FACILITY SECURITY REQUIREMENTS

TAPA
Transported Asset Protection Association

Exigences de sûreté des installations FSR 2020

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 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 des matières

FSR Table of Contents

FSR Table de matières (suite)

□□□

1. Introduction

1.1 Objet du présent document FSR

Ce document relatif aux exigences de sûreté des installations (FSR) constitue le référentiel officiel TAPA pour sécuriser un entrepôt. Ce référentiel international peut intervenir dans les accords commerciaux concernant la sûreté entre les chargeurs et les Prestataires de Services Logistiques (PSL) et/ou d'autres candidats sollicitant une certification.

Dans le développement de ce référentiel, TAPA reconnait qu'il existe de nombreuses différences de prestation de services d'entreposage et de stockage à l'échelle mondiale, régionale, et au sein des entreprises. Le référentiel FSR peut s'appliquer à tout ou partie des services fournis par un PSL/candidat. Selon la complexité et la taille de la chaîne logistique, la certification TAPA peut être obtenue par un seul ou plusieurs PSL/candidats et sous-traitants référencés.

Champ d'application

Le référentiel TAPA FSR peut s'appliquer aux cas suivants :

- Certification d'un site unique par un organisme certificateur indépendant (IAB).
- Certification Multi-site par un organisme certificateur indépendant.
- Auto-certification par les Auditeurs Agréés (AA) du PSL/candidat ou de l'organisme certificateur indépendant.

Public

Les utilisateurs courants des normes TAPA incluent : Les utilisateurs des référentiels TAPA sont, entre autres :

- Les chargeurs
- Les PSL/candidats
- Les forces de l'ordre et tous services d'Etat
- Les organisations professionnelles de la chaîne logistique
- Les assureurs

1. Introduction

1.2 Ressources nécessaires pour mettre en œuvre TAPA FSR

Les ressources nécessaires pour répondre aux exigences de TAPA FSR relèvent de la responsabilité du PSL/candidat. Les frais s'y rapportant sont à la charge de ce dernier, sauf si des accords contractuels entre le chargeur et le PSL/candidat en décident autrement

1.3 Protection des politiques et procédures du PSL/candidat

Les copies des documents relatifs aux politiques et procédures de sûreté ne seront transmises au chargeur que conformément aux accords entre le PSL/candidat et le chargeur et seront traitées comme des données confidentielles.

2. À propos de TAPA

2.1 Objectif de TAPA

Pour les fabricants de produits de valeur ou à haut risque ainsi que leurs prestataires de services logistiques, le vol de marchandises constitue l'un des plus grands défis de la chaîne logistique.

La menace n'émane plus seulement de délinquants opportunistes. Aujourd'hui, des réseaux criminels organisés opèrent sur la scène internationale et commettent des attaques de plus en plus sophistiquées (véhicules, locaux et personnel) pour parvenir à leurs fins.

TAPA constitue l'unique instance qui réunit, au niveau international, les fabricants, les prestataires de services logistiques, les transporteurs, les autorités ainsi que d'autres parties prenantes, autour d'un objectif commun, celui de réduire les pertes dans la chaîne logistique internationale. TAPA s'intéresse principalement à la lutte contre le vol, en utilisant des données du renseignement en temps réel et les toutes dernières mesures de prévention.

2.2 Mission de TAPA

La mission de TAPA est d'aider à protéger les biens de ses adhérents en minimisant les risques d'incidents dans la chaine logistique. TAPA réalise cette mission grâce au développement et à l'application des standards internationaux de sûreté, des bonnes pratiques, des outils technologiques, de la formation, du benchmarking, du partenariat avec les autorités, et de l'analyse proactive des tendances criminelles et des menaces de sûreté.

3. Normes TAPA

3.1 Référentiels de sûreté TAPA

Les référentiels internationaux de sûreté TAPA ont été créés afin d'assurer le transport et le stockage sécurisés des marchandises de haute valeur susceptibles de faire l'objet de vols :

- Le référentiel **FSR** correspond aux exigences minimales requises pour sécuriser un site ou un entrepôt logistique au sein d'une chaîne logistique.
- Le référentiel **TSR** porte exclusivement sur le transport routier et correspond aux exigences minimales requises pour sécuriser le transport des marchandises par route au sein d'une chaîne logistique.

Les référentiels internationaux de sûreté TAPA sont revus et révisés, si nécessaire, tous les trois ans.

