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

TAPA's mission is to minimise cargo losses from the supply chain. TAPA achieves this through the development and application of global security standards, recognized industry practices, technology, education, benchmarking, regulatory collaboration, and the proactive identification of crime trends and supply chain security threats

For more information, please go to:

Americas	www.tapaonline.org
ASIA	www.tapa-apac.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 Facility Security Requirements (FSR) represents minimum standards, specifically for secure warehousing, or in-transit storage, within a supply chain. TAPA FSR certification is discussed further in this document.

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 subcontractors, throughout the collection, transit, storage and delivery to the recipient, as specified in a release or contract. Where the FSR is referenced or included in the contract between the LSP and Buyer, the FSR is part of the contracted security requirements between Buyer and LSP, and shall be referenced in the LSP's security programme. Further, where the FSR is part of the contracted security requirements any alleged failure by the LSP to implement any part of the FSR shall be resolved in line with managing disputes under the terms of the contract negotiated between Buyer and LSP.

Legal Guidance: Scope, Translation, the "TAPA" brand and Limits of Liability.

The FSR is a global standard and all sections of the standard are mandatory unless an exception is granted via the waiver process. In geographical areas where English is not the first language, and where translation is necessary and applicable, it is the responsibility of the LSP and its agents to ensure that any translation of the FSR, or any of its parts, accurately reflects the intentions of TAPA in the development and publication of these standards. "TAPA" is a registered trademark of the Transported Asset Protection Association and may not be used without the express written permission of TAPA through its officially recognized regions.

TAPA standards and associated material are published through, and by TAPA, and may not be revised, edited, or changed by any party without the express written permission of TAPA. Misuse of the TAPA brand may result in removal of certification or legal action. By publication of these standards, TAPA provides no guarantee or assurance that all cargo theft events will be prevented, whether or not the standards are fully deployed and properly implemented. Any liability that may result from a theft of cargo in transit, or any other loss to cargo in transit under the FSR standards, will be for the account of the LSP and/or the Buyer in accordance with the terms and conditions in their contract with each other and any laws or statutes which may apply within the subject jurisdiction.

Contents

Transported Asset Protection Association

1. Scope

Transported Asset Protection Association

The FSR may apply to:

- any, or all locations within the global supply chain depending on risk and/or Buyer or LSP requirements, etc.
- LSP owned or operated facilities
- Buyer owned or operated facilities

2. Resources to implement the TAPA 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.

3. Protecting LSP Policies and Procedures

Transported Asset Protection Association

Copies of security policies and procedures documents will only be submitted to Buyer in accordance with signed disclosure agreements between LSP and Buyer and shall be handled as confidential information.

4. Certification/Classification

Transported Asset Protection Association

a. TAPA Certification

The LSP shall ensure an IAB, trained/qualified on the current FSR, is engaged to complete the audit and certification process. The audit format will be the current FSR audit form. Costs for TAPA certification shall be the responsibility of the LSP, unless otherwise negotiated with the Buyer(s).

The 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.

The Authorized Auditor shall inform the LSP of assessment / audit results within ten (10) working days from the completion of the audit. Any delays in issuing the audit results must be promptly communicated to the LSP and negotiated between the IAB and LSP. An informal summary of the findings/results should be shared with the LSP during the audit/assessment closing conference.

b. Classification Level: A, B, C

Facilities are classified into one of three FSR levels: "A" being the highest security level and "C" the lowest.

LSPs or Buyers may decide to become classified at a lower level to begin with, and then progress to B or A level as improvements are made to the facility. Additionally, as negotiated between Buyer and LSP, facilities located in high risk countries may be classified at level A while all other countries are classified at B, or C, level. In all cases, it is the responsibility of the Buyer to negotiate the classification level directly with the LSP.

LSPs must inform the Authorized Auditor which level they are seeking certification for, before the certification audit is begun.

The LSP or Buyer can request their own facility to be re-certified if either party considers the classification level to have changed.

5. Corrective Action/Compliance Monitoring

Transported Asset Protection Association

a. Corrective Action

If requirements are not met, the Authorized Auditor will submit a SCAR (Security Corrective Action Requirement) to the relevant LSP. The LSP shall respond to the auditor within ten (10) 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 Regional TAPA Waiver Committee approves a waiver, corrective action implementation shall not exceed sixty (60) days from notification to the LSP.

