FSR 2023

FACILITY SECURITY REQUIREMENTS

TAPA

Transported Asset Protection Association

Transported Asset Protection Association

Facility Security Requirements
FSR 2023

TAPA Standards

TAPA Americas
5030 Champion Blvd,
G-11 #266 Boca Raton,
Florida 33496
U.S.A.
www.tapaonline.org
Tel. (561) 617-0096

TAPA Asia Pacific
1 Paya Lebar Link, #04-01,
Paya Lebar Quarter,
Singapore 408533
www.tapa-apac.org
Tel. (65) 6514 0892

TAPA EMEA
Pastoor Ohllaan 39
3451 CB Vleuten
The Netherlands
www.tapaemea.org
Tel. +31 19573461

FSR Table of Contents

1. Introduction

1.1 Purpose of this FSR Document

This Facility Security Requirements (FSR) document is the official TAPA Standard for secure warehousing and storage. It is a common global Standard that can be used in business/ security agreements between Buyers and Logistics Service Providers (LSPs) and/or other Applicants seeking Certification.

In the development of this Standard, TAPA recognizes the multiple differences in how storage services are provided globally, regionally, and even within companies, and that the FSR may apply to all or part of the services provided by a LSP/Applicant. Depending on the complexity and size of the supply chain, compliance with TAPA Standards may be achieved through a single LSP/Applicant or multiple LSPs/ Applicants and qualified subcontractors.

Scope

TAPA has developed three options to support certification:

- Single site Certification by Independent Audit Body (IAB).
- Multi-site Certification by IAB.
- Self-audit Certification by Authorized Auditors (AA) by LSP/Applicant or IAB.

Audience

Typical users of the TAPA Standards include:

- Buyers
- LSPs/ Applicants
- Law Enforcement or other government organizations
- Professional Supply Chain Organizations
- Insurers

1. Introduction

1.2 Resources to Implement the TAPA FSR

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

1.3 Protecting LSP Policies and Procedures

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

2. About TAPA

2.1 TAPA's Purpose

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

The threat is no longer only from opportunist criminals. Today, organized crime rings are operating globally and using increasingly sophisticated attacks on vehicles, premises, and personnel to achieve their aims.

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. TAPA's primary focus is theft prevention through the use of real-time intelligence and the latest preventative measures.

2.2 TAPA's Mission

TAPA's mission is to help protect members' assets by minimizing 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.

3. TAPA Standards

3.1 TAPA Security Standards

The following global TAPA Security Standards have been created to ensure secure transportation and storage of high-value theft-targeted cargo:

- The Facility Security Requirements (FSR) represents minimum standards specifically for *secure warehousing, or in-transit storage,* within a supply chain.
- The Trucking Security Requirements (TSR) focuses exclusively on transport by truck and represents minimum standards specifically for *transporting products via road* within a supply chain.

TAPA global Security Standards are reviewed and revised as needed every three years.

This document addresses the FSR requirements only.

- The certification process for TAPA FSR is documented in TAPA FSR Certification Framework document.
- Both the current versions of the TAPA FSR and TAPA FSR Certification Framework document must be followed to achieve TAPA FSR certification status.

3.2 Implementation

Successful implementation of the TAPA Security Standards is dependent upon LSPs (Logistics Service Providers)/ Applicants, Buyers (owners of the cargo), and TAPA Authorized Auditors working together.

4. Legal Guidance

4.1 Scope

The FSR is a Global Standard and all sections of the Standard are mandatory unless an exception is granted through the official waiver process. (See Section 6.).

4.2 Translation

In geographical areas where English is not the first language, and where translation is necessary and applicable, it is the responsibility of the LSP/ Applicant 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.

4.3 The "TAPA" Brand

"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.

4.4 Limits of Liability

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 storage, or any other loss of cargo in storage under the FSR Standards will be for the account of the LSP/ Applicant 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.

5. Contracts and Subcontracting

5.1 Contracts

The safe and secure transportation, storage, and handling of the Buyer's assets is the responsibility of the LSP/ Applicant, its agents and subcontractors throughout the collection, transit, storage, and delivery, as specified in a release or contract.

Where the FSR is referenced or included in the contract between the LSP/Applicant and Buyer, it shall also be referenced in the LSP's/ Applicant's security program.

LSP shall provide Buyer with evidence of FSR Certification and, where appropriate, evidence that FSR requirements have been met. Further, any alleged failure by the LSP/ Applicant to implement the FSR requirements shall be resolved according to the terms of the contract negotiated between the Buyer and the LSP/ Applicant.

5.2 Subcontracting

Subcontractors of storage includes a contractual requirement that the subcontracting LSP/ Applicant meets all noted FSR Standards.

5.3 TAPA Complaint Investigation and Resolution

If TAPA receives a formal complaint concerning the performance of a certified LSP/ Applicant, TAPA (subject to validation) may require that the LSP/Applicant contract for a re-audit at the LSP/ Applicant expense. If the LSP/ Applicant fails the audit, or refuses to comply with this process, their certificate may be withdrawn.

6. Waivers

6. 1 Overview

A waiver is a written approval granted to either exempt a facility from a specific TAPA requirement or to accept an alternative compliance solution. A waiver may be requested if an LSP/ Applicant cannot meet a specific requirement in the FSR and can justify alternative measures. Waivers are valid for the period of the certification.