Ce document traite uniquement des exigences FSR

- Le processus de certification du TAPA FSR est documenté dans le document Cadre de certification du TAPA FSR.
- Les deux versions actuelles du document TAPA FSR et du cadre de certification TAPA FSR doivent être respectées pour obtenir le statut de certification TAPA FSR.

3.2 Mise en oeuvre

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.

La réussite de la mise en œuvre des référentiels de sûreté TAPA dépend de la collaboration des PSL/candidat, des chargeurs ainsi que des auditeurs agréés TAPA.

4. Conseils juridiques

4.1 Champ d'application

TAPA FSR est un référentiel international. Toutes les sections ont un caractère obligatoire, à moins qu'une exception ne soit accordée via la procédure de dérogation officielle (voir Section 6.)

4.2 Traduction

Dans les zones géographiques où l'anglais n'est pas la langue principale, et où une traduction est nécessaire pour sa mise en œuvre, le PSL/candidat et ses représentants doivent s'assurer que toute traduction du TAPA FSR (tout ou partie) reflète fidèlement les intentions de TAPA quant au développement et à la publication de ces référentiels.

4.3 La marque « TAPA »

« TAPA » est une marque déposée de la « Transported Asset Protection Association ». Elle ne saurait être utilisée sans l'autorisation formelle écrite des représentations régionales officielles TAPA. Les référentiels TAPA et toute documentation s'y rapportant sont publiés par TAPA ou par son intermédiaire, et ne sauraient être revus, édités ni modifiés par quiconque sans l'autorisation formelle écrite de TAPA.

Un usage abusif de la marque TAPA pourrait entraîner l'annulation de toute certification ou une action en justice.

4.4 Limites de la responsabilité

Par la publication de ces référentiels, TAPA ne fournit aucune garantie ni assurance que tous les vols de marchandises seront évités, que les référentiels soient ou non entièrement déployés et correctement mis en œuvre. Toute responsabilité pouvant résulter d'un vol, ou de toute autre perte de marchandises acheminées selon le référentiel TAPA FSR sera imputable au PSL/candidat et/ou au chargeur conformément aux modalités du contrat qui les lie et à toute législation ou règlementation pouvant s'appliquer dans la juridiction compétente.

5. Contrats et sous-traitance

5.1 Contrats et sous-traitance

Le transport, le stockage et la manutention en toute sécurité des biens du chargeur incombent au PSL/candidat, à ses représentants et sous-traitants à toutes les étapes spécifiées dans une demande de transport ou un contrat : enlèvement, acheminement, stockage et livraison.

Lorsque le référentiel FSR sera mentionné ou inclus dans le contrat entre le PSL/candidat et le chargeur, il y sera également fait référence dans le programme de sûreté du PSL/candidat.

Le PSL/candidat fournira au chargeur la preuve de sa certification FSR ou le cas échéant, des preuves que les exigences FSR ont été satisfaites. De plus, tout manquement présumé de mise en œuvre des exigences FSR sera résolu conformément aux modalités du contrat négocié entre le chargeur et le PSL/candidat.

5.2 Sous-traitance

Les sous-traitants concernés par l'entreposage et le stockage doivent être soumis à une exigence contractuelle selon laquelle le sous-traitant PSL/candidat respecte toutes les normes du FSR

Les sous-traitants non certifiés TAPA doivent faire l'objet d'un audit, conformément au contrat entre le chargeur et le PSL/candidat.

5.3 Instruction et résolution des réclamations par TAPA

Si TAPA reçoit une réclamation officielle au sujet des prestations d'un PSL/candidat certifié, elle pourra exiger (sous réserve de validation) de la part du PSL/candidat qu'il organise un nouvel audit à ses frais. Si ce dernier n'est pas satisfaisant ou que le PSL/candidat refuse de se conformer à ce processus, son attestation pourra lui être retirée.

.

6. Dérogation

6. 1 Présentation générale

Une dérogation est une autorisation écrite accordée soit pour exempter une entreprise d'une exigence TAPA spécifique, soit pour accepter une solution de conformité alternative. Elle peut être demandée si un PSL/candidat ne peut pas répondre à une exigence spécifique du FSR et peut légitimer la mise en place d'autres mesures. Les dérogations restent valables pendant toute la période de validité de la certification.

