FSR2017

FACILITY SECURITY REQUIREMENTS

TAPA
Transported Asset Protection Association

Transported Asset Protection Association

Facility Security Requirements
FSR 2017

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
c/o Global E2C Pte Ltd
1 Gateway Drive, Westgate
Tower #07-01,
Singapore 608531

www.tapa-apac.org
Tel. (65) 6514 9648

TAPA EMEA
Rhijngeesterstraatweg 40D
2341 BV Oegstgeest
The Netherlands

www.tapaemea.org
Tel. +44 1633 251325

FSR Table of Contents

FSR Table of Contents (continued)

◆◆◆

1. Introduction

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

The FSR may apply to the following:

- Any or all storage locations within the global supply chain, depending on risk and/or Buyer or LSP/Applicant requirements
- LSP/Applicant owned or operated facilities
- Buyer-owned or operated facilities

Audience

Typical users of the TAPA Standards include:

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

Glossary

A Glossary containing definitions of terms and acronyms used throughout this FSR appears in Appendix A.

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.

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

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.

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.

TAPA Contact Information

TAPA consists of three regions (Americas, Asia Pacific, and EMEA) to provide service to all its global members. For more information, please go to:

- TAPA Global:
  www.tapa-international.org
- Americas:
  www.tapaonline.org
- Asia Pacific:
  www.tapa-apac.org
- EMEA
  www.tapaemea.org

3. TAPA Standards

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 only and explains TAPA FSR Certification in Section 6.

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

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 8.)

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.

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.

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

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.

Subcontracting

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

6. TAPA FSR Certification/Re-Certification

FSR Classification Levels

Facilities are classified into one of three FSR Classification Levels, based on the level of protection needed:

- Level A = highest security protection
- Level B = mid-level security protection
- Level C = lowest security protection

LSPs/Applicants or Buyers may initially achieve certification at Level C, and then progress up to Level B or A, as improvements are made. Additionally, as negotiated between Buyer and LSP/Applicant, facilities located in high-risk countries may be classified at Level A, while all other countries are classified at Level B or C. In all cases, it is the responsibility of the Buyer to negotiate the Classification Level directly with the LSP/Applicant, depending on their specific cargo and risks.

A LSP/Applicant or Buyer may request re-certification if either party considers the Classification Level to have changed.

FSR Certification Options

To provide additional flexibility and encourage TAPA certifications, TAPA has developed 2 options to support certification.

Table 1

Option	Description	Level	Auditor Type*
IAB Certified	LSP/Applicant is certified via traditional process.	A, B, or C	TAPA IAB AA
Self-Certified	LSP/Applicant warehouse is self-certified.	C	LSP/Applicant AA

*See Glossary Definitions: Authorized Auditor (AA)

These options are described in more detail below.

IAB Certification (Levels A, B, or C)

The IAB will advise TAPA of the audit scope and results. If the audit is completed successfully, the IAB issues a certificate indicating the LSP/Applicant is now TAPA FSR Certified.

The level of certification (Level A, B, or C) will be specified on the certificate.

Self-Certification (Level C Only)

Level C Self-Certifications must be performed by an Authorized Auditor (AA). An AA can be an internal employee / associate, trained and authorized by TAPA as a FSR AA. Regardless of which type of auditor is used to conduct the Self-Certification, the completed Audit Form must be submitted to TAPA to receive the FSR Level C certification.

General Information

The LSP/Applicant shall ensure the appropriate auditor, trained/qualified on the current FSR, is engaged to complete the audit and certification process. See Table 1 for options.

Before the certification audit is scheduled/commences, LSPs/Applicants must inform the AA which Classification Level they are seeking in their certification process.

The audit tool is the current FSR Audit Form.

TAPA FSR certifications are site/facility specific. If the TAPA FSR audit requirements are all met, the LSP/Applicant shall be deemed to have passed the audit and will be certified for that specific facility location.

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

Costs for TAPA certification are the responsibility of the LSP/Applicant, unless otherwise negotiated with the Buyer(s).

FSR Re-Certification

The TAPA FSR certificate shall be valid for a period of three (3) years with no extension permitted.

To prevent any lapse in certification, a re-certification audit must be performed prior to the expiration date of the current certificate. Completion of any SCARs must also occur within the original 60-day allotted period and prior to the current certificate's expiration date (see Corrective Action / SCAR in Section 7).