All waiver requests for a specific security requirement (either in part or whole) must be submitted via a TAPA Waiver Request form to the Independent Audit Body (IAB)/ Authorized Auditor (AA) by the LSP/ Applicant (to be found on the TAPA website). The requesting LSP/ Applicant takes full responsibility for the accuracy of information provided in the waiver request.

Each waiver request must then be submitted through the IAB/AA to the TAPA Regional Waiver Committee for approval. It is the responsibility of the IAB/ AA to decide if the request is complete and justifies processing by TAPA; this includes verification of mitigating factor(s) and/or alternative security controls.

Should TAPA officials and/or Buyers challenge that waiver conditions have changed, TAPA will complete a formal investigation and LSP/ Applicant understands that the waiver may be revoked by TAPA.

6. 2 Waiver Business Process

If an LSP cannot meet a specific requirement in the FSR, the waiver process below is implemented.

Table 1: Responsibilities: Waiver Application / Evaluation

Step	Responsibility	Action
1.	LSP/ Applicant	Establishes and verifies mitigation measures.
2.	LSP/ Applicant	Completes TAPA Waiver Request form and submits to the IAB/ AA.
3.	IAB/ AA	Reviews and verifies integrity of the information contained in the TAPA Waiver Request form.
4.	IAB/ AA	Submits TAPA Waiver Request form to the TAPA Regional Waiver Committee.
5.	TAPA Regional Waiver Committee	Reviews request and either grants or denies the waiver.

6. Waivers

If Waiver Is Denied

If the TAPA Regional Waiver Committee does not approve the waiver request, the LSP/Applicant is required to implement the full security requirements of the FSR.

If Waiver Is Granted

If the TAPA Regional Waiver Committee approves the waiver request, the following actions will be taken:

Table 2: Waiver Approval

Step	Responsibility	Action
1.	TAPA Regional Waiver Committee	Documents and signs the waiver specifics.
2.	TAPA Regional Waiver Committee	Specifies the waiver lifespan (up to a maximum of three years) and sends a copy to the AA.
3.	AA	Notifies the LSP/ Applicant of the outcome of the Waiver Request.
4.	LSP/ Applicant	Complies with the waiver requirements. Failure to do so shall void the waiver approval.

6. 3 Waivers for Physical Barriers (under section 1) and for High Value Cage (HVC, under section 4.5)

TAPA will consider a waiver to all or part of the perimeter barrier requirements and/or for the HVC if all the following preconditions are met:

General:

- The waiver request is submitted using the official TAPA Waiver Request form process and is endorsed by the IAB/ AA.
- The waiver request includes details of any mitigating measures to ensure that vulnerable goods are not at unnecessary risk of theft or loss.
- A risk assessment must be completed and submitted with the waiver request. Any significant vulnerabilities identified in the risk assessment must be separately listed in the waiver and the actions taken to reduce the risk to an acceptable level.

6. Waivers

Mitigation measures to be in place and documented in the waiver request submission:

- **Perimeter barriers:**
  - Additional equipment, resources and procedures introduced to assist in the timely detection of unauthorized persons or vehicles, may include but are not limited to additional lighting, CCTV coverage, enhanced people and vehicle ID enforcement procedures, LSP vest or uniform only restricted areas.
  - Visible perimeter signs must be installed in local language indicating “No unauthorized access”, “No unauthorized parking”.
  - Visible signs on external dock doors or walls are to be installed instructing drivers, visitors etc. to proceed to appropriate lobby, security control.
  - Confirmation that procedures are in place ensuring cargo handling, shipping and receiving yard areas are inspected and compliant with waiver conditions at least weekly.

- **HVC:**
  - For HVC waivers the appropriate mitigation actions to minimize risk (where an HVC is not available) must be considered and documented in the annual Risk Assessment.
  - The waiver request includes an attached declaration signed by the LSP/ Applicant stipulating that no Buyers require an HVC.

7. Facility Security Requirements

Section	General requirements:	A	B	C
7.0				
7.0.1	All procedures or policies required by this Standard must be documented.	✔	✔	✔
7.0.2	Management must have formally appointed a person (AA) for security on site who is responsible for maintaining TAPA FSR, SCARS closure, risk asessment, management report and company supply chain security requirements. Another person (can be the same) will also be responsible for monitoring the FSR program. This includes scheduling compliance checks, communications with AAs, recertification, changes to the FSR Standard, etc. *Note: These persons can be an employee or outsourced person under contract to perform this role.*	✔	✔	✔
7.0.3	Internal audits (by a cross-functional team) on the security management system, self assessment reports by the internal AA and SCARS closure must be completed and documented.	✔	✔	✔
7.0.4	A procedure, log and/or key-plan is required for physical locks, access cards and/or keys that manage and control the physical and electronic keys. The procedure should include processes for duplication, storage, and responding to missing/ lost keys.	✔	✔	✔
7.0.5	A risk assessment that recognizes the likelihood and impact of security related events must be conducted and updated at least annually. Management must acknowledge that the identified risks have been evaluated and appropriate controls have been implemented to mitigate or eliminate the risks to an acceptable level. 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, need for anti-ram barriers for ground level accessible windows or dock doors, etc. Additional events may be considered based on local/country risks.	✔	✔	✔
7.0.6	The person who performs internal or yearly audits for the applicant / LSP (called the LSP AA) must be trained. This person can be the same person as mentioned under 7.6.3 or can be an outsourced person under contract to perform this role.	✔	✔	✔
7.0.7	To understand the FSR and to be capable to implement all its requirements, all applicant/ LSP AAs must have taken and passed the applicable exam for the TAPA Standard and version they are required to audit against.	✔	✔	✔