Le PSL/candidat doit remettre à l'Organisme Certificateur Indépendant/Auditeur Agréé chaque demande de dérogation pour une exigence de sûreté spécifique (tout ou partie), au moyen du formulaire de demande de dérogation TAPA (à télécharger sur le site TAPA). Le PSL/candidat qui sollicite une dérogation assume l'entière responsabilité de l'exactitude des informations fournies.

Chaque demande de dérogation doit être soumise, via l'Organisme Certificateur Indépendant/Auditeur Agréé, à la commission régionale TAPA en charge des dérogations afin d'être approuvée. C'est à l'Organisme Certificateur Indépendant/Auditeur Agréé que revient la responsabilité de décider de l'exhaustivité de la demande et si cette dernière justifie d'être examinée par TAPA. Cela comprend la vérification des mesures de diminution du risque et/ou des dispositifs de sûreté alternatifs.

Si les représentants de TAPA et/ou le chargeur contestent cette demande de dérogation, TAPA diligentera une enquête officielle et pourrait révoquer la demande de dérogation du PSL/candidat.

6. 2 Dérogations - processus administratif

Si un PSL/candidat ne peut se conformer à une exigence spécifique du FSR, le processus de dérogation ci-dessous sera mis en œuvre.

Tableau 1: Responsabilités : Demande de dérogation / Évaluation

Step	Responsibility	Action
1.	PSL/ candidat	Établit et vérifie les mesures de diminution du risque.
2.	PSL/ candidat	Remplit le formulaire de demande de dispense TAPA et le soumet à l'organisme d'audit indépendant/auditeur agréé. Remplit le formulaire de demande de dérogation TAPA et le soumet à l'Organisme Certificateur Indépendant / Auditeur Agréé.

Step	Responsibility	Action
3.	Organisme Certificateur Indépendant / Auditeur Agréé	Examine et vérifie l'intégrité des informations contenues dans le formulaire de demande de dérogation TAPA.
4.	Organisme Certificateur Indépendant / Auditeur Agréé	Soumet le formulaire de demande de dérogation TAPA à la commission régionale TAPA en charge des dérogations.
5.	Commission régionale TAPA en charge des dérogations	Examine la demande, puis accorde ou refuse la dérogation.

6. Dérogation

En cas de rejet de la dérogation.

Si la commission régionale TAPA en charge des dérogations rejette la demande, le PSL/candidat doit mettre en œuvre la totalité des exigences de sûreté du FSR.

En cas de validation de la dérogation

Si la commission régionale TAPA en charge des dérogations valide la demande, les actions suivantes doivent être mises en place :

Tableau 2: Approbation de la dérogation

Step	Responsibility	Action
1.	Commission régionale TAPA en charge des dérogations	Rend compte des détails de la dérogation et signe cette dernière.
2.	Commission régionale TAPA en charge des dérogations	Précise la durée de la dérogation (trois ans maximum) et envoie un exemplaire à l'Auditeur Agréé.
3.	Auditeur Agréé	Prévient le PSL/candidat de l'issue de la demande de dérogation.
4.	PSL/candidat	Se conforme aux exigences de la dérogation. Tout manquement annulera la validation de la demande.

6. 3 Dérogations pour les barrières physiques (sous la section 1) et les cages pour marchandises de haute valeur (HV sous-section 4.5)

TAPA envisagera une dérogation eu égard à tout ou partie des exigences relatives aux barrières physiques et/ou cages pour les marchandises de Haute Valeur si l'ensemble des conditions préalables suivantes sont remplies :

Généralités:

- La demande de dérogation est soumise au moyen du formulaire officiel de demande de dérogation TAPA. Elle est approuvée par l'Organisme certificateur indépendant/Auditeur Agréé.

- La demande de dérogation comprend les détails de toute mesure d'atténuation visant à s'assurer que les marchandises vulnérables ne sont pas exposées à un risque inutile de vol ou de perte.

- Une évaluation des risques doit être effectuée et soumise avec la demande de dérogation. Toute vulnérabilité importante identifiée dans l'évaluation des risques doit être énumérée séparément dans la dérogation et les mesures prises pour réduire le risque à un niveau acceptable.