Therefore, to assure adequate planning and preparation, it is recommended that the LSP/Applicant schedule the re-certification audit three (3) months before the current certificate expiration date. If the TAPA FSR certificate is issued within the aforementioned three-month period, the date of the new certificate will be the expiration date of the current certification. If corrective actions are not closed prior to the expiration date, and there is no waiver granted, the certification will expire.

A LSP/Applicant or Buyer may request re-certification if either party considers the Classification Level to have changed.

7. Audit Follow Up

Corrective Action / SCAR

If FSR requirements are not met, as discovered during the audit, the AA submits a Security Corrective Action Requirement (SCAR) to the relevant LSP/Applicant. The LSP/Applicant shall respond to the AA within ten (10) business days, documenting the action to be taken and the date the action will be completed. SCAR completion dates may be negotiated between the AA and the LSP/Applicant. However, unless the Regional TAPA Waiver Committee approves a waiver, corrective action implementation shall not exceed sixty (60) days from notification to the LSP/Applicant.

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

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

Compliance Monitoring

Self-Audits

The LSP/Applicant will ensure they have an internal process in place in order to monitor compliance, in years two and three, in between formal audits conducted by an AA.

The interim Self-Audits must reflect the FSR requirements.

- For TAPA FSR certifications issued by an IAB: The interim Self-Audit must be documented on the TAPA Audit Form and submitted to the **IAB** within 30 days of the anniversary date of the original certification.
- For Self-Certifications: The interim Self-Audit must be documented on the TAPA Audit Form and submitted to **TAPA** within 30 days of the anniversary date of the original Self-Certification.

Failure to comply will result in suspension of the original certification until the interim Self-Audit is properly completed. Gaps identified must be documented, assigned a due date for completion of corrective action(s), and tracked to closure within 60 days.

Table 2: Audit & Compliance Monitoring Schedule

Action	Frequency	A	B	C
Certification Audit (IAB/AA Certification Audit)	Every three (3) years	✔	✔	✔
LSP/Applicant Self-Certification Audit	Every three (3) years			✔
Self-Audits (interim compliance checks)	Annually at 1st and 2nd Anniversary	✔	✔	✔
LSP/Applicant Subcontractor Audit	In accordance with Buyer-LSP/Applicant contract	✔	✔	✔

Buyer Visits to LSP/Applicant

The Buyer and the LSP/Applicant recognize the importance of working in partnership to reduce risk within the supply chain. Both parties agree to schedule Buyer visits with reasonable notice; e.g., 10 business days, with scope and parameters mutually-agreed upon in advance and/or in accordance with the Buyer- LSP/Applicant contract. Loss investigations; i.e., thefts, damage, etc., shall be performed in accordance with the Buyer-LSP/Applicant contract.

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.

8. Waivers

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 (see Appendix B: TAPA Waiver Request form). 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

Waiver Business Process

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

Table 3: 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. (See Appendix B.)
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.

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 4: 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.

Waivers for High Value Cages (HVC)

TAPA will consider a waiver to all or part of the HVC requirements if all of the following preconditions are met:

- The waiver request is submitted using the official TAPA Waiver Request form and is endorsed by the IAB/AA.
- The waiver request includes an attached declaration signed by the LSP/Applicant stipulating that no Buyers require an HVC.
- The waiver request includes details of any mitigating measures to ensure that vulnerable goods are not at unnecessary risk of theft or loss.
- Appropriate mitigation actions to minimize risk (where an HVC is not available) are considered and documented in the annual Risk Assessment. Note: TAPA may request to review the Risk Assessment.

9. Facility Security Requirements

Section		A	B	C
1	**Perimeter**			
1.1	Warehouse External Cargo Handling, Shipping, and Receiving Yard (General)			
	CCTV			
1.1.1	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 loading and unloading in real time).	✔	✔	
	Lighting			
1.1.2	Lighting adequate in loading and unloading areas. *Note: Lighting may be constant, activated by alarm, motion, sound detection, etc., with immediate illumination provided.*	✔	✔	✔
	Procedures			
1.1.3	Procedure documented describing how unauthorized vehicles and persons are to be managed. Instruction on procedure must be delivered to relevant members of workforce, including guards	✔	✔	✔
1.1.4	Cargo handling and receiving yard is adequately controlled to prevent unauthorized access		✔	✔
1.1.5	For ground level accessible windows or dock doors, the annual Risk Assessment must evaluate the need for anti-ram barriers. (See Risk Assessment, Section 6.2.3.)	✔		
1.2	Option 1: Physical Barriers in Place			
	Physical Security			
1.2.1	Physical barrier encloses cargo handling, shipping and receiving yard.	✔		
1.2.2	Physical barrier height is a minimum 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.*	✔		
1.2.3	Physical barrier maintained in good condition.	✔		
1.2.4	Gate(s) manned or electronically controlled.	✔		
	Procedures			
1.2.5	Physical barrier is inspected for integrity and damage at least weekly.	✔		
1.3	Option 2: No Physical Barriers in Place			
	Physical Security			
1.3.1	Visible perimeter signs in local language indicating “No unauthorized access”, “No unauthorized parking”.	✔		