Section	Perimeter	A	B	C
7.1				
Warehouse External Cargo Handling, Shipping, and Receiving Yard (General)				
7.1.1	CCTV(Closed-Circuit Television)/ VSS (Video Surveillance System) able to view all traffic at external cargo handling, shipping and receiving yard (including entry and exit point(s)) ensuring all vehicles and individuals are recognizable at all times unless temporary obstruction due to operational needs (i.e., truck loading and unloading in real time).	✔	✔	
7.1.2	Lighting adequate in loading and unloading areas. *Note: Lighting may be constant, activated by alarm, motion, sound detection, etc., with immediate illumination provided.*	✔	✔	✔
7.1.3	Procedure describing how unauthorized vehicles and persons are to be managed within the external cargo handling, shipping and receiving yard. Instruction on procedure must be delivered to relevant members of workforce, including guards.	✔	✔	✔
7.1.4	Cargo handling, shipping and receiving yard is adequately controlled to prevent unauthorized access.		✔	✔
7.1.5	For ground level accessible windows or dock doors, the annual Risk Assessment must evaluate the need for anti-ram barriers. Additionally, should include evaluating use of window covers prevent unauthorized viewing of the interior spaces (See Risk Assessment, Section 7.0.5.).	✔		
Physical Barriers				
7.1.6	Physical barrier encloses cargo handling, shipping and receiving yard.	✔		
7.1.7	Physical barrier around the cargo handling, shipping and receiving yard has a minimum height of 6 feet/ 1.8 meters. *Note: The physical barrier, designed to prevent unauthorized access, must be a height of 6 feet/ 1.8 meters along its entire length, including areas where ground level changes, i.e., is lower.*	✔		
7.1.8	Physical barrier around the cargo handling, shipping and receiving yard maintained in good condition.	✔		
7.1.9	Gate(s) within the cargo handling, shipping and receiving yard barriers manned or electronically controlled.	✔		
7.1.10	Physical barrier around cargo handling, shipping and receiving yard is inspected for integrity and damage at least weekly.	✔		
External Dock Areas				
7.1.11	External Dock areas covered via color or “day/night” exterior CCTV/ VSS cameras.	✔	✔	✔
7.1.12	CCTV/ VSS Cameras mounted to be able to view all operations and movement around external dock area at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time).	✔	✔	✔

Section	Perimeter	A	B	C
7.1.13	All vehicles and individuals around external dock areas must be covered by CCTV / VSS cameras. which can clearly show the vehicle identification information and able to discern facial features of personnel. *Note: TAPA will allow existing certification holders without the capability to upgrade to camera resolution, to continue with their current resolution until the 2026 revision. New certificate holders or new sites must meet the new requirement.*	✔		
7.1.14	Vehicles and individuals around external dock areas must be covered and visible by CCTV/ VSS cameras in most cases.		✔	✔
7.1.15	All external areas around dock doors fully illuminated.	✔	✔	✔
Personal Vehicles Access				
7.1.16	Personal vehicles only permitted to cargo handling, shipping and receiving areas if pre-approved and restricted to signed/designated parking areas. No personal parking within 25m walking distance to external dock areas. The processes for the preapproval and restrictions in place.	✔	✔	✔

Section	Outside Walls, Roof, and Doors	A	B	C
7.2				
Exterior Sides of the Facility: CCTV				
7.2.1	Color or "day/night" exterior CCTV/ VSS camera in place covering all exterior sides of the facility.	✔		
7.2.2	Color or "day/night" exterior CCTV/ VSS camera system in place covering exterior sides of facility with doors, windows or other openings.		✔	
7.2.3	All views of exterior CCTV/ VSS camera system clear at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time).	✔		
7.2.4	All vehicles and individuals around exterior sides of the facilities be covered by CCTV/ VSS cameras, which can clearly show the vehicle identification information and able to discern facial features of personnel.	✔		
7.2.5	Vehicles and individuals visible in most cases by the exterior CCTV/ VSS cameras.		✔	
Exterior Walls and Roof				
7.2.6	Exterior walls and roof designed and maintained to resist penetration (Example: brick, block, tilt up concrete slab, sandwich panel walls).	✔	✔	✔
7.2.7	Any openable window, vent or other aperture in the facility exterior walls, or any sealed window installed lower than 3 meters from the working floor in the facility exterior walls, must have a physical barrier **or** be alarmed and linked to the main alarm system.	✔	✔	
7.2.8	Any openable window, skylight, vent, access hatch or other aperture in the facility roof, must have a physical barrier **or** be alarmed and linked to the main alarm system.	✔		