6. Dérogation

Les mesures d'atténuation des risques doivent être reprises et documentées dans la demande de dérogation:

- **Périmétrie : clôtures/barrières physiques:**

  - Tous les équipements, ressources et procédures supplémentaires à mettre en place permettant de détecter encore plus rapidement tout individu ou véhicule non autorisés peuvent inclure, mais sans s'y limiter, de l'éclairage additionnel, de la vidéosurveillance, des procédures de contrôle renforcé sur l'identité des personnes et des véhicules, des gilets (LSP) ou des uniformes dans des zones bien définies.
  - Une signalétique visible « accès non autorisé » et « stationnement interdit » doit être installée.

- Des consignes d'accès pour les conducteurs, visiteurs, … doivent être clairement affichées à l'extérieur (portes et mûrs) afin de les diriger vers l'entrée appropriée pour le contrôle sûreté.
- Confirmation que des procédures sont en place pour s'assurer que les aires de manutention, d'expédition et de réception du fret sont inspectées et conformes aux conditions de dérogation au moins une fois par semaine.

- **Cage pour les marchandises de Haute Valeur (HV):**

  - Concernant les dérogations des cages pour les marchandises de haute valeur, les mesures d'atténuation appropriées visant à réduire les risques (lorsqu'une CHV n'est pas disponible) doivent être prises en compte et documentées dans l'évaluation annuelle des risques.
  - Une déclaration, signée par le PSL/candidat est à joindre à la demande de dérogation, indiquant qu'aucun chargeur n'a besoin d'une Cage pour les marchandises de Haute Valeur.

7. Exigences de sûreté des installations (FSR)

Section	Exigences générales :	A	B	C
7.0				
7.0.1	Toutes les procédures ou politiques exigées par le présent référentiel doivent être documentées.	✔	✔	✔
7.0.2	Une procédure, un registre et/ou un plan de gestion de clés sont nécessaires pour gérer et contrôler les serrures, les cartes d'accès et/ou les clés qui gèrent et contrôlent les accès.	✔	✔	✔

Section	Périmétrie	A	B	C
7.1				
Zones extérieures de l'entrepôt pour la manutention, réception et expédition du fret (global)				
7.1.1	Couverture vidéo des aires de réception et d'expédition (incluant les points d'entrée et de sortie) capable de voir tout le trafic, de reconnaitre les personnes et les véhicules sauf en cas d'obstruction temporaire due aux besoins opérationnels (ex : pendant le chargement/déchargement d'un camion)	✔	✔	

Section	Périmétrie	A	B	C
7.1.2	Eclairage suffisant des aires de chargement et de déchargement. *A noter : l'éclairage peut être permanent ou par détection sur alarme, mouvement, sonore, etc... avec déclenchement immédiat)*	✔	✔	✔
7.1.3	Procédure documentée décrivant la conduite à tenir en cas d'intrusion des personnes ou des véhicules non autorisés. Ces consignes doivent être transmises aux employés concernés incluant les agents de sûreté.	✔	✔	✔
7.1.4	Les zones de manutention et de réception sont contrôlées de façon à prévenir tout accès non autorisé.		✔	✔
7.1.5	Pour les portes de quai et les fenêtres des bureaux de plain-pied donnant sur l'extérieur du bâtiment, l'évaluation annuelle des risques doit prendre en compte la nécessité d'un système anti-bélier (voir section 7.6.5)	✔		
Sécurité physique				
7.1.6	La clôture rigide entoure les zones de manutention, de réception et d'expédition du fret	✔		
7.1.7	La hauteur de la clôture rigide doit mesurer au minimum 1.8 m. A *noter : La clôture rigide, conçue pour empêcher toute intrusion, doit avoir une hauteur de 1,8 m sur toute sa longueur quelque soit le dénivelé du terrain*	✔		
7.1.8	La clôture autour de la cour de manutention, d'expédition et de réception de la cargaison est maintenue en bon état.	✔		
7.1.9	Lieu d'accès aux zones de manutention, de réception et d'expédition du fret physiquement ou électroniquement contrôlé	✔		
7.1.10	La barrière/clôture physique entourant la zone de manutention, d'expédition et de réception des marchandises est inspectée pour en vérifier l'intégrité et les dommages au moins une fois par semaine.	✔		
Aires de quai externes				
7.1.11	Zones extérieures du quai couvertes par des caméras couleur ou des caméras extérieures « jour/nuit ».	✔	✔	✔
7.1.12	Les caméras sont montées pour permettre de voir toutes les opérations et tous les mouvements autour de la zone extérieure du quai à tout moment, à moins qu'il n'y ait une obstruction temporaire en raison des besoins opérationnels (p. ex., chargement et déchargement des camions en temps réel).	✔	✔	✔
7.1.13	Tous les véhicules et les individus autour des quais extérieurs sont clairement reconnaissables.	✔		
7.1.14	Les véhicules et les individus autour des zones extérieures de quai visibles dans la plupart des cas		✔	✔
7.1.15	Toutes les zones extérieures autour des portes du quai sont entièrement éclairées	✔	✔	✔
Accès aux véhicules personnels				

