TERM | DEFINITION |
|-------------|---|
| Buyer | TAPA Member or authorized agent, example being the TAPA certified audit body |
| CCTV | Closed Circuit Television |
| DVR | Digital Video Recorder |
| FSR | Freight Security Requirements |
| Local crime | Criminal incidents occurring within a 5 mile radius of Supplier's facilities. |
| RSP | Retail Sales Price |

| TERM | DEFINITION |
|---------|---|
| SCAR | Supplier Corrective Action Requirement |
| TAPA CA | Technology Asset Protection Association Certified Auditor |
| VCR | Video Cassette Recorder |

2. Contract Acceptance

(a) Suppliers Responsibilities at Acceptance of the Contract

At acceptance of the contract, the Supplier shall submit to the regional representatives of the Buyer's Logistics organization and the Buyer's Security Management, a copy of the Supplier's security policy and procedures or plan for ensuring safe and secure transportation, in-transit storage and warehousing of Buyer's assets. Copies of Supplier's security procedures that are relevant to the security of Buyer's assets shall be submitted to the Buyer for review. Supplier's security procedures must not conflict with the agreed to FSR. Any and all documentation shall be handled as confidential information. In cases where the Supplier's security procedures do not meet the FSR, the Supplier shall take the following actions:

- I. The Supplier shall present a detailed written action plan, which outlines the non-compliant FSR area and the corrective action to be taken, with implementation dates not to exceed 60 days from date of acceptance of contract.
- II. Supplier will attain TAPA Certification within 60 days for all facilities that will handle Buyers assets.
- III. For areas that are not FSR compliant, a negotiated contingency plan between Supplier & Buyer shall be agreed and in place at commencement of contract. The contingency plan is designed for use where Supplier needs time to upgrade security on new routes and shall not exceed 60 days in duration.
- IV. Any exception to the 60 day duration referenced herein shall have prior written approval from the Buyer requiring FSR certification.
- V. Supplier will note and respond to Buyers concerns regarding security concerns not covered by the FSR.
- VI. The Supplier will only negotiate with the approved TAPA Certification body for waivers for non-applicable TAPA FSR security measures or where alternative actions are taken to control security risks. The regional TAPA governing body will approve/decline all waivers submitted by the supplier through the independent audit firm.
- VII. Suppliers who submit to FSR certification independent of a Buyer's requirement are not exempt from any portion of the FSR.

3. *Supplier Security Organization*

(a) Supplier Security Representative

By the effective date of the contract, the Supplier will designate a representative to liaise with the Buyer's representatives. The Supplier's Security Representative shall:

- I. Have the Supplier's designated security authority responsible for managing the compliance with the FSR.
- II. Have an adequate level of security competence and background.
- III. Assign at least one individual, security responsibilities for each of the geographical areas in which the contract is effective

(b) Supplier Loss Investigator

By the effective date of the contract, the Supplier will designate one or more Loss Investigators for leading and coordinating investigation and resolution of losses of Buyer's assets while under the responsibility of the Supplier. The Supplier shall ensure adequate and timely resources are available to investigate losses of Buyers assets in the location the loss is suspected to have occurred. Loss Investigators may be the same person as the Suppliers Security Representative, as long as both responsibilities are covered in full.

4) *Risk Assessment and Audits*

(a) Buyers and Suppliers Responsibilities for Risk Assessments and Audits

- I. At acceptance of a contract between the Buyer and the Supplier, the Supplier agrees to Buyer's right to conduct risk assessments or audits of all transit, storage and warehousing locations that will be used for Buyer's assets. Buyer can nominate an agent to perform audits on behalf of the Buyer. Normally the Buyer or its agent shall notify the Supplier at least five working days in advance of any audit, detailing its nature.
- II. Supplier shall ensure the TAPA certified audit body is engaged to ensure FSR audits and certification process is completed. Costs for TAPA certification shall be the responsibility of the Supplier.
- III. The requirement for TAPA certification is also extended to Supplier's sub-contractor's facilities and in-transit locations, where used to transit Buyer's assets.
- IV. The Buyer reserves the right to conduct unscheduled audits. The Buyer shall give a minimum of 24 hours notice to the Supplier
- V. TAPA certified auditors shall inform the Supplier of assessment/audit results within ten working days from the completion of the audit. A summary of the

findings/results should be given informally to the Supplier on the day of the audit/assessment at the closing conference.