Facility Security Requirements

Section		A	B	C
1.3.2	Visible signs on external dock doors or walls instructing drivers, visitors etc. to proceed to appropriate lobby, security control.	✔		
	Procedures			
1.3.3	Documented procedure requiring periodic sweeps/patrols by CCTV and/or guards and/or responsible member of the workforce.	✔		
1.4	External Dock Areas			
	CCTV			
1.4.1	Dock areas covered via color or “day/night” exterior cameras.	✔	✔	✔
	CCTV Performance			
1.4.2	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).	✔	✔	✔
1.4.3	All vehicles and individuals clearly recognizable.	✔		
1.4.4	Vehicles and individuals visible in most cases.		✔	✔
	Dock Door Lighting			
1.4.5	All dock doors fully illuminated.	✔	✔	✔
1.5	Personal Vehicles Access			
	Procedures			
1.5.1	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. The processes for the preapproval and restrictions to be documented	✔	✔	✔

Section		A	B	C
2	**Outside Walls, Roof, and Doors**			
2.1	Exterior Sides of the Facility: CCTV			
	CCTV			
2.1.1	Color or “day/night” exterior camera system in place covering all exterior sides of the facility.	✔		
2.1.2	Color or “day/night” exterior camera system in place covering exterior sides of facility with doors, windows or other openings.		✔	
	CCTV Performance			
2.1.3	All vehicles and individuals clearly recognizable.	✔		
2.1.4	Vehicles and individuals visible in most cases.		✔	
2.1.5	All views clear at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time)	✔	✔	
2.2	Exterior Walls and Roof			
	Physical Security			
2.2.1	Exterior walls and roof designed and maintained to resist penetration (Example: brick, block, tilt up concrete slab, sandwich panel walls).	✔	✔	✔
	Wall Physical Barrier or Intrusion Detection			

Facility Security Requirements

Section		A	B	C
2.2.2	Any open-able window, vent or other aperture must have a physical barrier **or** be alarmed and linked to the main alarm system.	✔	✔	
	Roof Physical Barrier or Intrusion Detection			
2.2.3	Any open-able window, skylight, vent, access hatch or other aperture must have a physical barrier **or** be alarmed and linked to the main alarm system.	✔		
	External Access to Roof			
2.2.4	External access to roof (ladder or stairs) physically locked and covered by CCTV (Color or "day/night" cameras) or alarmed.	✔		
2.2.5	External access to roof (ladder or stairs) physically locked.		✔	✔
	External Doors			
2.2.6	All facility external warehouse and office doors alarmed to detect unauthorized opening and linked to main alarm system.	✔	✔	✔
2.2.7	Each facility external warehouse or office door or opening can be uniquely identified per door or per zone within main alarm system.	✔		
2.2.8	All external warehouse (dock) doors always closed and secured when not in active use. Keys/Codes Controlled.	✔	✔	
	Warehouse Pedestrian Doors			
2.2.9	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) or glass is protected by bars/mesh and alarmed directly to the monitoring center	✔	✔	✔
	Emergency Exits			
2.2.10	Emergency exits that are used for emergency purposes only (Ex: Fire exits), and are alarmed at all times with an individual or zoned audible sounder, and identified / linked to main alarm system.	✔	✔	
	Dock Doors			
2.2.11	All dock doors of sufficient strength so the doors will deter and/or delay forced entry by use of small portable hand tools.	✔	✔	✔
2.2.12	**Non-operational hours:** Dock doors closed, secured (i.e. electronically disabled or physically locked). **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.	✔	✔	

