FSR2014

FACILITY SECURITY REQUIREMENTS

TAPA

Transported Asset Protection Association

About TAPA

Transported Asset Protection Association

Cargo crime is one of the biggest supply chain challenges for manufacturers of high value, high risk products and their logistics service providers.

The threat is no longer just from opportunist criminals. Today, organized crime rings are operating globally and using increasingly violent attacks on vehicles, premises and personnel to achieve their aims. The Transported Asset Protection Association (TAPA) represents businesses fighting back against cargo crime that want to use real-time intelligence and the latest preventive measures to protect goods in the supply chain. TAPA is a unique forum that unites global manufacturers, logistics providers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains. Today, globally, TAPA's 700+ members include many of the world's leading consumer product brands as well as their logistics and transport providers with combined annual sales of over US$900 billion, law enforcement agencies (LEA), insurers and other trade associations.

The Association's Mission is to help protect our members' assets by:

- Exchanging information on a global and regional basis
- Co-operating on preventive security
- Increasing support from the logistics and freight industry and from law enforcement agencies and Governments
- Promoting and enhancing TAPA's globally recognized and applied Security Requirements

If you manufacture, distribute or transport high value products, TAPA membership should be critical to the success of your business, safeguarding your goods and workforce, ensuring customer orders are fulfilled and protecting your business reputation and financial performance.

TAPA statistics prove repeatedly that our members are measurably reducing cargo crime compared to the rest of the industry

For more information, please go to:

Americas	www.tapaonline.org
ASIA	www.tapa-asia.org
EMEA	www.tapaemea.com

About TAPA Standards

Transported Asset Protection Association

TAPA Security Standards (FSR/TSR/TACSS) have been established to ensure the safe and secure transportation, storage handling of any TAPA member's (Buyer's) assets throughout the world.

The TAPA Security Standards specify the minimum acceptable standards for security throughout the supply chain and the methods to be used in maintaining those standards. The TAPA Security Standards outlines the process and specification for Logistic Services Provider (LSP) to attain TAPA certification for their facilities, handling and transit operations. It is the intention of TAPA members to select LSPs that meet TAPA certification requirements. The successful implementation of the TAPA Security Standards is dependent upon LSPs, Authorized Auditors and Buyers working in concert.

However, the safe and secure transportation, storage and handling of the Buyer's assets is the responsibility of the LSP, its agents and sub-contractors, throughout the collection, transit, storage and delivery to the recipient, as specified in a Release. LSPs must have written and verifiable processes for the selection of sub-contractors. Periodic reviews of sub-contractor processes and facilities must be conducted based on risk.

The TAPA Security Standards will be referenced in any contract between the LSP and Buyer, and into the LSP's own security programme. The result of the LSP's failure to implement any part of the TAPA Security Standards shall be part of the contract between Buyer and LSP for freight services, and the provisions of that contract shall govern the rights and responsibilities of the parties in this case.

The specifics of the TAPA Security Standards; FSR, TSR and TACSS are described in separate chapters in this scope document.

Contents

Transported Asset Protection Association

1. Scope

Transported Asset Protection Association

(a) Introduction

Facility Security Requirements (FSR) have been established to ensure the safe and secure in-transit storage and warehousing of any TAPA member's (Buyer's) 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 LSPs to attain TAPA certification for their facilities and transit operations. It is the intention of TAPA members to select LSPs that meet or exceed TAPA certification requirements. The successful implementation of the FSR is dependent upon LSPs, Authorized Auditors and Buyers working in concert.

However, the safe and secure in-transit storage and warehousing of the Buyer's assets is the responsibility of the LSP, its agents and sub-contractors, throughout the collection, transit and delivery to the recipient, as specified in a Release. LSPs must have written and verifiable processes for the selection of sub-contractors. Periodic reviews of sub-contractor processes and facilities must be conducted based on risk.

The FSR will be referenced in any contract between the LSP and Buyer, and into the LSP's own security programme. The result of the LSP's failure to implement any part of the FSR shall be part of the contract between Buyer and LSP for freight services, and the provisions of that contract shall govern the rights and responsibilities of the parties in this case.

(b) FSR Applicable Areas

The FSR shall apply to warehouse operations in 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 LSP to ensure that the translation accurately reflects the intentions of the Buyer and to ensure that every relevant member of the workforce is trained to understand and implement the FSR.