Section	Outside Walls, Roof, and Doors	A	B	C
7.2.9	External access to roof (ladder or stairs) must be: Physically locked and covered by CCTV/ VSS (Color or "day/night" cameras). or Physically locked and alarmed.	✔		
7.2.10	External access to roof (ladder or stairs) physically locked.		✔	✔
7.2.11	All facility external warehouse doors and office doors alarmed to detect unauthorized opening and linked to main alarm system. *Note: Dock doors are not covered by this requirement, see section 7.2.17 for dock door alarm requirements.*	✔	✔	✔
7.2.12	Each facility external warehouse door, office door or other opening must be uniquely identified per door or per zone within main alarm system.	✔		
7.2.13	All external warehouse doors always closed and secured when not in active use. Where applicable Keys/ Codes Controlled.	✔	✔	
7.2.14	Warehouse pedestrian doors and frames cannot be easily penetrated. If hinges on outside they must be pinned or spot-welded. Glass doors are unacceptable unless glass break detectors are fitted, or other local detection device is providing cover (e.g. PIR) and alarmed directly to the monitoring center or glass is protected by bars/ mesh.	✔	✔	✔
7.2.15	Emergency exits that are used for emergency purposes only (Ex: Fire exits), are alarmed at all times with an individual or zoned audible sounder.	✔	✔	
7.2.16	All dock doors of sufficient strength so the doors will deter and/or delay forced entry by use of small portable hand tools.	✔	✔	✔
7.2.17	**Dock Doors** **Non-operational hours:** Dock doors closed, secured (i.e. electronically disabled or physically locked). Dock doors alarmed to detect unauthorized intrusion and generate an alarm linked to the main alarm system. **Operational hours:** Dock doors must be closed when not in active use. Scissor gates, if used, must be secured by mechanical slide/ latch lock and be a minimum of 8 feet/ 2.4 meters high.	✔	✔	✔

Section	Office and Warehouse Entry and Exit Points	A	B	C
7.3				
Office Area Visitor Entry Point(s)				
7.3.1	Visitor entry point(s) are controlled by an employee/ guard/ receptionist that has been trained on badge issuance, controls, logging, visitors, escort requirement, etc. (process in place for visits outside operational hours).	✔	✔	✔
7.3.2	Office area visitor entry point(s) covered by CCTV; (Color or "day/night" cameras) individuals clearly recognizable at all times.	✔	✔	
7.3.3	Duress alarm present in office area visitor entry point(s) and tested weekly.	✔	✔	
7.3.4	All visitors to the office area identified using government-issued photo-ID (e.g. driver's license; passport or national ID card, etc.).	✔	✔	✔
7.3.5	All visitors to the office area registered and log maintained for minimum of 30 days.	✔	✔	✔
7.3.6	All visitor badges must be reconciled as the visitor leaves the premises and the full log checked daily.	✔	✔	
7.3.7	All visitors visibly display badges or passes and are escorted by company personnel.	✔	✔	
Workforce Entry Point(s)				
7.3.8	Workforce entry point(s) access controlled 24/7.		✔	✔
7.3.9	Workforce entry point(s) controlled through electronic access control device 24/7. Access logged.	✔		
7.3.10	Workforce entry point(s) covered by CCTV. (Color or "day/night" cameras).	✔	✔	
7.3.11	After vetting, all employees must be issued with company photo–ID badges.	✔	✔	
7.3.12	All other workforce must be provided with a company ID badge to make them recognizable within the facility.	✔	✔	
7.3.13	All workforce's badges clearly displayed.	✔	✔	
7.3.14	Workforce Badges must not be shared under any circumstances and a badge issuance policy must be in place.	✔	✔	
Driver and vehicle Identification				
7.3.15	All drivers identified using government-issued photo-ID (e.g. driver's license; passport or national ID card, etc.) and a driver log maintained.	✔	✔	✔
7.3.16	Verification that the driver's license is valid, the driver photo-ID has not expired, and matches the driver.	✔	✔	✔
7.3.17	Vehicle identifiers are logged manually (i.e. written) or with cameras. Include at a minimum license plate and vehicle type.	✔		

Section	Inside Warehouse and Office	A	B	C
7.4				
	Warehouse Area: Multi-Tenant Walls			
7.4.1	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).	✔	✔	✔
7.4.2	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 acceptable.*	✔	✔	✔
Internal Warehouse Areas				
7.4.3	Intrusion detection (e.g. infrared, motion, sound, or vibration detection), is required to monitor the internal warehouse areas. The alarms must be activated and linked to the main alarm system during non-operational hours (I.e. when warehouse is closed). *Note: If the warehouse is a true 24/7/366 operation, this requirement may be N/A if the risks and mitigations are documented in the local Risk Assessment.* (*See Section 7.0.5)* *Regardless of operational hours, perimeter intrusion detection or physical barriers are always required on external doors and ground-floor windows in office and warehouse. (See section 7.2.11).*	✔		
Internal Dock Doors and Dock Areas				
7.4.4	All internal dock doors and dock areas covered by CCTV. (Color or "day/night" cameras).	✔	✔	✔
7.4.5	Views of freight being loaded/unloaded at all internal dock doors and dock areas, clear at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time).	✔	✔	✔
7.4.6	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).	✔	✔	
Access Control Between Office and Dock/Warehouse				
7.4.7	Access controlled between office and dock/warehouse.	✔	✔	
7.4.8	Card access or intercom door alarms, for doors between office and dock/ warehouse, are locally audible **and** generate an alarm for response when held open for more than 60 seconds or immediately if forced open.	✔		
7.4.9	Door alarms for doors between office and dock/ warehouse are locally audible **or** send alarm for response when held open for more than 60 seconds or forced open.		✔	
7.4.10	LSP's/ Applicant's authorized workforce and escorted visitors permitted access to dock/warehouse areas based on a business need and restricted.	✔	✔	✔
7.4.11	Access list to dock/ warehouse areas reviewed at least quarterly to limit/verify that access permission is only granted to designated/ authorized personnel.	✔	✔	
High Value Cage (HVC) /Area				