Facility Security Requirements

Section		A	B	C
3	**Office and Warehouse Entry and Exit Points**			
3.1	Office Area Visitor Entry Point(s)			
	Access Controls			
3.1.1	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 in place for visits outside operational hours).	✔	✔	✔
	CCTV			
3.1.2	Visitor entry point(s) covered by CCTV; (Color or "day/night" cameras) individuals clearly recognizable at all times.	✔	✔	
	Alarms			
3.1.3	Duress (panic) alarm installed in covert position in visitor entry point(s) and tested weekly.	✔	✔	
	Procedures			
3.1.4	All visitors identified using government-issued photo-ID (e.g. driver's license; passport or national ID card, etc.).	✔	✔	✔
3.1.5	All visitors registered and log maintained for minimum of 30 days.	✔	✔	✔
3.1.6	All visitor badges must be reconciled as the visitor leaves the premises and the full log checked daily.	✔	✔	
3.1.7	All visitors visibly display badges or passes and are escorted by company personnel	✔	✔	
3.1.8	Visitor policy documented.	✔	✔	
3.2	Workforce Entry Point(s)			
	Access Controls			
3.2.1	Workforce entry point(s) access controlled 24/7.		✔	✔
3.2.2	Workforce entry point(s) controlled through electronic access control device 24/7. Access logged.	✔		
	CCTV			
3.2.3	Workforce entry point(s) covered by CCTV. (Color or "day/night" cameras).	✔	✔	
	Procedures			
3.2.4	After vetting, all employees must be issued with company photo–ID badges.	✔	✔	
3.2.5	All other workforce must be provided with a company ID badge to make them recognizable within the facility.	✔	✔	
3.2.6	All workforce's badges clearly displayed.	✔	✔	
3.2.7	Badges must not be shared under any circumstances and a badge issuance policy must be documented	✔	✔	

Facility Security Requirements

Section		A	B	C
3.3	Driver Identification			
	Procedures			
3.3.1	All drivers identified using government-issued photo-ID (e.g. driver's license; passport or national ID card, etc.) and a driver log maintained	✔	✔	✔
3.3.2	Vehicle identifiers are logged manually (i.e. written) or with cameras. Include at a minimum license plate and vehicle type.	✔		
3.3.3	Verification that photo-ID is not expired, matches the driver, and license appears valid.	✔		

Section		A	B	C
4	**Inside Warehouse and Office**			
4.1	Warehouse Area: Multi-Tenant Walls			
	Option 1: Physical Security			
4.1.1	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)	✔	✔	✔
	Option 2: Security System			
4.1.2	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.*	✔	✔	✔
4.2	Internal Warehouse Areas			
	Intrusion Detection			
4.2.1	Intrusion detection (e.g. infrared, motion, sound, or vibration detection), is required to monitor the internal warehouse space. 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.* *Regardless of operational hours, perimeter intrusion detection or physical barriers are required on external doors and ground-floor windows in office and warehouse. (See section 2.2.).*	✔		
4.3	Internal Dock Doors and Dock Areas			
	CCTV Coverage			
4.3.1	All internal dock doors and dock areas covered by CCTV. (Color or "day/night" cameras).	✔	✔	✔
4.3.2	Views of freight being loaded/unloaded clear at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time).	✔	✔	✔
4.3.3	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). .	✔	✔	

Facility Security Requirements

Section		A	B	C
4.4	Access Control Between Office and Dock/Warehouse			
	Access Controls			
4.4.1	Access controlled between office and warehouse or dock.	✔	✔	
4.4.2	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.	✔		
	Alarms			
4.4.3	Door alarms are locally audible **or** send alarm for response when held or forced open.		✔	
	Procedures			
4.4.4	LSP's/Applicant's authorized workforce and escorted visitors permitted access to dock/warehouse areas based on a business need and restricted.	✔	✔	✔
4.4.5	Access list reviewed at least quarterly to limit/verify that access permission is only granted to designated/ authorized personnel, processes are documented.	✔	✔	
4.5	High Value Cage/Area			
	Physical Security			
4.5.1	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.	✔	✔	
4.5.2	Perimeter caged or hard-walled on all sides, including top/roof.	✔	✔	
4.5.3	Locking device on door/gate	✔	✔	
	CCTV			
4.5.4	Complete CCTV (Color or "day/night" cameras) coverage on cage or vault entrance and internal area. *Note: If the cage / vault is too small to locate a camera inside, camera coverage of the entrance is sufficient.*	✔		
4.5.5	CCTV (Color or "day/night" cameras) coverage on cage or vault entrance.		✔	
	Access Controls			
4.5.6	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, 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.	✔		
	Intrusion Detection			
4.5.7	HVC 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.	✔		
	Procedures			
4.5.8	Perimeter of cage/vault maintained in good condition and inspected monthly for integrity and damage.	✔		