(c) Resources to Implement the FSR

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

1. Scope

Transported Asset Protection Association

(d) Definitions

TERM	DEFINITION
Authorized Auditor	An Auditor working for an IAB, who has attended the TAPA Training and is authorized to conduct audits of TAPA Standards
Buyer	Purchaser of services and/or owner of transported goods
Documented Procedure	Means that the procedure is established, documented, implemented and maintained. A single document may address the requirements for one or more procedure. A requirement for a documented procedure may be covered by more than one document. Records established to provide evidence of conformity to requirements and or the effective operation of the supply chain security
Findings	Any areas that do not achieve the required standard shall be subject to a corrective action.
FSR	Facility Security Requirements: Standard describing the security requirements for warehouse operations.
IAB	Independent Audit/Certification Body appointed by Transported Asset Protection Association
Local crime	Criminal incidents occurring within local area of LSP's facilities and/or operations
Logistic Service Provider (LSP)	A forwarder, a manufacturer, a carrier, a trucking company, a warehouse operator, or any other company providing direct services within the supply chain.
SCAR	LSP Corrective Action Requirement
TAPA SECURITY STANDARDS	Overall Security Requirements segmented in TAPA FSR, TSR and TACSS: Note the terms "freight" and "cargo" are utilized interchangeably for all intents and purposes within the TAPA scope and documents.
TACSS	TAPA Air Cargo Security Standards: Describing the security standards for air cargo transportation meant for air cargo handling operations. (Ground handlers)
TSR	Trucking Security Requirements: Standard describing the security requirements for surface transportation by truck and trailer/container.
Waiver	In the occurrence that a requirement in any of the TAPA Security Standards are not met, a waiver can be applied for, describing the reason why as well as the alternative measures taken to secure the risk that is addressed by this requirement. The regional waiver committees will review the waiver request and grant or deny the waiver.
Workforce	All employees, Temporary Agency Staff, Sub- contractors, unless individually identified

2. Contract Acceptance

Transported Asset Protection Association

(a) LSP's Responsibilities at Acceptance of the Contract

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

3. Risk Assessment and Audits

Transported Asset Protection Association

(a) Buyer's and LSP's Responsibilities for Risk Assessments and Audits

I. At acceptance of the contract between the Buyer and the LSP, the LSP agrees to the 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 their behalf. Buyer or its agent shall notify the LSP at least five (5) working days in advance of any audit.

II. LSP shall ensure the IAB is engaged to ensure FSR audits and certification process is completed. Costs for TAPA certification shall be the responsibility of the LSP.

III. The requirement for TAPA certification is also extended to any LSP sub-contractor's facility where the Buyer's assets will be stored, distributed or transit through.

IV. The Buyer reserves the right to conduct unscheduled audits. The Buyer shall give a minimum of 24 hours' notice to the LSP.

V. The Authorized Auditor shall inform the LSP of assessment/audit results within ten (10) working days from the completion of the audit. A summary of the findings/results should be given informally to the LSP on the day of the audit/assessment at the closing conference.

VI. LSP shall have deemed to pass the audit and be certified for that specific facility location if the TAPA FSR audit requirements are all met. If requirements are not met, the LSP shall close the identified SCAR in the agreed time scale or apply for a waiver for the particular requirement that failed. When the Authorized Auditor submits a SCAR to the LSP associated with the audit findings, the LSP shall respond to the auditor within ten working days, documenting the action to be taken and the date the action will be completed. SCAR completion dates may be negotiated between the auditor and the LSP. However, unless the IAB approves a waiver from process, corrective action implementation shall not exceed sixty (60) days from notification to the LSP.

VII. When the Authorized Auditor submits a SCAR to the LSP associated with the audit findings, the LSP shall respond to the Authorized Auditor within ten working days, documenting the action to be taken and the date the action will be completed. SCAR completion dates may be negotiated between the Authorized Auditor and the LSP. However, unless the IAB approves a waiver from process, corrective action implementation shall not exceed sixty (60) days from notification to the LSP.

VIII. The LSP is required to complete self-audits of their facilities and their sub-contractor's facilities on each anniversary date of the certification and provide the results to the IAB to retain the certification given.

(b) Monitoring LSP Corrective Action Requirements

The LSP shall submit progress updates/reports on all outstanding SCARs to the Authorized Auditor each month. Any SCAR not completed before the due date shall be escalated by the LSP's Security Representative to the LSP's Management. The reason(s) for non-compliance shall be documented and communicated to the Authorized Auditor. LSP'S failure to address a SCAR may result in the withholding of the TAPA certification. The LSP has the right to appeal directly to TAPA if the certification is withheld. TAPA shall arbitrate the dispute between the LSP and the Authorized Auditor and retains the right to issue a binding resolution to the dispute.