Section	Inside Warehouse and Office	A	B	C
7.4.12	The size and use of HVC may be dictated by Buyer/LSP/ Applicant agreement. If an agreement is not present, then the HVC must be able to store a minimum of 6 cubic meters of product.	✔	✔	
7.4.13	HVC/ Area perimeter caged or hard walled on all sides, including top/roof.	✔	✔	
7.4.14	HVC/ Area locking device on door/gate.	✔	✔	
7.4.15	Complete CCTV/ VSS (Color or "day/night" cameras) coverage on HVC entrance and internal area. *Note: If the HVC is too small to locate a camera inside, camera coverage of the entrance is sufficient.*	✔		
7.4.16	CCTV (Color or "day/night" cameras) coverage on HVC entrance.		✔	
7.4.17	If access to the HVC 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, 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.	✔		
7.4.18	HVC doors/gates are alarmed to detect forced entry. Alarms can be generated by door contacts and/or use of CCTV/ VSS motion detection to detect unauthorized access.	✔		
7.4.19	Perimeter of HVC maintained in good condition and inspected monthly for integrity and damage.	✔		
7.4.20	LSP/ Applicant to ensure that access to the HVC is only granted to designated/authorized personnel. Approved access list to HVC reviewed monthly and updated in real time when employee leaves employment or no longer requires access. Procedure for HVC access in place.	✔	✔	
Trash Inspection from Warehouse				
7.4.21	Internal and/or external warehouse main trash collecting bins/ compacting areas are monitored by CCTV/ VSS.	✔		
7.4.22	Where utilized, trash bags used inside the warehouse are transparent.		✔	✔

Pre-Loading and Staging				
7.4.23	No pre-loading or parking of FTL/ dedicated Buyer's trucks externally of the warehouse facility during non -operational hours, unless mutually agreed between Buyer and LSP/ Applicant. Alternative security measures must be implemented (e.g. additional security devices on container). *Note: "Externally of the warehouse facility" are those areas separate, away from, the facility, but still inside the LSP's/ Applicant's yard/ perimeter fence.*	✔	✔	✔
Personal Containers and Exit Searches				
7.4.24	Written security procedures define how 'personal containers' are controlled inside the warehouse. Personal containers include lunch boxes, backpacks, coolers, purses, etc.	✔	✔	
7.4.25	If allowed by local law, LSP/ Applicant must develop and maintain a documented procedure for exit searches. Activation of the procedure is at the discretion of the LSP/ Applicant and/or as per Buyer/ LSP/ Applicant agreement. At a minimum, the procedure must address the LSP's/ Applicant'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).	✔		
Control of Cargo-Handling Equipment				
7.4.26	Procedure requiring all forklift and other powered cargo-handling equipment being disabled during non-operational hours. *Note: This does not include hand-jacks/ pallet-jacks.*	✔	✔	
Container or Trailer Integrity; 7 points inspection				
7.4.27	7-point physical inspection performed on 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. *Note: This applies to all types of trailers & containers under lock and/or seal (I.e. Not limited to ocean freight containers).*	✔	✔	✔
Freight Handover Process; Security Seals				
7.4.28	Unless specifically exempt by Buyer, tamper evident security seals, are used on all direct, non-stop shipments. Seals shall be certified to ISO 17712 (I, S or H classification). *Note: Seals are not required on multiple stop shipments, due to the complexity and risk associated with drivers carrying multiple seals.*	✔	✔	✔
7.4.29	LSP/Applicant must have documented procedures in place for management and control of security seals, trailer (container) door locks, pin locks, and other security equipment.	✔	✔	✔
7.4.30	Security seals are only affixed or removed by authorized personnel, i.e. warehouse staff, who are instructed to recognize, and report compromised seals. Seals must never be affixed or removed by the driver unless on Buyer exemption.	✔	✔	✔

7.4.31	Procedures in place for recognizing and reporting compromised security seals.	✔	✔	✔
Cargo Integrity; Loading/Unloading Validation Process				
7.4.32	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 ensure abnormalities are consistently recognized, documented and reported to the LSP/ Applicant and/or Buyer. Manual and/or electronic records must be of evidential quality. If drivers are not present to witness this activity, Buyer/ LSP/ Applicant must ensure alternative count verification such as scans and/or CCTV/ VSS images, collected and retained specifically for this purpose. *Note: In addition to missing pieces, abnormalities may include damage, missing straps or tape, cuts, or other obvious openings, indicating a possible theft or pilfering.*	✔	✔	✔
Fraudulent Pick-Ups				
7.4.33	Truck driver ID, cargo pickup documentation, and applicable Buyer-specified pre-alert details are validated prior to loading. Procedure must be in place.	✔	✔	✔

Section	Security Systems; Design, Monitoring and Responses.	A	B	C
7.5				
Monitoring Post				
7.5.1	Monitoring of alarm events 24x7x366 via an internal or 3rd party external monitoring post, protected from unauthorized access. *Note: Monitoring posts may be located on or off site, and can be company owned, or third party. In all cases, access must be controlled through the use of an electronic access control system (badges), locks, or biometric scanners.*	✔	✔	✔
7.5.2	Monitoring post to respond on all security system alarms in real-time 24x7x366.	✔	✔	✔
7.5.3	Monitoring post acknowledges alarm-activation and escalates in less than 3 minutes.	✔	✔	✔
7.5.4	Alarm monitoring reports available.	✔	✔	✔
7.5.5	Monitor post response procedures in place.	✔	✔	✔
Intruder Detection System (IDS)				
7.5.6	All IDS activated during non-operational hours and linked to the main alarm system.	✔	✔	✔
7.5.7	60 days of IDS alarm records maintained.	✔	✔	
7.5.8	IDS alarm records securely stored and backed up.	✔		
7.5.9	IDS alarm records securely stored.		✔	