Facility Security Requirements

Section		A	B	C
4.5.9	LSP/Applicant to ensure that access 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. Processes are documented.	✔	✔	
4.6	Keys Control Buyer Assets			
	Procedures			
4.6.1	Where applicable, keys controlled in areas where Buyer's assets are transiting or stored.	✔	✔	✔
4.6.2	Written plan for control and issue of keys and access cards issued.	✔	✔	
4.7	Trash Inspection from Warehouse			
	CCTV			
4.7.1	Internal and/or external warehouse main trash collecting bins/ compacting areas are monitored by CCTV.	✔		
	Procedures			
4.7.2	Where utilized, trash bags are transparent.		✔	✔
4.8	Pre-Loading and Staging			
	Procedures			
4.8.1	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/Applicants yard / perimeter fence.*	✔	✔	✔
4.9	Personal Containers and Exit Searches			
	Procedures			
4.9.1	Written security procedures define how 'personal containers' are controlled inside the warehouse. Personal containers include lunch boxes, backpacks, coolers, purses, etc.	✔	✔	
4.9.2	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)	✔		

Facility Security Requirements

Section		A	B	C
4.10	Control of Cargo-Handling Equipment			
	Procedures			
4.10.1	Documented 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.*	✔	✔	
4.11	Container or Trailer Integrity			
	Procedures			
4.11.1	Seven-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. Procedure documented. *Note: This applies to all types of trailers & containers under lock and/or seal (I.e. Not limited to ocean freight containers).*	✔	✔	✔
4.12	Freight Handover Process; Security Seals			
	Procedures			
4.12.1	Unless specifically exempted by Buyer, tamper evident 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*	✔	✔	✔
4.12.2	LSP/Applicant must have documented procedures in place for management and control of seals, trailer (container) door locks, pin locks, and other security equipment.	✔	✔	✔
4.12.3	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.	✔	✔	✔
4.12.4	Procedures in place for recognizing and reporting compromised seals.	✔	✔	✔
4.13	Cargo Integrity; Loading/Unloading Validation Process			
	Procedures			
4.13.1	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/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 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.*	✔	✔	✔
4.14	Fraudulent Pick-Ups			
	Procedures			
4.14.1	Truck driver ID, cargo pickup documentation, and applicable Buyer-specified pre-alert details are validated prior to loading.	✔	✔	✔

Facility Security Requirements

Section		A	B	C
5	**Security Systems; Design, Monitoring and Responses.**			
5.1	Monitoring Post			
	Physical Security			
5.1.1	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.*	✔	✔	✔
	Alarms Response			
5.1.2	All security system alarms responded to in real-time 24x7x366.	✔	✔	✔
5.1.3	Monitoring post acknowledges alarm-activation and escalates in less than 3 minutes.	✔	✔	✔
	Procedures			
5.1.4	Alarm monitoring reports available.	✔	✔	✔
5.1.5	Documented response procedures.	✔	✔	✔
5.2	Intruder Alarm System			
	Procedures			
5.2.1	All systems activated during non-operational hours and linked to the main alarm system	✔	✔	✔
5.2.2	60 days of security system alarm records maintained.	✔	✔	
5.2.3	Security system alarm records, securely stored and backed up.	✔		
5.2.4.	Security system alarm records securely stored.		✔	
5.2.5	Documented procedure to ensure security system 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.	✔	✔	✔
	Alarms Transmitted and Monitored			
5.2.6	Alarm transmitted on power failure/loss. *Note: For systems with Uninterrupted Power Supply (UPS), the alarm is transmitted when the UPS battery fails.*	✔	✔	✔
5.2.7	Alarm set verification in place. *Note: Documented procedures validating that alarms are armed during non-operational hours.*	✔	✔	✔
5.2.8	Alarm transmitted on device and/or line failure.	✔	✔	
5.2.9	Back-up communication system in place on device and/or line failure.	✔	✔	