Section	Périmétrie	A	B	C
7.1.16	Les véhicules personnels ne sont autorisés dans les aires de manutention, d'expédition et de réception que s'ils sont pré approuvés et réservés aux aires de stationnement désignées. Aucun stationnement personnel à moins de 25m à pied des quais extérieurs. Les processus de pré approbation et les restrictions en place	✔	✔	✔

Section	Murs extérieurs, Toit et Portes	A	B	C
7.2				
Côtés extérieurs de l'entrepôt : Vidéosurveillance				
7.2.1	Tous les côtés de l'entrepôt couverts par des caméras extérieures couleur ou " jour/nuit"	✔		
7.2.2	Caméras extérieures couleur ou "jour/nuit" couvrant les côtés de l'entrepôt qui ont des portes, fenêtres ou toute autre ouverture.		✔	
7.2.3	Toutes les vues du système de caméras extérieures sont dégagées de manière permanente, à moins d'obstruction temporaire en raison des besoins opérationnels (c.-à-d. chargement et déchargement des camions en temps réel).	✔		
7.2.4	Tous les véhicules et les individus clairement reconnaissables par le système de caméra extérieure.	✔		
7.2.5	Véhicules et individus visibles dans la plupart des cas par le système de caméra extérieure.		✔	
Murs extérieurs et le toit				
7.2.6	Les murs extérieurs et le toit conçus et entretenus pour résister à toute intrusion (ex : murs en brique en béton, dalle de béton, etc ...)	✔	✔	✔
7.2.7	Toute fenêtre, évent ou autre ouverture, ou toute autre partie vitrée non ouvrable installée à moins de 3 mètres du sol doit être munie d'un système de barreaudage ou d'une alarme reliée au système d'alarme principal.	✔	✔	
7.2.8	Toute fenêtre, puits de lumière, évent, ou autre type d'ouvrant au toit de l'entrepôt doit être équipée de barreaudage **ou** être équipée d'une alarme reliée au système d'alarme principal	✔		
7.2.9	L'accès externe au toit (échelle ou escalier) doit être physiquement verrouillé et sous couverture vidéo (caméras couleur ou « jour/nuit »). **ou** Physiquement verrouillé et sous alarme.	✔		
7.2.10	Accès extérieur au toit (échelle ou escalier) physiquement verrouillé.		✔	✔

Section	Murs extérieurs, Toit et Portes	A	B	C
7.2.11	Toutes les portes extérieures de l'entrepôt et des bureaux sont munies d'un système d'alarme pour détecter les ouvertures non autorisées et reliées au système d'alarme principal. *Remarque : Les portes des quais ne sont pas concernées par cette exigence. Voir la section 7.2.17 pour connaître les exigences relatives à l'alarme des portes des quais.*	✔	✔	✔
7.2.12	Toutes les portes extérieures de l'entrepôt et des bureaux ou autres ouvertures doivent être identifiées individuellement ou par zone dans le système d'alarme principal.	✔		
7.2.13	Toutes les portes extérieures d'accès à l'entrepôt (portes de quai, ...) toujours fermées et sécurisées quand elles ne sont pas utilisées. Contrôle des clés/codes.	✔	✔	
7.2.14	Les encadrements et les portes piétons de l'entrepôt doivent résister aux tentatives d'intrusion. Si les charnières sont à l'extérieur, elles doivent être fixées ou soudées par points. Les portes en verre ne sont pas acceptées sauf si des détecteurs bris de glace ou tout autre dispositif de détection équivalent sont fixés (ex : IF). Ou si le verre est protégé par des barres et sous alarme reliée directement au centre de contrôle.	✔	✔	✔
7.2.15	Toutes les issues de secours en permanence sous alarme avec une sirène sonore locale individuelle ou par zone identifiée et reliée au système d'alarme principal	✔	✔	
7.2.16	Toutes les portes de quai de matériaux permettant de décourager et/ou retarder toute intrusion à l'aide de petits outils manuels	✔	✔	✔
7.2.17	Portes de quai : **En dehors des heures ouvrées** : Portes de quai fermées et sécurisées (physiquement verrouillées ou électroniquement déconnectées) Portes du quai munies d'un système d'alarme pour détecter toute intrusion non autorisée et déclencher une alarme reliée au système d'alarme principal **Durant les heures ouvrées** : Portes de quai fermées quand elles ne sont pas utilisées. En cas de "grilles ciseaux", elles doivent être sécurisées par des moyens de protection mécaniques (barre, lame, serrure) et doivent mesurer au minimum 2.40 m de haut	✔	✔	✔