Section	Security Systems; Design, Monitoring and Responses.	A	B	C
7.5.10	Procedure to ensure IDS access is restricted to authorized individuals or system administrators. This includes servers, consoles, controllers, panels, networks, and data. Access privileges must be promptly updated when individuals depart the organization, or change roles, no longer requiring access.	✔	✔	✔
7.5.11	Alarm transmitted on power failure/ loss of the IDS. *Note: For systems with Uninterrupted Power Supply (UPS), the alarm is transmitted when the UPS battery fails.*	✔	✔	✔
7.5.12	IDS alarm set verification in place. *Note: Procedures validating that alarms are armed during non-operational hours.*	✔	✔	✔
7.5.13	IDS alarm transmitted via fixed line or wireless and/or communications mode failure.	✔	✔	
7.5.14	Back-up communication system in place on IDS device and/or line failure.	✔	✔	
Automatic Access Control System (AACS)				
7.5.15	90 days of AACS transaction records available. Records securely stored; backed up.	✔	✔	
7.5.16	Procedure to ensure AACS access is restricted to authorized individuals or system administrators. Access privileges must be promptly updated when individuals depart the organization, or change roles, no longer requiring access.	✔	✔	
7.5.17	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.). Process in place.	✔	✔	
CCTV				
7.5.18	Digital recording of CCTV/ VSS in place.	✔	✔	✔
7.5.19	Recording speed for CCTV/ VSS is set as a minimum for 8 frames per second (fps) per camera.	✔	✔	✔
7.5.20	Digital recording functionality checked daily on operational days via procedure. Records available.	✔	✔	✔
7.5.21	CCTV/ VSS recordings stored for a minimum of 30 days where allowed by local law. LSP/Applicant must provide evidence of any local laws that prohibit the use of CCTV and/or limit the video data storage to less than 30 days.	✔	✔	✔
7.5.22	Access tightly controlled to CCTV/ VSS system, including hardware, software, and data/video storage. This room must be locked if the CCTV/ VSS storage system is on premise with access controls in place.	✔	✔	✔
7.5.23	CCTV/ VSS images, for security purposes, are only viewed by authorized personnel.	✔	✔	✔

Section	Security Systems; Design, Monitoring and Responses.	A	B	C
7.5.24	Procedures in place detailing CCTV/ VSS data protection policy regarding use of real time and archive images in accordance with local law.	✔	✔	
Exterior and Interior Lighting				
7.5.25	Exterior and interior lighting levels are sufficient to support CCTV images that allow investigation and evidential quality image recording.	✔	✔	
7.5.26	Exterior and interior lighting levels are sufficient to clearly recognize all vehicles and individuals.	✔		

Section	Training and Procedures	A	B	C
7.6				
Escalation Procedures				
7.6.1	Local procedures in place for handling Buyer's assets including process for timely reporting of lost, missing or stolen Buyer's assets. Incidents to be reported by the LSP/ Applicant to the Buyer within 24 hours. Obvious thefts reported immediately. Process consistently followed.	✔	✔	✔
7.6.2	Emergency Buyer and LSP/ Applicant facility management contacts for security incidents listed and available. Listing updated every 6 months and includes law enforcement emergency contacts	✔	✔	✔
Management Commitment				
7.6.3	Management must develop, communicate, and maintain a security policy to ensure all relevant persons (i.e. employees and contractors) are clearly aware of the provider's security expectations.	✔	✔	✔
Training				
7.6.4	Security/ Threat Awareness training to be provided to all members of the work force in the first 60 days of employment and thereafter every 2 years.	✔	✔	✔
7.6.5	Information security awareness training focused on protecting Buyer's electronic and physical shipping data provided to workforce having access to Buyer's information.	✔	✔	✔
Access to Buyer's Assets				
7.6.6	Procedure(s) in place to protect Buyer's assets (i.e. cargo) from unauthorized access by the workforce, visitors, etc.	✔	✔	
Information Control				
7.6.7	Access to shipping documents and information on Buyer's assets controlled based on "need to know".	✔	✔	✔
7.6.8	Access to shipping documents and information on Buyer's assets monitored and recorded.	✔	✔	✔
7.6.9	Shipping Documents and information on Buyer's assets safeguarded until destruction.	✔	✔	✔
Security Incident Reporting				
7.6.10	Security incident reporting and tracking system in place, used to implement proactive measures.	✔	✔	