Facility Security Requirements

Section		A	B	C
5.3	Electronic Access Control system			
	Access Recording Retention			
5.3.1	90 days of system transaction records available. Records securely stored; backed up.	✔	✔	
	Access Restriction			
5.3.2	Documented procedure to ensure system 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.	✔	✔	
	Review of Access Reports			
5.3.3	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.). Documented process in place.	✔	✔	
5.4	CCTV			
	Physical			
5.4.1	Digital recording in place.	✔	✔	✔
5.4.2	Minimum 3 frames per second per camera.	✔	✔	✔
	CCTV Procedures			
5.4.3	Digital recording functionality checked daily on operational days via documented procedure. Records available.	✔	✔	✔
5.4.4	CCTV 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.	✔	✔	✔
5.4.5	Access tightly controlled to CCTV system, including hardware, software, and data/video storage.	✔	✔	✔
5.4.6	CCTV images, for security purposes, are only viewed by authorized personnel.	✔	✔	✔
5.4.7	Documented procedures in place detailing CCTV data protection policy regarding use of real time and archive images in accordance with local law	✔	✔	
5.5	Exterior and Interior Lighting			
	Procedures			
5.5.1	Exterior and interior lighting levels are sufficient to support CCTV images that allow investigation and evidential quality image recording	✔	✔	✔
5.5.2	All vehicles and individuals clearly recognizable	✔		

Facility Security Requirements

Section		A	B	C
6	**Training and Procedures**			
6.1	Escalation Procedures			
	Procedures			
6.1.1	Local documented 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	✔	✔	✔
6.1.2	Emergency Buyer and LSP/Applicant facility management contacts for security incidents listed and available. Listing updated at 6 monthly intervals and includes law enforcement emergency contacts	✔	✔	✔
6.2	Management Commitment			
	Procedures			
6.2.1	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 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*	✔	✔	✔
6.2.2	Management must develop, communicate, and maintain a documented security policy to ensure all relevant persons (i.e. employees and contractors) are clearly aware of the provider's security expectations.	✔	✔	✔
6.2.3	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 about vulnerabilities and mitigation. 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.	✔	✔	✔
6.3	Training			
	Training			
6.3.1	Security / Threat Awareness training provided every 2 years to all members of the work force that includes both general, and any specific / unique local risks.	✔	✔	✔
6.3.2	Information security awareness training focused on protecting Buyer's electronic and physical shipping data provided to workforce having access to Buyer's information	✔	✔	
6.4	Access to Buyer's Assets			
	Procedures			
6.4.1	Documented procedure(s) in place to protect Buyer's assets (i.e. cargo) from unauthorized access by the workforce, visitors, etc.	✔	✔	

Facility Security Requirements

Section		A	B	C
6.5	Information Control			
	Procedures			
6.5.1	Access to shipping documents and information on Buyer's assets controlled based on "need to know."	✔	✔	✔
6.5.2	Access monitored and recorded.	✔	✔	✔
6.5.3	Documents safeguarded until destruction.	✔	✔	✔
6.6	Security Incident Reporting			
	Procedures			
6.6.1	Security incident reporting and tracking system in place, used to implement proactive measures.	✔	✔	
6.7	Maintenance Programs			
	Procedures			
6.7.1	Documented maintenance programs in place for all technical (physical) security installations/systems to ensure functionality at all times (e.g. CCTV, Access Controls, Intruder Detection, and Lighting).	✔	✔	✔
6.7.2	Preventative maintenance conducted once a year, or in accordance with manufacturer's specifications.	✔	✔	✔
6.7.3	Functionality verifications of all systems once per week and documented, unless system failure is immediately / automatically reported or alarmed.	✔	✔	
6.7.4	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.	✔	✔	
6.8	Contractor Orientation			
	Procedures			
6.8.1	LSP/Applicant to ensure all subcontractors/vendors are aware of and comply with LSP/Applicant relevant security programs	✔		
6.9	Shipping and Receiving Records			
	Procedures			
6.9.1	Documents legible, complete and accurate (i.e. time, date, signatures, driver, shipping and receiving personnel, shipment details and quantity, etc.).	✔	✔	✔
6.9.2	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.	✔	✔	✔
6.9.3	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	✔	✔	✔

Facility Security Requirements

Section		A	B	C
6.10	Pre-Alert Process in Place			
	Procedures			
6.10.1	Where Buyer requires, pre-alert process applied to inbound and/or outbound shipments. 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	✔	✔	✔
6.11	General procedures			
	General			
6.11.1	Wherever procedures are required, they must be documented	✔	✔	✔
	Locks and Keys			
6.11.2	Wherever physical locks and/or keys are required, there must be a documented procedure, log and/or key plan to track how keys are managed and controlled.	✔	✔	✔