Section	Points d'entrée et de sortie des bureaux et de l'entrepôt	A	B	C
7.3				
Point(s) d'entrée bureaux pour les visiteurs				
7.3.1	Points d'accès aux visiteurs contrôlés par un employé/réceptionniste/poste de garde formé à la remise de badges, au contrôle des mesures, à l'enregistrement et à l'accompagnement des visiteurs, etc… (procédure en place pour la gestion des visiteurs en dehors des horaires d'ouverture)	✔	✔	✔
7.3.2	Points d'accès aux visiteurs sous couverture vidéo (caméras couleur ou jour/nuit). Individus clairement reconnaissables en permanence.	✔	✔	
7.3.3	Alarme de contrainte discrètement installé aux accès visiteurs et testé chaque semaine	✔	✔	
7.3.4	Tous les visiteurs identifiés à partir d'un document officiel avec photo (passeport, carte nationale d'identité, permis de conduire...)	✔	✔	✔
7.3.5	Tous les visiteurs enregistrés. Les informations sont conservées un minimum de 30 jours.	✔	✔	✔
7.3.6	S'assurer de la restitution des badges à chaque départ d'un visiteur. Contrôle journalier complet de la liste	✔	✔	
7.3.7	Tous les visiteurs doivent clairement porter les badges ou les laissez-passer temporaires. Tous les visiteurs doivent être accompagnés par un membre du personnel de l'entreprise	✔	✔	
Point(s) d'entrée des employés				
7.3.8	Accès aux employés contrôlés 24/7.		✔	✔
7.3.9	Accès aux employés contrôlés par un dispositif électronique (contrôle d'accès) 24/7. Tous les accès sont enregistrés	✔		
7.3.10	Point(s) d'accès aux employés sous couverture vidéo (caméras couleur ou jour/nuit)).	✔	✔	
7.3.11	Après validation, les employés doivent avoir un badge identifiant de la société avec photo	✔	✔	
7.3.12	Pour les autres (sous-traitants, intérimaires…), ils doivent être munis d'un badge société pour les rendre reconnaissables dans l'entrepôt	✔	✔	
7.3.13	Tous les badges doivent être portés et clairement visibles	✔	✔	
7.3.14	En aucun cas, les badges ne doivent être partagés. Procédure documentée pour l'émission/gestion des badges	✔	✔	
Identification des conducteurs et des véhicules				
7.3.15	Tous les conducteurs doivent être identifiés à l'aide d'un document officiel avec photo (passeport, carte nationale d'identité, permis de conduire…). Enregistrements des conducteurs conservés.	✔	✔	✔
7.3.16	Vérification que le permis de conduire est valide, que la pièce d'identité avec photo du conducteur n'a pas expiré et qu'elle correspond au conducteur	✔	✔	✔

Section	Points d'entrée et de sortie des bureaux et de l'entrepôt	A	B	C
7.3.17	Les véhicules doivent être identifiés et enregistrés manuellement (ex : par écrit) ou par vidéosurveillance. Incluant au minimum la plaque d'immatriculation et le type de véhicule	✔		