Section	Training and Procedures	A	B	C
Maintenance Programs				
7.6.11	Maintenance programs in place for all technical (physical) security installations/ systems to ensure functionality at all times (e.g. CCTV/ VSS, Access Controls, Intruder Detection, and Lighting).	✔	✔	✔
7.6.12	Preventative maintenance conducted once a year, or in accordance with manufacturer's specifications.	✔	✔	✔
7.6.13	Functionality verifications of all systems once per week and documented, unless system failure is immediately/ automatically reported or alarmed.	✔	✔	
7.6.14	A repair order must be initiated within 48 hours of when the fault is discovered. For any repairs expected to exceed 24 hours, alternative mitigations must be implemented.	✔	✔	
Contractor Orientation				
7.6.15	LSP/ Applicant to ensure all subcontractors/vendors are aware of and comply with LSP/ Applicant relevant security programs.	✔	✔	✔
Shipping and Receiving Records				
7.6.16	Shipping and Receiving Documents legible, complete and accurate (i.e. time, date, signatures, driver, shipping and receiving personnel, shipment details and quantity, etc.).	✔	✔	✔
7.6.17	LSP/ Applicant must maintain records of all collections and proof of deliveries, for a period of not less than two years, and make them available to loss investigations as necessary.	✔	✔	✔
7.6.18	Proof of delivery must be provided in accordance with written agreement between the Buyer and the LSP/ Applicant, where Buyer requires, destination to notify origin within the agreed timeframe of receipt of shipment, reconciling pre-alert shipment details.	✔	✔	✔
Pre-Alert Process in Place				
7.6.19	Where Buyer requires, pre-alert process applied to inbound and/or outbound shipments is in place. Pre-alert details must be agreed by Buyer and LSP/ Applicant. Suggested details include: departure time, expected arrival time, trucking company, driver name, license plate details, shipment info (piece count, weight, bill-of-lading number, etc.) and trailer seal numbers.	✔	✔	✔

Section	Workforce Integrity	A	B	C
7.7				
7.1	**Screening/ Vetting/ Background Checks (as allowed by local law)**			
7.7.1	The LSP/ Applicant must have a screening/ vetting/ background process that includes at a minimum, past employment and criminal history checks. Screening/ vetting applies to all applicants, including employees and contractors. The LSP/ Applicant will also require an equivalent process be applied at contracting companies supplying TAS workers.	✔	✔	✔

Section	Workforce Integrity	A	B	C
7.7.2	TAS worker is required to sign declaration that they have no current criminal convictions and will comply with LSP's/ Applicant's security procedures.	✔	✔	✔
7.7.3	LSP/ Applicant will have agreements in place to have required screening/ vetting/ background 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.	✔	✔	✔
7.7.4	Procedure for dealing with applicant's/ workforce's false declaration pre & post hiring.	✔	✔	✔
Termination or Rehiring of Workforce *Note: Termination includes both voluntary and involuntary separations—terminated and resigned members of workforce.*				
7.7.5	Recover physical assets from terminated workforce to include company IDs, access badges, keys, equipment, IT assets and sensitive information. Documented procedure required.	✔	✔	✔
7.7.6	Protect Buyer's data: Terminate access for terminated workforce to physical or electronic systems including those that contain Buyer's data (inventory or schedules) Procedure required.	✔	✔	✔
7.7.7	Workforce checklist for onboarding and off boarding in place for verification.	✔	✔	✔
7.7.8	Re-hiring: Procedures are in place to prevent LSP/ Applicant from re-hiring workforce if denial/ termination criteria are still valid. *Note: Records are reviewed prior to re-hiring (Ex: background of previously terminated personnel or – rejected applicants (previously denied employment).*	✔	✔	✔

8. Central Function Requirements (Only applicable for Multi-site certification)

Section	Central Function	A	B	C
8.1	**General**			
8.1.1	There is a central function to manage the security management system for all sites as defined in the scope of the Multi-site certification.	✔	✔	✔
8.1.2	All sites shall have a legal or contractual relationship with the central function.	✔	✔	✔
8.1.3	A single security management system is established to ensure that all its sites within the system are meeting the requirements of the applicable TAPA Security Standard.	✔	✔	✔
8.1.4	The central function and its management system shall be subject to internal audits to ensure continued compliance to TAPA Standards.	✔	✔	✔

Section	Central Function	A	B	C
8.1.5	The central function shall carry out audits of in scope sites to ensure that each site meets the applicable TAPA FSR requirements. The audits must be done with the appropriate TAPA audit templates. All the individual yearly site audits must be completed and must be available to the auditor prior to the certification process.	✔	✔	✔
8.1.6	The central function shall have the authority and rights to require all sites comply to TAPA Security Standards and to implement corrective and preventative actions as needed. *Note: Where applicable this should be set out in the formal agreement between the central function and the sites.*	✔	✔	✔
8.2	**8.2 Policies and Procedures**			
8.2.1	The central function shall maintain documented policies and procedures for its security management systems that are applicable for all its sites.	✔	✔	✔
8.2.2	The central function shall ensure that appropriately policies and procedures are updated, communicated, deployed and implemented by all sites as required.	✔	✔	✔
8.2.3	The policies and procedures shall be maintained and are easily accessible by all sites as required.	✔	✔	✔
8.3	**8.3 Self-Assessment audit report carried out for all sites**			
8.3.1	The central function shall mandate all sites to carry out self-assessment and all self-assessment reports shall be submitted to the central function for records and reviews. Records should be maintained for at least two (2) years.	✔	✔	✔
8.3.2	The central function shall ensure that all SCARs from the self-assessment and audits are appropriately closed to improve its security management systems.	✔	✔	✔
8.3.3	All sites shall submit progress updates and reports on all outstanding SCARs to the central function. The central function shall escalate to the LSP's/ Applicant's management if SCARs are not completed before its due dates. Records should be maintained for at least two (2) years.	✔	✔	✔
8.4	**8.4 Records of inspections, logs (visitor logs, Driver log,), 7-point inspections**			
8.4.1	The central function shall have procedures in place to ensure all sites maintain records of inspections, visitor logs, driver logs and 7-point inspection etc.	✔	✔	✔
8.5	**8.5 Risk Assessments of all the sites**			
8.5.1	The central function shall have procedures in place to ensure that appropriate risk assessments and management are done on all the sites and its records are maintained for at least two (2) years.	✔	✔	✔
8.6	**CCTV and alarm layout of the sites**			
8.6.1	The central function shall have procedures in place that ensures that all sites review and maintain documents on all physical security systems like CCTV and alarm layout.	✔	✔	✔
8.7	**Alarm and Access Control records**			
8.7.1	The central function shall have procedures in place that ensure that all Alarm and Access Control systems are maintained and tested to ensure their operational effectiveness.	✔	✔	✔