Section		A	B	C
7	**Workforce Integrity**			
7.1	Screening/Vetting/Background Checks (as allowed by local law)			
	Procedures			
7.1.1	The LSP/Applicant 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/Applicant will also require an equivalent process be applied at contracting companies supplying TAS workers.	✔	✔	✔
7.1.2	TAS worker is required to sign declaration that they have no current criminal convictions and will comply with LSP's/Applicant's security procedures.	✔	✔	✔
7.1.3	LSP/Applicant 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.	✔	✔	✔
7.1.4	Procedure for dealing with applicants/workforce's false declaration pre & post hiring.	✔	✔	✔
7.2	Termination or Rehiring of Workforce *Note: Termination includes both voluntary and involuntary separations—terminated and resigned members of workforce.*			
	Procedures			
7.2.1	Recover physical assets from terminated workforce to include company IDs, access badges, keys, equipment, or sensitive information. Documented procedure required.	✔	✔	✔
7.2.2	Protect Buyer's data: Terminate access to physical or electronic systems that contain Buyer's data (inventory or schedules). Documented procedure required.	✔	✔	✔
7.2.3	Workforce checklist in place for verification	✔	✔	✔

Facility Security Requirements

Section		A	B	C
7.2.4	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).*	✔	✔	✔

Appendix A: FSR Glossary

Term	Acronym (if applicable)	Definition
Adequately		In a satisfactory manner, so no or very minimal gaps exist in local procedures.
Authorized Auditor	AA	An Auditor working for an **IAB** who has passed TAPA-administered training and is authorized to conduct audits and issue certifications with TAPA Standards at all levels (FSR A, B, C and TSR 1, 2, 3) **OR** An Auditor working for an **LSP/Applicant or Buyer** who has passed TAPA-administered training and is authorized to issue **Self-Certifications** for FSR Level C or TSR Level 3 only.
Applicant		Entity seeking TAPA certification. While applicants are typically Logistics Service Providers (LSP), they can also be Buyers seeking certification for their own warehouses or trucking fleets.
Backed Up		To have made a copy of a data file or document which is stored securely in a separate location accessible to security staff for investigative purposes.
Black Spots		These are areas where tracking technology does not work or where latency (delay in reporting) exceeds one hour. Different tracking technologies may exhibit different "black spots" within their coverage maps.
Buyer		Purchaser of services and/or owner of transported and/or stored goods.
Buyer Exemption		Where "unless on Buyer exemption" is specified within a requirement, this can be a justifiable reason to record an N/A result or used to support a waiver request. The LSP/Applicant must have evidence supporting Buyer exemption finding such as documented approval from all Buyers. This evidence must be referenced in the audit and shared with the AA to allow them to validate the N/A result or in support of a waiver request.
Closed-Circuit Television	CCTV	An internal or external color or "day/night" camera video surveillance system. Signals are transmitted to monitors, recording and control equipment.
Curtain-Sided Trailers		These include trailers whose sides are constructed of fabric, either reinforced (anti-slash) or not, which are intended to be rolled up for loading/unloading operations.
Days		Unless otherwise defined in the requirement(s), "days" is defined as "calendar days" and include weekends and holidays.
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.
Facility Security Requirements	FSR	TAPA Standard that describes the security requirements for warehouse operations.
Findings(s)		Observation(s) of non-compliance with a TAPA Standard requirement. Note: All findings will be documented in a SCAR.