Section	Intérieur Quai/Entrepôt et Bureaux	A	B	C
7.4				
Entrepôt : Murs mitoyens				
7.4.1	Intérieur : Pour les séparations du sol au plafond mitoyennes, les murs et le toit doivent être conçus et entretenus pour résister à toute intrusion (ex : brique, béton...)	✔	✔	✔
7.4.2	Intérieur : Si les séparations du sol au plafond mitoyennes sont construites avec des grilles métalliques de sécurité ou avec tout autre système de barrière de protection efficace, alors elles doivent également être sous alarme pour détecter toute intrusion. A noter: les filets, les grillages ou les grilles de faible qualité ne sont pas acceptés	✔	✔	✔
Zones intérieures de l'entrepôt				
7.4.3	Un système de détection d'intrusion (ex : infrarouge, mouvement, sonore ou par vibration) est exigé pour sécuriser l'intérieur de l'entrepôt. Les alarmes doivent être activées et reliées au système d'alarme principal en dehors des heures d'ouverture (quand l'entrepôt est fermé). A noter : si l'activité du site est permanente 24/7/366, alors cette exigence peut être considérée comme N/A à partir du moment où cette diminution du risque est prise en compte dans l'évaluation locale des risques. Indépendamment des heures d'ouverture, le périmètre des portes extérieures et des fenêtres du rez-de-chaussée de l'entrepôt et des bureaux doit être protégé par un système d'alarme ou une clôture rigide (voir section 7.2.11).	✔		
Zones et portes de quai intérieures				
7.4.4	Toutes les zones et portes de quai intérieures sous couverture vidéo (caméras couleur ou jour/nuit)	✔	✔	✔
7.4.5	Opérations de chargement/déchargement clairement visibles en permanence sauf en cas d'obstruction temporaire due aux besoins opérationnels (ex : pendant le chargement/déchargement d'un camion)	✔	✔	✔
7.4.6	les marchandises des clients en permanence (100%) sous couverture vidéo dans les zones de circulation ou de transit (palletisage/dépalletisage - vers et en provenance des racks et des quais, couloirs de transit).	✔	✔	
Contrôle d'accès entre les bureaux et le quai/entrepôt				
7.4.7	Contrôle d'accès entre les bureaux et l'entrepôt ou le quai	✔	✔	
7.4.8	Système par carte ou interphone équipé d'une alarme sonore locale déclenchée au bout de 60 secondes en cas d'ouverture prolongée ou immédiatement en cas d'ouverture forcée	✔		

Section	Intérieur Quai/Entrepôt et Bureaux	A	B	C
7.4.9	Alarme sonore des portes entre les bureaux et l'entrepôt locale ou envoi d'un signal en cas d'ouverture prolongée ou forcée de plus de 60 secondes.		✔	
7.4.10	Accès à l'entrepôt et au quai uniquement par les employés autorisés et par les visiteurs accompagnés basés et limités aux besoins opérationnels.	✔	✔	✔
7.4.11	Liste des accès révisée au moins chaque trimestre afin de limiter/vérifier les autorisations. Procédure documentée	✔	✔	
La Cage/zone Haute Valeur (cage HV)				
7.4.12	La taille et l'utilisation de la cage HV peuvent être définies en accord avec les chargeurs. En l'absence d'accord, le minimum de stockage doit être de 6m3.	✔	✔	
7.4.13	La cage de haute valeur (HV) est grillagée ou constituée de parois solides sur tous les côtés incluant le dessus/toit	✔	✔	
7.4.14	La cage HV est équipée d'un dispositif de verrouillage sur la porte/ portail.	✔	✔	
7.4.15	Couverture vidéo complète (caméras couleur ou jour/nuit) de la cage ou sur l'entrée et la zone interne. *A noter : si la surface de la cage est trop petite pour installer une caméra à l'intérieur, une caméra sur l'entrée de la cage est suffisante.*	✔		
7.4.16	Couverture vidéo (caméras couleur ou jour/nuit) sur l'entrée de la cage		✔	
7.4.17	**Si accès à plus de 10 personnes** : contrôle d'accès électronique nécessaire **Jusqu'à 10 personnes** : système de verrouillage (serrure/cadenas) autorisé. Dans ce cas, pour chaque opération par du personnel autorisé, les mouvements des clés doivent être enregistrés par du personnel approuvé. Les clés doivent être comptabilisées à la fin de chaque opération	✔		
7.4.18	L'accès (porte/portail) de la cage HV doit être sous alarme pour détecter toute intrusion. Par des contacteurs aux portes et/ou alarme vidéo (détection de mouvements)	✔		
7.4.19	La zone /cage HV maintenue en bon état et inspectée sur une base mensuelle (intégrité/ dommage).	✔		
7.4.20	Le PSL/candidat s'assure que l'accès est seulement accordé à du personnel autorisé. La liste du personnel autorisé est revue et mise à jour mensuellement, immédiatement en cas de départ d'un employé ou si l'autorisation n'est plus nécessaire. Procédure documentée	✔	✔	
Inspection des poubelles de l'entrepôt				