- VI. Supplier shall have deemed to pass the audit and certified if a TAPA FSR audit score of 60% or more is achieved and all mandatory items are scored at least 1. Supplier shall still be responsible for completing SCAR items in the agreed time scale, even when certification is achieved. Clearance of the non-mandatory SCAR is at the option of the Supplier but must be disclosed to Buyer.
- VII. When the TAPA certified auditor submits a SCAR to the Supplier associated with the audit findings, the Supplier shall respond to the auditor within ten working days, documenting the action to be taken, the date the action will be completed. SCAR completion dates may be negotiated between the auditor and the Supplier. However, unless the TAPA certification body approves a waiver from process, corrective action implementation shall not exceed sixty days from notification to the Supplier
- VIII. The Supplier is required to complete self-audits of their facilities and their subcontractor's facilities as detailed in section IV paragraph (d).

(b) Monitoring Supplier Corrective Action Requirements

The Supplier shall submit to the TAPA auditor progress updates on all outstanding SCAR's at monthly intervals. Any SCAR's not completed on or before the due date are to be escalated by the Supplier's Security Representative to the Supplier's Management and reasons for non-compliance are to be documented and communicated to the TAPA auditor. Supplier failure to address SCAR's may result in the TAPA certification being withheld. The Supplier has the right to appeal to TAPA directly if certification is withheld. TAPA will agree to a process for adjudication between the Supplier and the TAPA auditor and has the right to impose a resolution on both parties.

(c) Storage/Warehousing Building Classification Assessment

The Building Classification Assessment is designed to categorize the facility into one of three categories, "A" being the highest security requirement and "C" the lowest. For facilities not previously classified, the Supplier must complete a classification assessment before the effective date of the contract and give results to the Buyer. Separate TAPA audit forms for A, B, & C facilities exist. The Supplier, in cooperation with the TAPA auditor, shall complete the final classification assessment within 30 days of acceptance of contract. The TAPA Certification body shall periodically complete their own classification assessments and ultimately make the decision on the final classification to be assigned to each of Supplier facilities handling or storing of Buyer's assets. The Supplier or Buyer can request the facility to be re-assessed if either party considers the assessment category to have changed.

- I. The Building Classification Assessment methodology is set forth below.
 - Pre-Contract & where TAPA Certification has not been previously granted.
 - Using TAPA audit forms, Supplier classifies facilities that will be used in the transport of Buyer's assets by being rated at least 1 in each of the mandatory audit areas and obtain a score 60% or greater on the audit score.

- Final classification is attained (within 30 days), when the Supplier facility complies with or has agreements in place with the TAPA auditor, that will meet all the requirements of a category and is assessed by an independent TAPA auditor.

(d) Supplier/Buyer Facility Security Audit Schedule

For the duration of the contract the Supplier will conduct security audits of their facility or their subcontractor’s facility in line with the audit schedule published below. The format of the audit is to be agreed with the Buyer. It is suggested the Supplier use the same audit format as the Buyer will use in Section 3. Results of Supplier self-audits shall be forwarded to the certifying body within 2 weeks of the self-assessment. A self-assessment is to be conducted annually within the anniversary month of the independent audit.