In all cases, the LSP shall submit monthly progress updates/reports on all outstanding SCARs to the Authorized Auditor. 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 noncompliance 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.

Note: It is not necessary for the Authorized Auditor to re-audit the facility in order to close a SCAR. Evidence of SCAR closure (i.e. achieving compliance) can be presented to the Authorized Auditor in the form of written correspondence, web meetings or conference calls, photographs, etc.

b. Compliance Monitoring

Self-Audits: For the duration of the contract the LSP, or Buyer (if Buyer's facility is FSR certified) will conduct documented self-audits according to the audit schedule published below. The self-audit must reflect the FSR requirements. Results of self-audits shall be forwarded to the IAB within ten (10) working days of completion.

Subcontractor Audits: Subcontractors that are not TAPA certified, must be audited in accordance with the Buyer – LSP contract.

Buyer site visits to LSPs: The Buyer and the LSP recognize the importance of working in partnership to reduce risk within the supply chain.

Both parties agree to schedule Buyer site visits with reasonable notice (Ex: 10 working days), with scope and parameters mutually agreed in advance and/or in accordance with the Buyer/LSP contract. Loss investigations (i.e. thefts, damage, etc) shall be performed in accordance with the Buyer/LSP contract.

Audit Schedule

CLASSIFICATION	LSP/SUBCONTRACTOR'S SECURITY AUDIT REQUIREMENTS
"A" "B" "C"	Certification Audit: IAB / Authorized Auditor Certification audit conducted 1st year, valid for three years, then re-certification is required.
	LSP Self-Audit: Annually and submitted to the Authorized Auditor (who performed the original audit) within two weeks of original certification anniversary dates.
	LSP Subcontractor Audit: In accordance with the Buyer – LSP contract.

6. Recertification

Transported Asset Protection Association

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, including completion of any SCARs within the sixty (60) day allotted period (see corrective action section). Therefore, to assure adequate planning and preparation, it is recommended the LSP arrange the re-certification audit three (3) months before the current certificate expiration date. Where the TAPA FSR certificate is issued within the foresaid three (3) month period, the date of the new certificate will be the expiration date of the current certification. Should the corrective actions not be closed prior to the expiration date, and there is no waiver granted, the certification will expire.

7. Subcontracting

Transported Asset Protection Association

Subcontractors that are not TAPA certified must be audited in accordance with the Buyer–LSP contract.

8. 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 must 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

9. Definitions

Transported Asset Protection Association

TERM	DEFINITION
ADEQUATELY	In a satisfactory manner so no or very minimal gaps exist in local procedures
AUTHORIZED AUDITOR	An Auditor working for an IAB, who has attended the TAPA Training and is authorized to conduct audits of TAPA Standards
AT ALL TIMES	100% unless a temporary obstruction/delay of a few minutes due to operational movements
BUYER	Purchaser of services and/or owner of transported goods
BACKED UP	To make a copy of a data file which is stored securely in a separate location and can be used as a security copy.
CCTV	An internal and /or external colour or day/night camera system
DOCUMENTED PROCEDURE	A written description of a prescribed action or process. A single documented procedure may address multiple actions or processes. Conversely, actions or processes may be documented across one, or more, procedures
FINDINGS	Finding: an "observation of non-compliance with a TAPA standard requirement" Note: All findings will be documented in a SCAR.
FCL	FCL is full container-load and indicates that the cargo is dedicated for one Buyer
FTL	FTL is a full-truckload and indicates that the cargo is dedicated for one Buyer
FSR	Facility Security Requirements: Standard describing the security requirements for warehouse operations.
HARD SIDED TRAILERS	Hard sided trailers include trailers whose sides, floor and top are constructed of metal or other solid material
HVTT	High Value Theft Targeted Cargo
IAB	Independent Audit/Certification Body appointed by Transported Asset Protection Association
LTL	LTL is less than load, usually referring to a consolidated load that may be in a truck or container and may contain cargo for multiple Buyers
LOCAL CRIME INCIDENT	Criminal incidents occurring within the certified facility and or the local area to the LSP
LOGISTIC SERVICE PROVIDER (LSP)	A forwarder, a carrier, a trucking company, a warehouse operator, or any other company providing direct services within the supply chain.
MOU	Memorandum of Understanding between the Independent Audit Bodies and TAPA. Specifies the procedures the audit body shall follow to support the certification scheme
RECOGNIZABLE	A unique or distinguishing feature that identifies the specific object or person
REGULARLY	At least weekly
SCAR	Security 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	Waiver: Written approval to exempt a facility from a TAPA requirement or accept an alternative compliance solution. Note: The TAPA Regional Waiver Committee review and grant or deny all waivers (see waiver process).
WORKFORCE	All Employees, Temporary Agency Staff, Subcontractors, unless individually identified