3. Risk Assessment and Audits

Transported Asset Protection Association

(c) Storage/Warehouse/Distribution 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 LSP must complete a classification assessment before the effective date of the contract and give results to the Buyer. Separate TAPA FSR audit forms for A, B, & C facilities exist. The LSP, in cooperation with the Authorized Auditor, shall complete the final classification assessment within thirty (30) days of acceptance of contract. The IAB shall periodically complete their own classification assessments and ultimately make the decision on the final classification to be assigned to each of the LSP's facilities, handling or storing of the Buyer's assets. The LSP or Buyer can request the facility to be re-assessed if either party considers the assessment category to have changed.

(d) LSP/Buyer Facility Security Audit Schedule

For the duration of the contract the LSP will conduct security audits of their facility or their sub-contractor's facility in line with the audit schedule published below. The format of the audit is to be agreed upon with the Buyer. It is suggested the LSP use the same audit format as the Buyer will use in Section 3. Results of LSP self-audits shall be forwarded to the IAB within ten (10) working days of the self-assessment. A self-assessment is to be conducted annually within the anniversary month of the independent audit.

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

The TAPA FSR certificate shall be valid for a period of three (3) years with no extension permitted. In order to avoid and prevent any lapse in certification, a re-certification audit must be performed prior to the expiration date of the current certificate (This includes the completion of any corrective actions within the sixty-day period). The LSP should arrange the re-certification audit with the Authorized Auditor within three (3) months of the certificate expiration date and ensure that sufficient planning and preparation is made so that there is no lapse of the certification.

Where the TAPA FSR certificate is issued within the foresaid three-month period, the date of the certificate issuance will be the expiration date of the current certification. Should the corrective actions not be closed prior to the expiration date, the certification will expire.

CLASSIFICATION	LSP/SUB-CONTRACTOR'S SECURITY AUDIT REQUIREMENTS
"A"	Independent Auditor: Certification audit conducted 1st year, valid for three years, then re-certification is required. LSP Self Assessment: Annually and submitted to the Authorized Auditor (who performed the original audit) within two weeks of original certification anniversary dates.
"B"	Independent Auditor: Certification audit conducted 1st year, valid for three years, then re-certification is required. LSP Self Assessment: Annually and submitted to the Authorized Auditor (who performed the original audit) within two weeks of original certification anniversary dates.
"C"	Independent Auditor: Certification audit conducted 1st year, valid for three years, then re-certification is required. LSP Self Assessment: Annually and submitted to the Authorized Auditor (who performed the original audit) within two weeks of original certification anniversary dates.

4. Waivers

Transported Asset Protection Association

(a) Waivers

In exceptional circumstances, the Authorized Auditor may be confronted with a waiver request for a specific security requirement in part or whole on behalf of the LSP. Each waiver must be submitted via the IAB to the TAPA Regional Waiver Committee for approval.

In the first instance it is the Authorized Auditor'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 the TAPA Regional Waiver Committee if alternative security controls are introduced to mitigate the security exposure.

Waivers are valid for up to a maximum of 3 years.
The original requirement must be completed on the expiration date of the waiver or requested and approved again.

(b) Waiver Process

I. LSP considers a specific requirement in the FSR is not required from a security standpoint.

II. LSP completes and submits Waiver Request form to Authorized Auditor. One form should be completed for each FSR Waiver Request

III. Authorized Auditor reviews Waiver Request(s) and determines if request is valid.

IV. Authorized Auditor submits the Waiver Request form to the TAPA Regional Waiver Committee

V. If approved:

- *1 Waiver specifics are documented and signed by an authorized person on the TAPA Regional Waiver Committee
- *2 The TAPA Regional Waiver Committee assigns date for how long waiver will be approved and sends copy to the IAB
- *3 The IAB will notify the LSP of the outcome of the Waiver Request
- *4 LSP shall meet all requirements of waiver in the agreed upon time frame. Failure to do so shall result in the removal of the waiver approval.

VI. If not approved: LSP required to implement full requirement of FSR

Annex 1 Facility Security Requirements

Transported Asset Protection Association

Please Note the following Agreement:

1) Section 1.1.1 will become Mandatory from day 1 (January 1st 2014)
2) Due to possible budget problems to install such a fence, you have to apply for a waiver and we will grant waiver up to June 30, 2015.
3) After this date waivers will only be granted if officially approved by the waiver committees in each region.