Supplier will allow Buyer to conduct audits when pre-arranged. Supplier will, at a minimum, audit the Supplier’s facilities in line with the audit requirements published below. The Buyer or the TAPA Certified Auditor reserves the right to increase or decrease the frequency of the audits by giving prior notification to the Supplier. The format of the TAPA audits will be to use the standard audit format contained in Section 3.

| CLASSIFICATION | SUPPLIERS/SUBCONTRACTORS SECURITY AUDIT REQUIREMENTS |
|----------------|--|
| “A” | <ul style="list-style-type: none"> • Independent auditor: Certification audit conducted 1st year, validation audit conducted the following year (Note: Certification audits are conducted every other year). • Supplier Self Assessment: Annually and submitted to the TAPA CA (who performed the original audit) within two weeks of original certification anniversary. |
| “B” | <ul style="list-style-type: none"> • Independent auditor: Certification audit conducted 1st year, validation audit conducted the following year (Note: Certification audits are conducted every other year). • Supplier Self Assessment: Annually and submitted to the TAPA CA (who performed the original audit) within two weeks of original certification anniversary. |
| “C” | <ul style="list-style-type: none"> • No audits by Buyer or independent auditor. • Supplier audits, when requested by Buyer. |

5. *Security/Loss Investigations*

(a) Supplier Investigation Responsibilities

- I. The Supplier, its agents and sub-contractors shall actively cooperate with law enforcement authorities, and the Buyer or their appointed agents in the conduct of an investigation into product, material or equipment that is lost, stolen, damaged or tampered with while under the responsibility of the Supplier or when the Supplier can provide assistance to any such investigation. All information, including regular updates, gathered by the Supplier, its sub-contractors or agents during the investigation shall be shared with the Buyer.
- II. A reporting procedure shall be included in the Suppliers own security procedures, see Section 2
- III. The Buyer shall have the right to oversee or participate in such investigations

6. *Waivers*

(a) Waivers

In exceptional circumstances, the TAPA CA may be confronted with a waiver request for a specific security requirement in part or whole on behalf of the supplier. TAPA has a sub team that reviews and approves/denies all waiver requests. It is the TAPA CA's responsibility to decide whether the request is valid and that substantial mitigating reason(s) exist that led to the waiver application. Request for waivers are more likely to be approved by TAPA if alternative security controls are introduced to mitigate the security exposure.

Waivers are valid for up to a maximum of 1 year. The original requirement must be completed on the expiration date of the waiver or requested and approved again.

(b) Waiver Process

- I. Supplier considers a specific requirement in the FSR is not required from a security standpoint.
- II. Supplier completes and submits Request For Waiver form to TAPA CA (See Section 3). One form should be completed for each FSR waiver request
- III. TAPA CA reviews waiver request(s) and determines if request is valid. Each TAPA region currently administers waiver requests independently and the regional Board of Directors should be contacted for appropriate waiver process.
- IV. If approved: -
 - Waiver specifics are documented and signed by the TAPA Certified Auditor
 - TAPA Certified Auditor assigns date for how long waiver will be approved, sends copy to Supplier

- Supplier will meet all requirements of waiver in agreed time scales. Failure to do so will result in waiver approval being removed.
- TAPA Certified Auditor informs Buyer of waiver.

V. If not approved:

- Supplier required to implement full requirement of FSR

7. Supplier Facility and Truck Security

(a) Procedures

Section 2 lists the detailed requirements for the Supplier's security procedures.

(b) Supplier Facility Security Requirements (Summary)

The Supplier's facility security is to be based on good physical barriers, the efficient operation of intruder alarm and CCTV surveillance and strict adherence to agreed operational procedures. The facility should not be located in an area that has a high incidence of crime or is adjacent to derelict land or a run-down area. Requirements for the Supplier's facility physical security are detailed in Section 2.

For purposes of audit, Preventive Measures are specific tactics to achieve acceptable levels of security for a given Area of Concern as identified in the TAPA audit form. These specific tactics have been identified through the knowledge and experience of industry security and logistics professionals, and represent best known methods and proven operational processes. However, in evaluating specific Preventive Measures of an individual Supplier, where such Supplier employs alternative methods that result in meeting or exceeding security requirements of the FSR, such methods shall be accepted, and rationale for acceptance noted in the audit "Comments" section. Additionally, specific tactics in the audit form which are in direct violation of Supplier documented policies and procedures shall be considered for removal from audit scoring on a case-by-case basis.