Term	Acronym (if applicable)	Definition
Freight		Goods, cargo, or merchandise being transported or stored.
Full Container Load	FCL	Indicates that the cargo is dedicated for one Buyer.
Full Truckload	FTL	Indicates that the cargo is dedicated for one Buyer.
Hard-Sided Trailers		Includes trailers whose sides, floor, and top are constructed of metal or other solid material.
High Value Theft-Targeted	HVTT	Cargo that is at an elevated risk for theft.
Identifiable		To be able to identify or establish as being a particular person or object.
Independent Audit Body	IAB	An audit company approved by TAPA and contracted by the LSP/Applicant or Buyer seeking TAPA Certification.
Intrusion Detection		A system (i.e., devices and software) that records information related to observed events, notifies security monitoring stations, and produces reports. Example technologies include motion, sound, sonar, microwave, and infrared.
Key Controls		Restricts access to keys by using a key register and key plan that is fully documented and part of the training program.
Less Than Load	LTL	Usually refers to a consolidated load that may be in a truck or container and may contain cargo for multiple Buyers.
Logistics Service Provider	LSP	A forwarder, a carrier, a trucking company, a warehouse operator, or any other company that provides direct services handling freight within the supply chain.
Memorandum of Understanding	MOU	A written agreement between the Independent Audit Bodies and TAPA that specifies the procedures the audit body shall follow to support the certification. A MOU expires 3 years from its inception.
Not Applicable	N/A	A condition that in certain circumstances can be accepted by the Authorized Auditor when conducting TAPA certification audits. N/A can only be considered when the TAPA requirement response of "Yes or No" is truly not appropriate and/or the requirement is not capable of being applied. N/A cannot be used to avoid compliance due to cost or operational concerns. N/A(s) entered into the certification audit template, must contain, or refer to, documented supporting details that describe and justify the N/A decision. Examples of where N/A could be utilized: - • Protection of doors, windows, or other openings, that do not exist. • Securing of roof ladders that are not required to be installed at that facility (I.e. no external ladders present at the facility). • Warehouse is a true 24/7/366 operation such that intrusion detection in the interior spaces is not applicable. • Requiring subcontractors to comply with TAPA Standards, when the LSP/Applicant does not use subcontractors. *Note: Use of N/A is not the same as a waiver. Waivers are considered when an applicable requirement cannot be complied with and risks are adequately mitigated with alternative technical or process controls.*

Term	Acronym (if applicable)	Definition
Physical Barrier		Any physical element that deters penetration. May include items such as fences, walls, floors, roofs, grills, bars, padlocks, chains, gates, or other structures.
Real Time		Direct, without any delay.
Recognizable		To be able to recognize a person, place, or thing from knowledge of appearance or characteristics.
Security Corrective Action Requirement	SCAR	The documented observation of non-compliance with a TAPA Standard requirement.
Self-Audit		Compliance verification conducted by the TAPA-certified entity (warehouse or trucking company) using the applicable TAPA Audit Form, as per the schedule specified in the FSR or TSR Standard.
Self-Certification		A process by which an entity certifies their own company to the TAPA FSR Level C or TSR Level 3.
TAPA FSR Certified Company		An LSP/Applicant that has been found by an AA to have met the applicable FSR requirements.
TAPA Security Standards		Global logistics standards developed by TAPA to secure cargo during storage (FSR) and transport by road (TSR).
TAPA FSR Audit Forms		Standard audit templates for the measurement of conformance to FSR
Temporary		Non-permanent and/or short term.
Temporary Agency Staff	TAS	Temporary workforce
Trucking Security Requirements	TSR	TAPA Standard describing the security requirements for surface transportation by truck and trailer/container.
Waiver		Written approval to exempt a LSP/Applicant from a TAPA requirement or accept an alternative compliance solution. Note: The TAPA Regional Waiver Committee reviews waiver requests, then grants or denies all waivers.
Workforce		All employees, temporary agency staff, and subcontractors, unless individually identified.

Appendix B:
TAPA Standards - Waiver Request Form

Instructions: Complete a separate Waiver Request form for each requirement to be considered for a Waiver. Section 1-5 must be completed before submission to TAPA.

Please note that the waiver request form is available as a download from TAPA via https://www.tapa-global.org/industry-standards.html

1. LSP/Applicant

Company Name	
Address (where waiver applies)	
Date of Request	
LSP/Applicant Responsible Person	
Name	
Phone	
Email	
Signature	

2. Existing Requirement to be Considered for Waiver

TAPA Standard, Version and Level	
TAPA Requirement number and full text	

3. Reasons and Impact of Non-Compliance

Reasons why requirement cannot be complied with?	
Impact/risks if no mitigation controls were implemented	

4. Mitigation

Mitigation measures and security controls that will be implemented	
List of attachments and supporting documentation that support this request (plans, images, procedures, official evidence etc.)	

5. Approved Auditor

Date	
Company Name	
Approved Auditor	
Name	
Phone	
Email	
AA Supporting LSP's/Applicant's Request Y/N?	
Reasons for Y/N Response	
Signature	

6. TAPA Approval/Denial (TAPA use only)

Date	
Waiver Number	
Approved/Denied	
Reason Approved/Denied	
Conditions to be followed by LSP/Applicant if Approved	
Waiver Approved From /To Dates	
Authorized by / On Behalf of TAPA: Name	
Authorized Signature	