	Security requirements and areas of concern.	A	B	C
1	Perimeter Security			
1.1.	Cargo handling and shipping and receiving yard			
1.1.1.	Physical barrier encloses cargo handling and shipping and receiving yard.	✓		
1.1.2.	Physical barrier height is a minimum of 6 feet / 1.8 meters	✓		
1.1.3.	Physical barrier maintained in good condition.	✓		
1.1.4.	Physical barrier is inspected for integrity and damage regularly	✓		
1.1.5.	Gate(s) manned or electronically controlled.	✓		
1.1.6.	Cargo handling and receiving yard is adequately controlled to prevent unauthorized access		✓	✓

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
	CCTV Systems			
1.2.	CCTV shipping and receiving yard.			
1.2.1.	CCTV able to view all traffic at shipping and receiving yard (including entry and exit point) ensuring all vehicles and individuals are identifiable.	✓	✓	
1.3.	CCTV coverage of all external dock area.			
1.3.1.	Dock areas covered via colour or "day/night" exterior cameras.	✓	✓	✓
1.3.2.	Cameras mounted to be able to view all activity around external dock area	✓		
1.3.3.	Cameras mounted to be able to view most activity around external dock area.		✓	✓
1.3.4.	All vehicles and individuals clearly identifiable.	✓		
1.3.5.	Vehicles and individuals visible in most cases		✓	✓
1.4.	CCTV system exterior sides of the facility.			
1.4.1.	Colour or "day/night" exterior camera system in place covering all exterior sides of the facility.	✓		
1.4.2.	Colour or "day/night" exterior camera system in place covering exterior sides of facility with doors, windows or other openings.		✓	
1.4.3.	All vehicles and individuals clearly identifiable.	✓		
1.4.4.	Vehicles and individuals visible in most cases.		✓	
1.4.5.	All views clear at all times.	✓		

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
	Lighting:			
1.5.	Flood lighting of loading/unloading areas.			
1.5.1.	Lighting adequate in loading and unloading areas.	✓	✓	✓
1.5.2.	All vehicles and individuals clearly identifiable.	✓		
1.5.3.	Vehicles and individuals visible in most cases		✓	✓
1.6.	Dock doors lighting.			
1.6.1.	All dock doors fully illuminated.	✓	✓	✓
1.7.	Exterior and interior lighting			
1.7.1.	Exterior and interior lighting levels are such that CCTV images and recordings are visible and clear.	✓	✓	✓
1.7.2.	All vehicles and individuals are clearly identifiable.	✓		
	Perimeter Alarm Detection			
1.8.	All facility external doors alarmed.			
1.8.1.	All facility external doors (warehouse and office) alarmed to detect unauthorized opening and linked to main alarm system.	✓	✓	✓
1.8.2.	Each emergency exits (in warehouse or office) alarmed at all times with an individual audible sounder and linked to main alarm system.	✓	✓	✓
1.8.3.	Each facility external door (warehouse or office) opening can be uniquely identified per door or per zone within main alarm system.	✓		

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
	Perimeter windows, and other openings			
1.9.	Windows and any openings in warehouse walls and roof secured.			
1.9.1.	All Windows and any openings (smoke vents, air vents), in warehouse walls protected by physical means (bars, mesh or any other material that would harden opening to burglary),	✓	✓	
	or			
1.9.2.	Alarm system that specifically covers those openings to detect entry.	✓	✓	
1.9.3.	Any other openings in roof (smoke vents. air vent, sky-lights) protected by physical means (bars, mesh or any other material that would harden opening to burglary),	✓		
	or			
1.9.4.	Alarm system that specifically covers those openings to detect entry.	✓		
1.10.	Secure Floor-mounted warehouse windows (N/A if no windows)			
1.10.1.	Floor-mounted warehouse windows (at ground floor) and street-level dock doors and ramps protected by anti-ram posts or other physical barrier.	✓	✓	
1.11.	Dock Doors construction.			
1.11.1.	All dock doors of sufficient strength to delay forced entry by use of portable hand tools or ramming by vehicle.	✓	✓	✓
1.12.	Pedestrian doors from warehouse.			
1.12.1.	Warehouse pedestrian doors (excluding designated Emergency exit doors) cannot be easily penetrated; hinges on inside or spot welded or pinned if on the outside	✓	✓	✓
1.12.2.	Warehouse pedestrian doors and frames constructed of reinforced steel or suitable alternative.	✓	✓	

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
	Perimeter windows, and other openings			
1.13.	Exterior walls and roof designed and maintained to resist penetration or alarmed.			
1.13.1.	Exterior walls and roof designed and maintained to resist penetration (Example: brick, block, tilt up concrete slab, sand-witch panel walls).	✓	✓	✓
1.13.2.	Interior multi-tenant walls and roof constructed/designed and maintained to resist penetration (Example: brick, block, tilt up concrete slab, sand-witch panel walls) (Note – wire mesh/ netting of any kind is not allowable)	✓	✓	✓
	or			
1.13.3	Alarmed to detect any intrusion	✓	✓	✓
1.14.	External access to roof secured. N/A if no external roof access.			
1.14.1.	External access to roof (ladder or stairs) secured by physical or electronic means.	✓	✓	✓
1.14.2.	Keys controlled.	✓	✓	✓
1.14.3.	External access to roof (ladder or stairs) covered by CCTV.	✓		