Annex 1 Facility Security Requirements

	Security requirements and areas of concern.	A	B	C
1	Perimeter Security			
1.1.	Warehouse cargo handling, shipping and receiving yard			
Option 1:				
1.1.1.	Physical barrier encloses cargo handling, 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 .		✓	✓
	or			
Option 2: (no physical barrier)				
1.1.7.	Visible perimeter signs in local language indicating “No unauthorized access”, “No unauthorized parking”.	✓		
1.1.8.	Visible signs on external dock doors or walls instructing drivers, visitors etc. to proceed to appropriate lobby, security control.	✓		
1.1.9.	Documented procedure requiring periodic sweeps/patrols by CCTV and/or guards and/or responsible member of the workforce.	✓		
1.1.10.	Procedure documented describing how unauthorized vehicles and persons are to be managed. Training on procedure must be delivered to relevant members of workforce, including guards.	✓		
1.1.11.	For ground level accessible windows or dock doors, the annual risk assessment must evaluate the need for anti-ram barriers (see Risk Assessment: section 5.2.3).	✓		
1.1.12.	Cargo handling and receiving yard is adequately controlled to prevent unauthorized access.		✓	✓

Annex 1 Facility Security Requirements

	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 recognizable at all times unless temporary obstruction due to operational needs (i.e. truck unloading).	✓	✓	
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 operations and movement around external dock area.	✓		
1.3.3.	Cameras mounted to be able to view all operations and movement around external dock area unless temporary obstruction due to operational needs (i.e. truck unloading).		✓	✓
1.3.4.	All vehicles and individuals clearly recognizable.	✓		
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 recognizable.	✓		
1.4.4.	Vehicles and individuals visible in most cases.		✓	
1.4.5.	All views clear at all times unless temporary obstruction due to operational needs (i.e. truck unloading).	✓	✓	

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. (Constant light or activated by alarm or motion detection providing immediate illumination).	✓	✓	✓
1.5.2.	All vehicles and individuals clearly recognizable.	✓		
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 sufficient to support CCTV images that allow investigation and evidential quality image recording.	✓	✓	✓
1.7.2.	All vehicles and individuals clearly recognizable.	✓		
	Perimeter Alarm Detection			
1.8.	All facility external doors alarmed			
1.8.1.	All facility external warehouse doors alarmed to detect unauthorized opening and linked to main alarm system.	✓	✓	✓
1.8.2.	All exits from warehouse used for emergency purposes only (Fire exits etc) alarmed at all times with an individual or zoned auditable sounder so area can be identified and linked to main alarm system.	✓	✓	
1.8.3.	Each facility external warehouse door or 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.	All windows and any openings (smoke vents, air vents), in warehouse walls alarmed to detect unauthorized opening and linked to main alarm system.	✓	✓	
1.9.3.	Any part of the roof designed to be open (smoke vents, air vents, sky-lights) protected by physical means (bars, mesh or any other material that would harden opening to burglary).	✓		
	or			
1.9.4.	Any other openings in warehouse roof (smoke vents, air vents, sky-lights) alarmed to detect unauthorized opening and linked to main alarm system.	✓		
1.10.	Dock Doors construction			
1.10.1.	All dock doors of sufficient strength so the doors will deter and/or delay forced entry by use of small portable hand tools.	✓	✓	✓
1.11.	Pedestrian doors from warehouse			
1.11.1.	Warehouse pedestrian doors and frames cannot be easily penetrated; if hinges on outside they must be pinned or spot welded.	✓	✓	✓
1.12.	Exterior walls and roof designed and maintained to resist penetration or alarmed			
1.12.1.	Exterior walls and roof designed and maintained to resist penetration (Example: brick, block, tilt up concrete slab, sandwich panel walls).	✓	✓	✓
1.12.2.	Interior floor to ceiling multi-tenant walls and roof constructed/designed and maintained to resist penetration (Example: brick, block, tilt up concrete slab, sandwich panel walls).	✓	✓	✓
	or			
1.12.3.	If Interior floor to ceiling multi-tenant walls are constructed of security grade wire mesh or other industry recognized secure barrier then it is also to be alarmed to detect intrusion. Note: netting, low grade fencing or non-security grade mesh is not allowable.	✓	✓	✓