(c) Handling Operations

The various points at which the Buyer's assets will be transferred from one operation to another (i.e. truck to warehouse, warehouse to truck, truck to airline handler, airline handler to aircraft) are all viewed as areas of risk. The Supplier shall ensure all procedures for these operations are detailed and communicated to the Buyer. The Supplier shall notify the Buyer of any known deviation from these procedures.

(d) High Value Shipments by truck (Summary)

Shipments of Buyer's assets by truck between the Suppliers facilities and delivery to the final destination shall be subject to minimum-security requirements. The table in Section 2 also specifies the truck security requirements. The level of Security required is dependant on independent agreement between Buyer and Supplier.

Section 2 – Specifications

Contents:

- I. Supplier Facility/Truck Freight Security Requirements

I. Supplier Facility/Truck Freight Security Requirements

| Supplier Facility/Truck Freight Security Requirements ✓ = Requirement ✓M = Requirement & mandatory to pass audit | Applicable to Final Classification | | |
|---|------------------------------------|----|----|
| | A | B | C |
| 1. Perimeter Security | | | |
| 1.2. CCTV Systems | | | |
| 1.2.1 CCTV external coverage of shipping and receiving yard, including entry / exit point, to cover movement of vehicles and individuals. | ✓M | | |
| 1.2.2 CCTV coverage of all external dock area. | ✓M | ✓M | ✓M |
| 1.2.3 CCTV system able to view all exterior sides of the facility. | ✓M | | |
| 1.3. Lighting | | | |
| 1.3.1 Flood lighting of enclosed loading/unloading areas. | ✓ | ✓ | |
| 1.3.2 Dock doors illuminated externally at night. | ✓ | ✓ | ✓ |
| 1.3.3 External and internal lighting levels that support high quality CCTV images and recording. | ✓M | ✓M | ✓M |
| 1.4 Perimeter alarm detection | | | |
| 1.4.1 All facility external doors alarmed and linked to main alarm system. | ✓M | ✓M | ✓M |
| 1.5 Perimeter windows, doors & other openings | | | |

| Supplier Facility/Truck Freight Security Requirements | Applicable to Final Classification | | |
|--|------------------------------------|----|----|
| | A | B | C |
| <p>✓ = Requirement</p> <p>✓M = Requirement & mandatory to pass audit</p> | | | |
| 1.5.1 Any windows or other openings in warehouse walls and roof secured. | ✓M | ✓M | ✓ |
| 1.5.2 Ground floor warehouse windows protected by anti-ram posts or other physical barrier. | ✓ | | |
| 1.5.3 Dock doors of sufficient strength or design to prevent or delay forced entry by use of portable hand tools or ramming by vehicle. | ✓ | | |
| 1.5.4 Reinforced exit doors from warehouse (steel doors and frames or suitable alternative). | ✓ | ✓ | |
| 1.5.5 Exterior walls designed to resist penetration by removing building fabric, cutting or ramming by vehicle. | ✓ | ✓ | |
| 2. Access Control – Office Areas | | | |
| 2.1 Office Entrances | | | |
| 2.1.1 Visitor office access points controlled. | ✓ | | |
| 2.1.2 All office access points controlled. | ✓M | ✓M | |
| 2.1.3 Access control processes both during and outside normal operating hours to ensure access is granted only for authorized Supplier employees and visitors. | ✓ | ✓ | ✓M |
| 3. Facility Dock/Warehouse | | | |
| 3.1. Access control between office and dock/warehouse | | | |
| 3.1.1 Security controlled access points (e.g., Guard, card access or CCTV with intercom). | ✓M | ✓ | |
| 3.2. Limited access to dock areas | | | |
| 3.2.1 Only suppliers authorized employees and escorted visitors permitted access to dock/warehouse. | ✓ | ✓ | ✓ |
| 3.3. High value storage area | | | |