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
2	Access Control - Office Areas Office Entrances			
2.1.	Visitor entry point(s) controlled.			
2.1.1.	Access at visitor entry point(s) controlled by an employee/guard/receptionist that has been trained on badge issuance, controls, logging visitors, escort requirement, etc (process for out of hours visits in place)	✓	✓	✓
2.1.2.	Visitor entry point(s) covered by CCTV; individuals clearly identifiable	✓	✓	
2.1.3.	Access at visitor entry point(s) securely controlled by electronic card access.	✓		
2.1.4.	Duress (panic) alarm installed.	✓	✓	
2.2.	Workforce entry point(s) controlled (24/7)			
2.2.1.	Workforce entry point(s) access controlled 24/7		✓	✓
2.2.2.	Workforce entry point(s) controlled through electronic access control device 24/7. Access logged.	✓		
2.2.3.	Workforce entry point(s) covered by CCTV.	✓	✓	

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
3	Facility Dock/Warehouse Access control between office & dock/ warehouse			
3.1.	Security controlled access points (e.g., Guard, card access or CCTV with intercom).			
3.1.1.	Access controlled between office and warehouse or dock.	✓	✓	
3.1.2.	Door alarms are locally audible and send alarm for response when held or forced open.	✓		
3.1.3.	Door alarms are locally audible or send alarm for response when held or forced open.		✓	
3	Limited access to dock areas			
3.2.	Access to dock/warehouse			
3.2.1.	LSP's authorized workforce and escorted visitors permitted access to dock/warehouse areas based on a business need and restricted.	✓	✓	✓
3.2.2.	Access list in place and updated on a regular basis or upon need.	✓	✓	
3	High Value storage areas			
3.3.	High Value Cage specifications			
3.3.1.	Perimeter caged or hard-walled on all sides, including top/roof.	✓	✓	
3.3.2.	Locking device on door/gate	✓	✓	
3.3.3.	Complete CCTV coverage on cage or vault entrance and internal area.	✓		
3.3.4.	CCTV coverage on cage or vault entrance.		✓	
3.3.5.	Access logged and access list in place to limit/verify that access is only granted to designated/authorized personnel.	✓	✓	
3.3.6.	Perimeter of cage/vault maintained in good condition and regularly inspected for integrity and damage.	✓		
3.3.7.	Access controlled electronically.	✓		
3.3.8.	Alarmed doors/gates.	✓		
3.3.9.	Access list reviewed on regular basis to limit/verify that access is only granted to designated/authorized personnel, processes are documented.	✓	✓	
3.3.10.	Size must meet customer's requirements or, when no customer requirements exists, must at least have space for 6 pallet positions	✓	✓	

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
3	All external dock and warehouse doors secured			
3.4.	External dock and warehouse doors secured			
3.4.1.	Dock doors closed (when not in active use) and secured by slide or bolt latch.	✓	✓	
	or			
3.4.2.	Scissor gates (minimum height of 8 feet / 2.4 meters) or equivalent in place and used on dock doors when not in active use.	✓	✓	
3.4.3.	All external warehouse doors always closed and secured when not in active use.	✓	✓	✓
3.4.4.	Keys controlled.	✓	✓	✓
	CCTV coverage			
3.5.	Internal dock doors and dock areas.			
3.5.1.	All internal dock doors and dock areas covered by CCTV.	✓	✓	✓
3.5.2.	Clear views of freight being loaded/unloaded.	✓	✓	✓
3.6.	Buyer-designated assets under CCTV surveillance			
3.6.1.	Buyer-designated assets under 100% CCTV surveillance while in LSP's Facility (this does not require 100% of floor coverage, rather 100% coverage of Buyer's Assets e.g. CCTV from dock, to pallet breakdown/build-up area, to high-value cage/vault).	✓	✓	
	Intrusion detection			
3.7.	Intrusion detection. N/A if warehouse activity is true 24x7x366 operation.			
3.7.1.	Intrusion detection alarms installed in office and warehouse to detect all intrusions.	✓	✓	✓
3.7.2.	System activated during non-operational hours.	✓	✓	✓
3.7.3.	Intrusion detection alarms installed in office and warehouse to detect all intrusions with space to be zoned based on hours of operation.	✓		
3.7.4.	Anti-masking used on passive infrared devices.	✓		