Section	Central Function	A	B	C
8.7.2	The central function shall have procedures in place that all sites maintain records of all intrusion detection and access control testing and incidents.	✔	✔	✔
8.8	**Training records**			
8.8.1	The central function shall have procedures in place to ensure that all sites maintain proper training records on security management training of its employees.	✔	✔	✔
8.8.2	The central function shall have procedures in place to ensure all sites maintain security training records of all site personnel. Records should be maintained for at least two (2) years.	✔	✔	✔
8.9	**8.9 Screening/ vetting records**			
8.9.1	The central function shall have procedures in place to ensure that all sites perform the screening and vetting of records at regular intervals to ensure the integrity and effectiveness of the security management systems.	✔	✔	✔
8.9.2	The central function shall have procedures in place to ensure records of reviews including its findings and corrective/ preventive 8.1.6 actions are maintained. Records will be maintained for at least two (2) years.	✔	✔	✔
8.10	**8.10 Management Review to evaluate the self-audits; SCARs raised; any losses, thefts; Risk Assessments.**			
8.10.1	The central function shall, at a minimum conduct regular management review to ensure the compliance, effectiveness and improvement to its security management systems.	✔	✔	✔
8.10.2	The management reviews shall, amongst others, cover effectiveness of self-audits, SCARs closures, risk assessments, incidents and improvement actions.	✔	✔	✔
8.10.3	The central function shall maintain records of all management reviews for at least two (2) years.	✔	✔	✔

9.0. IT and Cyber Security Threat– Enhanced Option

FSR includes optional Cyber Security Threat enhancements that are deemed a higher level of protection and can be used in addition to the modules. This optional enhancement is intended to be selected by the LSP/ Applicant and/or their Buyer as additional requirements for their operational security needs. When this optional enhancement is selected in the pre-certification assessment to be part of the certification audit, all requirements become mandatory.

Section	IT and Cyber Security Threat– Enhanced Option
9.	**Mandatory requirements**
9.1	The LSP/ Applicant must have security policies for IT and cyber threat. The policies can be separate or in a combined document. The policies must explain: - 1. The actions of the LSP/ Applicant to identify and respond to threats. 2. The policies and procedures in place to protect, detect, test, and respond to security events. 3. The methods for the recovery of IT systems and/or data. 4. The communications protocol to Buyers/ Clients to mitigate supply chain impact within 24 hours of knowledge of incident. 5. How the policies are reviewed annually and updated as appropriate.

Section	IT and Cyber Security Threat– Enhanced Option
9.2	The LSP/ Applicant must deliver information awareness training to all employees. This training must: - 1. Cover the roles and responsibilities that computer users have in maintaining security and the associated benefits. 2. Have a system in place that ensures records of persons receiving training are maintained and retained for a minimum of 2 years.
9.3	The LSP/ Applicant must have a written policy in place for ensuring Cyber Security measures are in place with sub-contractors and /or vendors that ensure: 1. LSP's/ Applicant's Cyber Security requirements are communicated to subcontractors and/or vendors and embedded in agreements. 2. Where subcontractors and/or vendors do not recognise or refuse to adopt LSP's/Applicant's Cyber Security requirements, measures are documented and in place that mitigate the risks to the LSP's/ Applicant's Cyber Security requirements and their customers.
9.4	The LSP/ Applicant must have a Power Interruption Mitigation plan (e.g. alternative power supply or backup generator), that ensures power is routed to critical IT systems (identified in the local risk assessment) for a minimum of 48 hours.
9.5	LSP's/ Applicant's Information Systems must have licensed anti-virus and anti-malware software installed. The anti-virus and anti-malware software must contain the latest updates.
9.6	LSP/ Applicant must have appropriate IT Disaster Recovery Plan (DRP) for recovering from compromised system attacks, including but not limited to, all necessary data and software back-up and recovery arrangements.
9.7	LSP's/ Applicant's Information Systems must be backed up. Such backups must be tested regularly, and backup data must be encrypted and transferred to a secondary, off site location.
9.8	LSP/ Applicant must implement a policy for all user accounts to manage and control access to Information Systems by using unique individual identifiers and strong passwords. Procedures in place to ensure: 1. Password compliance audit program in place. 2. An initial unique password must be assigned to each new account at the time of creation. 3. Initial passwords cannot contain the user's name, identification number or otherwise follow a standard pattern based on user information. 4. Passwords will be communicated to users in a secure manner, and only after validating the identity of the user. 5. Users must be required to change passwords on initial login. 6. Passwords must be changed at least every 90 days.

Publishing and copyright information

The TAPA copyright notice displayed in this document indicates when the document was last issued.

Publication history

First published in August 2023

First (Present) edition published in August 2023

This Publicly Available Specification comes into effect on 15th September 2023