Annex 1 Facility Security Requirements

	Security requirements and areas of concern.	A	B	C
	Perimeter Windows, And Other Openings			
1.13.	External access to roof secured. N/A if no external roof access			
1.13.1.	External access to roof (ladder or stairs) physically locked and covered by CCTV (Colour or "day/night" cameras).	✓		
1.13.2.	External access to roof (ladder or stairs) physically locked.		✓	✓
1.13.3.	Keys controlled.	✓	✓	✓

Annex 1 Facility Security Requirements

	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; (Colour or "day/night" cameras) individuals clearly recognizable at all times .	✓	✓	
2.1.3.	Duress (panic) alarm installed in covert position in visitor entry point(s) and tested regularly.	✓	✓	
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. (Colour or "day/night" cameras).	✓	✓	

Annex 1 Facility Security Requirements

	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.	Card access or intercom door alarms are locally audible and generate an alarm for response when held open for more than 60 seconds or immediately if forced open.	✓		
3.1.3.	Door alarms are locally audible or send alarm for response when held or forced open.		✓	
	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 reviewed on regular basis to limit/verify that access is only granted to designated/authorized personnel, processes are documented.	✓	✓	

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
	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 (Colour or "day/night" cameras) coverage on cage or vault entrance and internal area.	✓		
3.3.4.	CCTV (Colour or "day/night" cameras) 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.	If access to the HV cage is needed by more than 10 persons then access is to be controlled electronically by card/fob. If access is required by 10 or less persons then a heavy duty lock or padlock system supported by a controlled key issuing system. Keys can be signed out to individuals to cover a shift but must not be transferred without approval and recorded in the key log. All keys to be returned and accounted for when not in use.	✓		
3.3.8.	HV cage doors/gates are alarmed to detect forced entry. Alarms can be generated by door contacts and/or use of CCTV motion detection to detect unauthorized access.	✓		
3.3.9.	Approved access list to HV cage reviewed monthly and updated in real time when employee leaves employment or no longer requires access. LSP to ensure that access is only granted to designated/authorized personnel. Processes are documented.	✓	✓	
3.3.10.	The size and use of HV cages may be dictated by Buyer/LSP agreement. If an agreement is not present then the HV cage must be able to store a minimum of 6 cubic meters of product.	✓	✓	

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
	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).	✓	✓	
3.4.2.	Dock doors secured during non -operational hours (so that doors cannot be opened due to being electronically disabled or physically locked).	✓	✓	
	or			
3.4.3.	Scissor gates secured by mechanical slide/latch locking hardware (minimum height of 8 feet/2.4 meters) or equivalent in place and used on dock doors when not in active use.	✓	✓	
3.4.4.	All external warehouse doors always closed and secured when not in active use.	✓	✓	✓
3.4.5.	Keys/Codes Controlled.	✓	✓	✓
	CCTV Coverage			
3.5.	Internal dock doors and dock areas.			
3.5.1.	All internal dock doors and dock areas covered by CCTV. (Colour or "day/night" cameras).	✓	✓	✓
3.5.2.	Views of freight being loaded/unloaded clear at all times unless temporary obstruction due to operational needs (i.e. truck unloading).	✓	✓	✓
3.6.	Buyer assets under CCTV surveillance			
3.6.1.	Buyer assets under 100% CCTV surveillance in cargo movement or staging areas (i.e. pallet breakdown/build up areas, routes to and from storage racks, dock, transit corridors).	✓	✓	
	Intrusion Detection			
3.7.	Intrusion detection. N/A if risks documented, mitigated in local risk assessment and warehouse activity is true 24x7x366 operation			
3.7.1.	All facility external warehouse doors alarmed to detect unauthorized opening and linked to main alarm system.	✓	✓	✓
3.7.2.	System activated during non-operational hours.	✓	✓	✓
3.7.3.	Intrusion detection alarms installed in office and warehouse to detect intrusions outside non-operational hours.	✓		