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
4	Security Systems			
4.1.	Monitoring post.			
4.1.1.	Monitoring of alarm events 24x7x366 via a monitoring post, secured from attack	✓	✓	✓
4.2.	Alarms response			
4.2.1.	All security system alarms responded to in real-time 24x7x366.	✓	✓	✓
4.2.2.	Monitoring post acknowledges alarm-activation and escalates in less than 3 minutes.	✓	✓	✓
4.2.3.	Alarm monitoring reports available.	✓	✓	✓
4.2.4.	Documented response procedures.	✓	✓	✓
	Intruder alarm systems			
4.3.	System alarm records			
4.3.1.	60 days of security system alarm records maintained.	✓	✓	
4.3.2.	Security system alarm records and securely stored and backed up.	✓		
4.3.3.	Security system alarm records securely stored.		✓	

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
4	Security Systems			
4.4.	System restrictions.			
4.4.1.	Security system access restricted (Central equipment and data access)	✓	✓	✓
4.4.2.	Controls changed when individuals depart.	✓	✓	✓
4.4.3.	Documented procedure.	✓	✓	
4.5.	Alarms transmitted and monitored.			
4.5.1.	Alarm transmitted on power failure/loss.	✓	✓	✓
4.5.2.	Alarm set verification in place.	✓	✓	✓
4.5.3.	Alarm transmitted on device and/or line failure.	✓	✓	
4.5.4.	Back-up communication system in place on device and/or line failure.	✓	✓	
4.5.5	Documented response procedures.	✓	✓	✓

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
4	CCTV systems			
4.6.	CCTV recording.			
4.6.1.	Digital recording in place.	✓	✓	✓
4.6.2.	Digital recording functionality checked daily on operational days.	✓	✓	✓
4.6.3.	Minimum 3 frames per second per camera.	✓	✓	✓
4.6.4	Documented procedure. Records available.	✓	✓	✓
4.7.	CCTV access			
4.7.1.	Access tightly controlled to CCTV system.	✓	✓	✓
4.7.2.	Security of storage controls adequate (central system and data).	✓	✓	✓
4.7.3.	CCTV images in view of only authorized or designated personnel.	✓	✓	✓
4.7.4.	Documented procedures in place detailing data protection.	✓	✓	
4.8.	CCTV recording retention.			
4.8.1.	CCTV recordings stored for a minimum of 30 days	✓	✓	✓

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
4	Electronic access control system			
4.9.	Access recording retention.			
4.9.1.	90 days of system transaction records available. Records securely stored; backed up	✓	✓	
4.10.	Access restriction.			
4.10.1	Access restricted to access control system functions.	✓	✓	
4.10.2.	Controls changed when individuals depart.	✓	✓	
4.10.3	Documented procedure.	✓	✓	
4.11.	Review of access reports.			
4.11.1.	Reviews conducted (for any irregularities and access levels) at least once a quarter.	✓	✓	✓
4.11.2.	Documented procedure.	✓	✓	

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
5	Security Procedures			
5.1.	Escalation procedures.			
5.1.1.	Local documented procedures in place for handling Buyer's assets and escalation of security incidents to the Buyer and consistently followed	✓	✓	✓
5.1.2.	Process for timely reporting of lost, missing or stolen Buyer's assets. Incidents to be reported by the LSP to the Buyer within 12 hours. Obvious thefts reported immediately. Process consistently followed.	✓	✓	✓
5.1.3	Emergency Buyer and LSP facility management contacts for security incidents listed and available.	✓	✓	✓
5.1.4.	Listing regularly updated and includes law enforcement contacts.	✓	✓	✓
5.2.	Management commitment			
5.2.1.	The LSP to provide evidence of its commitment, by appointing a member of senior management responsible for the FSR programme and with the necessary authority.	✓	✓	✓
5.2.2.	The LSP must have in place a Security Policy endorsed by senior management, communicated to all relevant workforce and third parties, including contractors and visitors, with the intent that these persons are made aware of their individual security management-related obligations. This policy to be documented, implemented and maintained, and be reviewed regularly for relevance to the supply chain.	✓	✓	✓
5.2.3.	Documented procedures for identification and assessment of security threats and risks relating to their facility/routes, and must as a minimum, be appropriate to the nature and scale of their operations. The assessment shall consider the physical failure; operational; nature environmental events; factors outside of its control.	✓	✓	✓
5.2.4.	Documented procedures for identification and its compliances to the legal, statutory and all its stakeholders' security requirements.	✓	✓	✓