| Supplier Facility/Truck Freight Security Requirements | Applicable to Final Classification | | |
|--|------------------------------------|----|----|
| | A | B | C |
| <p>✓ = Requirement</p> <p>✓M = Requirement & mandatory to pass audit</p> | | | |
| 3.3.1 Restricted-access, caged/vault area for assets on site more than 2 hours: High-grade security mesh, chain-link, or hard-wall, including top/roof; alarmed, CCTV, controlled access. | ✓M | | |
| 3.3.2 Restricted-access, caged/vault area for assets on site more than 6 hours: High-grade security mesh, chain-link, or hard-wall, including top/roof; CCTV, controlled access. | | ✓M | ✓ |
| 3.4 All external dock and warehouse doors secured | | | |
| 3.4.1 All external dock and warehouse doors closed and locked unless required to be opened for normal transit operations. | ✓ | ✓ | ✓ |
| 3.5 CCTV coverage | | | |
| 3.5.1. Internal docks covered by CCTV. | ✓M | ✓M | ✓M |
| 3.5.2. Buyer designated assets under 100% CCTV surveillance while in Supplier facility (this does not require 100% of floor coverage, rather 100% coverage of buyer's assets e.g. CCTV from dock, to pallet breakdown or buildup area, to HVP cage). | ✓M | ✓M | |
| 3.6 Motion detection alarms | | | |
| 3.6.1 Motion detection alarms inside warehouse and activated when entire facility is vacated (N/A if facility is <u>true</u> 24x7x366 operation). | ✓M | ✓M | |
| 4. Security Systems | | | |
| 4.1. Monitoring of security systems | | | |
| 4.1.1 Manned security monitoring post 24x7x366; monitoring post secure from attack. | ✓M | ✓M | ✓ |
| 4.1.2 All security system alarms responded to in real-time 24x7x366. | ✓ | ✓ | ✓ |
| 4.2 Intruder alarm system | | | |

| Supplier Facility/Truck Freight Security Requirements | Applicable to Final Classification | | |
|--|------------------------------------|-----|----|
| | A | B | C |
| <p>✓ = Requirement</p> <p>✓M = Requirement & mandatory to pass audit</p> | | | |
| 4.2.1 Minimum of 60 day records on system alarms. | ✓ | ✓ | |
| 4.2.2 Restricted access to alarm system. | ✓M | ✓M | ✓ |
| 4.2.3 Alarms monitored. | ✓M | ✓M | ✓ |
| 4.3 CCTV system | | | |
| 4.3.1 All CCTV images are recorded in “real-time” (VCR or digital-recording system). See Scoring Matrix for clarification. | ✓ M | ✓ M | ✓ |
| 4.3.2 Restricted access to CCTV system functions. | ✓M | ✓M | ✓ |
| 4.3.3 Minimum 30-day retention of all CCTV recordings; recordings are held in secure storage area. | ✓M | ✓M | ✓M |
| 4.3.4 Preventative maintenance plan in place for CCTV systems (can be contracted or in-house). | ✓ | ✓ | ✓ |
| 4.4 Electronic access control system | | | |
| 4.4.1 Minimum 60 days records on system transactions. | ✓ | ✓ | |
| 4.4.2 Restricted access to system functions. | ✓ | ✓ | |
| 4.4.3 Quarterly review of access reports. | ✓ | ✓ | ✓ |
| 4.5 Security system maintenance | | | |
| 4.5.1 Preventative maintenance plan in place to routinely test and service access control and alarm systems. | ✓ | ✓ | ✓ |
| 5. Security Procedures | | | |
| 5.1 Adequate documented security procedures | | | |
| 5.1.1 Local documented procedures for handling Buyer’s assets and escalation procedures for communicating security incidents to Buyer. | ✓ | ✓ | ✓ |