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 an internal or 3rd party external 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, securely stored and backed up.	✓		
4.3.3.	Security system alarm records securely stored.		✓	

Annex 1 Facility Security Requirements

	Security requirements and areas of concern.	A	B	C
	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.	✓	✓	

Annex 1 Facility Security Requirements

	Security requirements and areas of concern.	A	B	C
	CCTV Systems			
4.6.	CCTV recording			
4.6.1.	Digital recording in place.	✓	✓	✓
4.6.2.	Digital recording functionality checked daily on operational days via documented procedure. Records available.	✓	✓	✓
4.6.3.	Minimum 3 frames per second per camera.	✓	✓	✓
4.7.	CCTV access			
4.7.1.	Access tightly controlled to CCTV system, including hardware, software, and data/video storage.	✓	✓	✓
4.7.2.	CCTV images, for security purposes, are only viewed by authorized personnel.	✓	✓	✓
4.7.3.	Documented procedures in place detailing CCTV data protection policy regarding use of real time and archive images in accordance with local law.	✓	✓	
4.8.	CCTV recording retention			
4.8.1.	CCTV recordings stored for a minimum of 30 days where allowed by local law. LSP to provide evidence of local law if less than 30 days retention is possible.	✓	✓	✓

Annex 1 Facility Security Requirements

	Security requirements and areas of concern.	A	B	C
	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.	Access system reports reviewed at least quarterly to identify irregularities or misuse (i.e. multiple unsuccessful attempts, false readings (i.e. disabled card), evidence of card sharing to allow unauthorized access, etc.).	✓	✓	
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 emergency contacts.	✓	✓	✓
5.2.	Management commitment			
5.2.1.	The supplier must have a formally appointed person for security on site who is responsible for maintaining TAPA FSR and company supply chain security requirements. The supplier must also have a person (can be the same) responsible for monitoring the FSR programme.	✓	✓	✓
5.2.2.	Management must develop, communicate, and maintain a documented security policy to assure all relevant persons (i.e. employees and contractors) are clearly aware of the provider's security expectations.	✓	✓	✓
5.2.3.	A facility risk assessment which recognizes the likelihood and impact of security related events must be conducted/updated at least annually. The risk assessment process must be documented and require management to make informed decisions that record if mitigation of risk is necessary. At a minimum, the following common internal/external events must be assessed: theft of cargo or information, unauthorized access to facilities or cargo, tampering with/destruction of security systems, fictitious pickups of cargo, security continuity during workforce shortages, or natural disasters, etc. Additional events may be considered based on local/country risks.	✓	✓	✓

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
	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 every 2 years.	✓	✓	✓
5.3.2.	Training is delivered to all members of workforce and includes both general security risks, in addition to any specific 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 recognizable 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, visitors and contractors 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

	Security requirements and areas of concern.	A	B	C
	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.). Copies not made unless allowed by local privacy laws.	✓	✓	✓
5.8.2.	Driver log maintained.	✓	✓	✓
5.8.3.	Where allowed by local law, vehicle identifiers are logged manually (i.e. written) or with cameras. Include at a minimum licence plate, vehicle type and colour.	✓		
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.	Where applicable keys controlled in areas where Buyer's assets are transiting or stored.	✓	✓	✓
5.9.2.	Written plan for control and issue of keys and access cards issued.	✓	✓	
5.10.	Trash inspection from warehouse			
5.10.1	Internal and/or external warehouse main trash collecting bins/ compacting areas are monitored by CCTV.	✓		
5.10.2.	Where utilized trash bags are transparent.		✓	✓