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
5	Security Procedures			
5.3.	Training			
5.3.1.	Security Awareness / Threat awareness training provided to all workforce within the scope of the facility security programme. Training repeated each 2 years	✓	✓	✓
5.3.2.	Training developed and rolled out based on local risks	✓	✓	✓
5.4.	ID badges.			
5.4.1.	After vetting, all employees must be issued with company photo–ID badges	✓	✓	
5.4.2.	All other workforce must be provided with a company ID badge to make them identifiable within the facility.	✓	✓	
5.4.3.	All workforce's badges clearly displayed	✓	✓	
5.5.	Access to Buyer's assets.			
5.5.1.	Written and documented procedures in place to restrict employees, visitor and contractor access to Buyer's assets.	✓	✓	
5.6.	Visitor policy			
5.6.1.	All visitors identified using government-issued photo-ID (e.g.; driver's licence; passport or national ID card, etc.).	✓	✓	✓
5.6.2.	All visitors registered and log maintained for minimum of 30 days.	✓	✓	✓
5.6.3.	All visitor badges reconciled against log.	✓	✓	
5.6.4.	All visitors visibly display temporary badges or passes.	✓	✓	
5.6.5.	All visitors escorted by company personnel.	✓	✓	
5.6.6	Visitor policy documented	✓	✓	

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
5	Security Procedures			
5.7.	Document Control			
5.7.1.	Access to shipping documents and information on Buyer's assets controlled based on "need to know".	✓	✓	✓
5.7.2.	Access monitored and recorded.	✓	✓	✓
5.7.3.	Documents safeguarded until destruction.	✓	✓	✓
5.7.4.	Information security awareness training provided to workforce having access to information.	✓	✓	
5.8.	Driver identification.			
5.8.1.	All drivers identified using government-issued photo-ID (e.g.; driver's licence; passport or national ID card, etc.).	✓	✓	✓
5.8.2.	Driver log maintained	✓	✓	✓
5.8.3.	Vehicle licence plate and description logged.	✓		
5.8.4.	Verification that photo-ID is not expired, matches the driver, and licence appears valid	✓		
5.9.	Keys control Buyer assets			
5.9.1.	Keys controlled in areas where Buyer's assets are transiting or stored.	✓	✓	✓
5.9.2.	Written key plan in place.	✓	✓	
5.10.	Trash inspection			
5.10.1	Full trash inspection programme or compacting in place in dock/warehouse area.	✓		
5.10.2.	Random trash inspection programme in place in dock/warehouse area.		✓	
5.10.3.	Clear trash bags utilized.	✓		
5.10.4.	Inspection/interior compacting monitored by CCTV.	✓		

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
5	Security Procedures			
5.11.	Security incident reporting			
5.11.1.	Security incident reporting and tracking system in place, used to implement proactive measures.	✓	✓	
5.12.	Pre-loading and Staging			
5.12.1.	No pre-loading/post-delivery and staging of Buyer's assets in trailers/containers allowed unless when in Buyer's contract or formal written / signed off approved by Buyer.	✓	✓	✓
5.13.	Personal containers			
5.13.1.	Written Security procedures define how entry of 'personal containers' (defined as lunch boxes, backpacks, coolers, purses, etc.) into the warehouse is controlled.	✓	✓	
5.14.	Exit searches.			
5.14.1.	Documented procedure for exit search or inspection programme from secure area in place based on Buyer's and LSP's risks.	✓		
5.15.	Personal vehicles access			
5.15.1.	Personal vehicles not allowed access to shipping and receiving yard/area unless fully supervised and controlled	✓	✓	✓
5.15.2.	Documented procedure.	✓	✓	✓
5.16.	Control of cargo-handling equipment.			
5.16.1.	All forklifts, hand-jacks, pallet-loaders or other cargo-handling equipment disabled, locked or secured during non-operational hours.	✓	✓	
5.16.2.	Documented procedure.	✓	✓	

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
5	Security Procedures			
5.17	Container or trailer integrity.			
5.17.1.	Seven-point physical inspection process performed for all dedicated containers or trailers: Front wall, Left side, Right side, Floor, Ceiling/Roof, Inside/outside doors and locking mechanism, Outside/Undercarriage	✓	✓	✓
5.17.2.	Documented procedure.	✓	✓	✓
5.18.	Maintenance programmes.			
5.18.1.	Documented maintenance programmes in place for all technical (physical) security installations/systems to ensure functionality at all times (e.g. CCTV, Access controls, Intruder detection, Lighting).	✓	✓	✓
5.18.2.	Preventive maintenance conducted once a year.	✓	✓	✓
5.18.3.	Documented procedure, followed by physical/visual checks of all systems once per week.	✓	✓	
5.18.4.	Response-time to initiate / call out is less than 48 hrs.	✓	✓	
5.19	Assessment process			
5.19.1.	LSP must have a programme in place to perform a security risk analysis of the facility	✓		
5.19.2.	LSP to have a sub - contractor / vendor management process in place	✓		