| Supplier Facility/Truck Freight Security Requirements | Applicable to Final Classification | | |
|---|------------------------------------|----|---|
| | A | B | C |
| <p>✓ = Requirement</p> <p>✓M = Requirement & mandatory to pass audit</p> | | | |
| 5.1.2 Process for timely reporting of lost, missing or theft of Buyer's assets. Incidents to be reported by the Supplier to the Buyer within 12 hours; Obvious thefts reported immediately. | ✓ | ✓ | ✓ |
| 5.1.3 Emergency customer and local management contacts for security incidents listed and available. | ✓ | ✓ | ✓ |
| 5.1.4. Supplier Security Policy Statement available and communicated to all employees. | ✓ | ✓ | ✓ |
| 5.1.5 Security awareness training (including robbery response training) for all employees. | ✓ | ✓ | ✓ |
| 5.1.6 Employee and contractor company photo-ID badges issued and worn. | ✓ | ✓ | |
| 5.1.7 Procedures in place to restrict Supplier's employees, visitors and contractors access to Buyer's assets. | ✓ | ✓ | ✓ |
| 5.1.8 Badge policy for visitors/contractors in place. | ✓ | ✓ | ✓ |
| 5.1.9 Adequate control of paperwork. Restricting knowledge of transit of buyer's assets to "need to know" only (Information Security). | ✓ | ✓ | ✓ |
| 5.1.10 At inbound checkpoint for drivers and crews, identity and authorization are validated by officially-issued photo-ID (e.g.; drivers' license; passport or national ID card). | ✓M | ✓M | ✓ |
| 5.1.11 Keys controlled in areas where Buyers assets are transiting or stored. | ✓ | ✓ | ✓ |
| 5.1.12 Random trash inspection procedures in place for trash removal from dock/warehouse. | ✓ | ✓ | |
| 5.1.13 Security incident reporting system and method of tracking local security incidents. | ✓ | ✓ | |
| 5.1.14 Pre-loading or post-delivery storage of buyer's assets in trailers. | ✓ | ✓ | ✓ |

| Supplier Facility/Truck Freight Security Requirements | Applicable to Final Classification | | |
|--|------------------------------------|----|----|
| | A | B | C |
| <p>✓ = Requirement</p> <p>✓M = Requirement & mandatory to pass audit</p> | | | |
| 5.1.15 Personal containers (defined as lunch box, backpacks, coolers, purses, etc.) are controlled in the warehouse. | ✓ | ✓ | |
| 5.1.16 Exit Searches performed on exit from secure areas used for Buyer assets. | ✓ | ✓ | |
| 5.1.17 Personal vehicles access to shipping and receiving yard controlled. | ✓ | ✓ | |
| 5.1.18 Procedure in place to verify box and pallet integrity upon receipt. | ✓ | ✓ | |
| 5.2. Background checks (vetting) within constraints of Local Country laws | | | |
| 5.2.1 Criminal history check in place encompassing 5-year criminal history and employment check (vetting within constraints of local county laws). | ✓M | ✓M | ✓M |
| 5.3. Terminated employees & contractors procedure | | | |
| 5.3.1 Termination procedures in place for employees and contractors, ensuring return of ID's, access cards, keys and other sensitive information. | ✓ | ✓ | ✓ |
| 5.3.2 Procedures in place preventing systems access to Buyer's data by terminated employees. | ✓ | ✓ | ✓ |
| 5.3.3. Records maintained to consider background of previously terminated personnel before re-hiring. | ✓ | ✓ | ✓ |
| 6. Standard Truck Security Requirements | | | |
| 6.1 Adequate cargo truck security devices installed | | | |
| 6.1.1 Solid-top, hard-sided, locked cargo doors or reinforced soft-sided trailer. | ✓ | ✓ | ✓ |
| 6.1.2. Security tamper-evident seals for trucks carrying Buyer only shipments. | ✓ | ✓ | ✓ |
| 6.1.3. Vehicle immobilization devices in place. | ✓ | ✓ | |