Annex 1 Facility Security Requirements

Transported Asset Protection Association

	Security requirements and areas of concern.	A	B	C
	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 or parking of FTL/dedicated Buyers trucks during non -operational hours, externally of the warehouse facility unless mutually agreed between Buyer and LSP including identification and implementation of any alternative preventative security measures (e.g. additional security devices on container)	✓	✓	✓
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.	If allowed by local law, LSP must develop and maintain a documented exit search or inspection procedure. Activation of the procedure is at the discretion of the LSP and/or as per LSP/Buyer agreement. The procedure as a minimum must contain LSP's right to search criteria should a need arise to introduce searches when they are normally not required (e.g. when workforce pilferage is suspected).	✓		
5.15.	Personal vehicles access			
5.15.1.	Personal vehicles only permitted to shipping and receiving areas if pre-approved and restricted to signed/designated parking areas. No personal parking within 25m walking distance to dock areas.	✓	✓	✓
5.15.2.	Documented procedure.	✓	✓	✓
5.16.	Control of cargo-handling equipment			
5.16.1.	All forklift and other powered cargo-handling equipment disabled 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
	Security Procedures			
5.17.	Container or trailer integrity			
5.17.1.	Seven-point physical inspection process or equivalent checks performed for all outbound dedicated Buyer's 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.	Preventative maintenance conducted once a year, or in accordance with manufacturer's specifications.	✓	✓	✓
5.18.3.	Functionality verifications of all systems once per week and documented, unless system failure is immediately / automatically reported or alarmed.	✓	✓	
5.18.4.	Response-time to initiate/call out for security system is not more than 2 working days.	✓	✓	
5.19.	Contractor Orientation			
5.19.1.	LSP to ensure all subcontractors/vendors are aware of and comply with LSP relevant security programmes	✓		

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 (As allowed by local law, the following requirements apply to all LSPs)			
6.1.1.	The LSP must have a screening / vetting process that includes at a minimum, past employment and criminal history checks. Screening / vetting applies to all applicants, including employees and contractors. The LSP will also require an equivalent process be applied at contracting companies supplying TAS workers.	✓	✓	✓
6.1.2.	TAS (Temp Agency or Subcontracted worker) is required to sign declaration that they have no current criminal convictions and will comply with LSP's security procedures.	✓	✓	✓
6.1.3.	LSP will have agreements in place to have required information supplied by the agency and/or subcontractor providing TAS workers, or shall conduct such screening themselves. Screening must include criminal history check and employment checks.	✓	✓	✓
6.1.4.	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 Handover 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.	LSP must have documented procedures in place for management and control of seals, trailer (container) door locks, pin locks, and other security equipment.	✓	✓	✓
7.1.3.	For Buyer FTL/dedicated truck loads seals affixed and only removed by authorized personnel other than the driver unless Buyer exempts	✓	✓	✓
7.1.4.	Procedures in place for recognizing and reporting compromised seals.	✓	✓	✓
7.2.	Shipping and receiving records			
7.2.1.	Documents legible, complete and accurate (i.e. time, date, signatures, driver, shipping and receiving personnel, shipment details and quantity, etc.).	✓	✓	✓
7.2.2.	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.	The LSP must have documented procedures specifying relevant box and pallet counts before loading and after discharge.	✓	✓	✓
7.4.	Loading unloading validation			
7.4.1.	Robust procedures in place ensuring that all Buyer assets shipped and received are validated at point of handover by conducting a manual and/or electronic piece count. Process must be documented and ensure abnormalities are consistently recognised, documented and reported to the LSP and/or Buyer. Manual and/or electronic records must be of evidential quality. If drivers are not present to witness this activity, LSP/Buyer must ensure alternative count verification such as scans and/or CCTV images, collected and retained specifically for this purpose.	✓	✓	✓

Annex 1 Facility Security Requirements

	Security requirements and areas of concern.	A	B	C
	Freight Handover Process			
7.5.	Pre-alert process in place			
7.5.1.	Where Buyer requires, pre-alert process applied to inbound and/or outbound shipments.	✓	✓	✓
7.5.2.	Where Buyer requires, pre-alert details must be agreed by Buyer and LSP. Suggested details include: departure time, expected arrival time, trucking company, driver name, licence plate details, shipment info (piece count, weight, bill-of-lading number, etc.) and trailer seal numbers.	✓	✓	✓
7.6.	POD (Proof of Delivery)			
7.6.1.	Destination to notify origin within 4 hours of receipt of shipment, reconciling pre-alert shipment details.	✓	✓	✓
7.7.	Fraudulent pick-ups			
7.7.1.	Incoming truck driver ID and collection documentation validated and where Buyer requires process that ensures the details match the pre-alert received.	✓	✓	✓

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

Transported Asset Protection Association