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
6	Background Checks (Vetting) Workforce Integrity			
6.1.	Screening/vetting of workforce			
6.1.1.	Applicants required to disclose previous employment history, gaps in employment, current criminal convictions, job terminations in similar/same industry, job related qualifications.	✓	✓	✓
6.1.2.	The procedure must identify the person / resources responsible for conducting the vetting / screening process which includes, but not limited to, criminal history and employment checks and verification of information provided by the applicant.	✓	✓	✓
6.1.3.	TAS worker required to sign declaration that they have no current criminal convictions and will comply with LSP's security procedures	✓	✓	✓
6.1.4.	LSP will have agreements in place to have required information supplied by the agency and/or sub -contractor providing TAS workers, or shall conduct such screening themselves. Screening must include criminal history check and employment checks.	✓	✓	✓
6.1.5.	Procedure for dealing with applicants/workforce's false declaration pre & post hiring.	✓	✓	✓
6.2.	Termination of workforce			
6.2.1.	Documented procedures in place for termination of members of the workforce. The procedures to include return of ID's, access cards, keys and other sensitive information and/or equipment.	✓	✓	✓
6.2.2.	Workforce checklist in place for verification	✓	✓	✓
6.2.3.	Procedures are in place to prevent LSP from re-hiring workforce if denial/termination criteria are still valid.	✓	✓	✓
6.2.4.	Procedures are in place to prevent terminated workforce from having access to Buyer's data and records.	✓	✓	✓

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
7	Freight hand over process			
7.1.	Security seals			
7.1.1.	Process in place for the use of tamper evident security seals, electronic or manual, that meets the ISO 17712 standard, unless on Buyer's exemption.	✓	✓	✓
7.1.2.	Access to and issuance of seals controlled.	✓	✓	✓
7.1.3.	Seals affixed and removed by authorized personnel other than the driver.	✓	✓	✓
7.1.4.	Procedures in place for recognizing and reporting compromised seals	✓	✓	✓
7.2.	Shipping and receiving records			
7.2.1.	All cargo verified against shipping documents (Proof of Delivery, Bill of Loading, Waybill, etc.) and manifest to ensure proper marking, weights, counts, etc	✓	✓	✓
7.2.2.	Documents legible, complete and accurate (i.e. time, date, signatures, driver, shipping and receiving personnel, shipment details and quantity, etc.).	✓	✓	✓
7.2.3.	LSP must maintain records of all collections and proof of deliveries, for a period of not less than two years, which can be accessed when investigation of loss is necessary.	✓	✓	✓
7.3.	Box and pallet integrity verified upon receipt & delivery			
7.3.1.	LSP must have documented procedures that box and pallet verifications needs to be performed before any loading is carried out and as soon as unloading is completed. The required documentation demonstrating such verifications needs to be kept for a period of 2 years.	✓	✓	✓
7.4.	Proof of shipping and receiving records			
7.4.1.	LSP must have documentation that provides evidence that the cargo is verified against shipping documents and manifest to ensure proper marking, weights, counts, etc. These documents must be legible, complete and accurate (i.e. time, date, signatures, driver, shipping and receiving personnel, shipment details and quantity, etc.)	✓	✓	✓

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
7	Freight hand over process			
7.5.	Driver to be present for loading and unloading			
7.5.1.	LSP to have a documented procedure requiring driver to be present for loading and unloading (if allowed) and piece count conducted by driver. There must be documented evidence of this practice.	✓	✓	✓
7.6.	Pre-alert capability in place			
7.6.1.	Pre-alert capability in place and documented for both inbound and/or outbound shipments	✓	✓	✓
7.6.2.	Pre-alerts include at a minimum: departure time, expected arrival time, trucking company, driver name, shipment info (pc count, weight, bill-of-lading number, etc.) and trailer seal numbers.	✓	✓	✓
7.7	POD (Proof of Delivery)			
7.7.1.	Destination to notify origin within 4 hours of receipt of shipment, reconciling pre-alert shipment details.	✓	✓	✓
7.8.	Fraudulent pick-ups			
7.8.1.	Documented procedure in place to ensure that the incoming truck details match the pre-alert received. At a minimum the following information must be verified; expected arrival time, trucking company, driver name, license plate details, shipment pick-up info (pc count, weight, bill-of-lading number, etc.)	✓	✓	✓

Annex 2: Waiver Request Form

Transported Asset Protection Association

DATE OF REQUEST		LSP	Waiver #:
FACILITY LOCATION			
NAME OF PERSON REQUESTING WAIVER			Position
SIGNATURE			
NAME OF AUDIT BODY			NAME OF AUDITOR
THE REQUIREMENT FOR WHICH WAIVER IS BEING REQUESTED AND FOR WHICH STANDARD (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 3 year)			
Approved By (Name):			
Approved By (Signature):			
Date:			Waiver Reference #

FSR2014

TAPA

Transported Asset Protection Association