| Supplier Facility/Truck Freight Security Requirements | Applicable to Final Classification | | |
|---|------------------------------------|---|---|
| | A | B | C |
| <p>✓ = Requirement</p> <p>✓M = Requirement & mandatory to pass audit</p> | | | |
| 6.1.4 Two way voice communications system between vehicle cab, Supplier's base (and escorts, if applicable) and procedures for reporting. | ✓ | ✓ | ✓ |
| 6.1.5 Written contingency plans in place for reporting unscheduled events (i.e. stops, delays, route deviation). | ✓ | ✓ | ✓ |
| 6.1.6 Truck cabin and ignition keys secured from unauthorized use at all times. | ✓ | ✓ | ✓ |
| 6.2. Scheduled routing | | | |
| 6.2.1 Routes, schedules and planned stops assessed for risk and reviewed. | ✓ | ✓ | |
| 6.3. Loading/unloading | | | |
| 6.3.1 Proof of shipping and receiving records (time, date, driver, shipping and receiving personnel, shipment details and quantity). | ✓ | ✓ | ✓ |
| 6.3.2 Policy in place requiring driver to be present for loading and unloading when allowed. | ✓ | ✓ | ✓ |
| 7. Pre-Alerts | | | |
| 7.1 System of Pre-Alerts in place (Supplier to Supplier) | | | |
| 7.1.1 Pre-alert capability in place. | ✓ | ✓ | |
| 7.1.2 Destination to notify origin within 4 hours of receipt of shipment, reconciling pre-alert shipment details. | ✓ | | |
| 8. Enhanced Security Requirements | | | |
| 8.1 Driver training | | | |
| 8.1.1 Supplier to provide robbery response training, detailing safe and secure actions to be taken during the event driver is threatened. Details of training are to be available to Buyer. | ✓ | ✓ | |

| Supplier Facility/Truck Freight Security Requirements | Applicable to Final Classification | | |
|--|------------------------------------|---|---|
| | A | B | C |
| <p>✓ = Requirement</p> <p>✓M = Requirement & mandatory to pass audit</p> | | | |
| 8.1.2 Security Awareness training provided to drivers on mitigating risk. Details of training are to be available to buyer. | ✓ | | |
| 8.2 Truck escorts (armed where local law permits) Cost shall be borne by Buyer | | | |
| 8.2.1 Capability to provide overt and covert escorts with real time communications to base and local police; written documentation in place. | ✓ | | |
| 8.2.2 Documented response procedures and training for escort personnel. | ✓ | | |
| 8.3 Vehicle tracking – subject to availability and negotiated between Buyer and Supplier | | | |
| 8.3.1 GPS or similar technology installed on all vehicles transporting Buyer’s assets. | ✓ | | |

Section 3 – Forms

Contents:

- I. Request for Waiver

FORM 3.1 – REQUEST FOR WAIVER

| | | | |
|---|--|---------------------------|------------------|
| DATE OF REQUEST | | SUPPLIER | Waiver #: |
| FACILITY LOCATION | | | |
| NAME OF PERSON REQUESTING WAIVER | | | |
| POSITION | | | |
| SIGNATURE | | | |
| FREIGHT SECURITY REQUIREMENT FOR WHICH WAIVER IS BEING REQUESTED (ONE REQUIREMENT ONLY, USE ADDITIONAL REQUEST FORMS IF NECESSARY): | | | |
| REASON FOR WAIVER REQUEST: | | | |
| ALTERNATIVE ACTIONS IMPLEMENTED OR PLANNED TO REDUCE RISK : | | | |
| This Section For TAPA Use Only | | | |
| Waiver Approved (Y/N) | | | |
| Date Waiver Commenced | | | |
| Date Waiver Expires (maximum 1 year) | | | |
| Approved By (Name): | | | |
| Approved By (Signature): | | | |
| Date: | | Waiver Reference # | |