Section	Intérieur Quai/Entrepôt et Bureaux	A	B	C
7.4.21	Principaux bacs de l'entrepôt collectant les ordures (intérieur et/ou extérieur) et la zone de compactage sous couverture vidéo	✔		
7.4.22	Utilisation de sacs poubelle transparents.		✔	✔
Pré-chargement et stationnement des FTL/camions				
7.4.23	Pas de pré-chargement ou de stationnement des FTL/camions à l'extérieur de l'entrepôt pendant les heures de fermeture sauf en cas d'un commun accord avec le chargeur incluant des mesures de protection supplémentaires (ex : des dispositifs de sécurité complémentaires sur les unités de fret). A noter : "à l'extérieur de l'entrepôt" est considéré comme une zone séparée, loin des installations mais qui reste toujours dans le périmètre clôturé.	✔	✔	✔
Effets personnels et fouilles aux sorties				
7.4.24	Procédure de sûreté écrite définissant l'accès des effets personnels dans l'entrepôt. Les "effets personnels" incluent les sacs à dos, glacières, paniers, sacs, etc.…	✔	✔	
7.4.25	Si la loi locale l'autorise, le PSL/candidat doit développer et maintenir une procédure documentée pour la fouille des effets personnels. L'activation de cette procédure est à la discrétion du PSL/candidat ou avec l'accord du chargeur. Cette procédure doit au minimum contenir l'autorisation de fouille en cas de nécessité (exemple: suspicion de spoliation/vol)	✔		
Contrôle des équipements de manutention				
7.4.26	Tous les chariots élévateurs et les autres matériels de manutention électriques désactivés durant les heures de fermeture. Procédure documentée. A noter : cela n'inclut pas les diables et les transpalettes manuels	✔	✔	
Intégrité des containers ou des remorques. Inspection des 7 points.				

7.4.27	Inspection physique en "7 points " ou contrôle équivalent effectués pour tous les conteneurs/remorques en partance : parois avant, côté gauche, côté droit, plancher, toit, portes et dispositifs de fermeture intérieur/extérieur, sous le châssis. Procédure documentée. *A noter : cela s'applique à tous les camions/conteneurs disposant d'un dispositif de fermeture par serrure/scellé. (Par exemple ne se limite pas seulement aux conteneurs maritimes)*	✔	✔	✔
Transfert/acheminement du fret : gestion des plombs/scellés				
7.4.28	Sauf en cas d'exemption par le chargeur, des plombs/scellés inviolables doivent être apposés sur tous les envois directs et sans rupture de charge. Les plombs/scellés doivent répondre à la norme ISO 17712 (classifications I-S-HS). A noter : les plombs/scellés ne sont pas exigés en cas d'arrêts multiples (plusieurs adresses de livraison) en raison de la complexité et du risque lié au fait que le conducteur a plusieurs plombs/scellés en sa possession	✔	✔	✔
7.4.29	Procédure documentée pour la gestion et le contrôle des plombs/scellés, le verrouillage des camions/conteneurs (serrures et/ou tout autre équipement de sûreté)	✔	✔	✔
7.4.30	Les plombs/scellés sont fixés ou retirés uniquement par du personnel autorisé (employés qui ont les informations pour faire le rapprochement). Les plombs/scellés ne doivent jamais être fixés ou retirés par le conducteur sauf en cas d'exemption du chargeur	✔	✔	✔
7.4.31	Procédure en place pour reconnaitre et répertorier les plombs compromis	✔	✔	✔
Intégrité du fret : procédures de validation des chargements/déchargements				
7.4.32	Procédure fiable garantissant que toutes les marchandises reçues ou expédiées sont quantitativement contrôlées (manuellement ou électroniquement) lors de leur manutention. Procédure documentée qui s'assure que les anomalies sont systématiquement identifiées, relevées et signalées au PSL/candidat ou au chargeur. Les enregistrements manuels ou électroniques doivent être précis. Si les conducteurs n'assistent pas à ce contrôle, le chargeur/PSL/candidat doit assurer un contrôle quantitatif alternatif comme le scannage ou l'enregistrement vidéo avec des données conservées pour la même utilité. *A noter : en plus des pièces manquantes, ce contrôle peut aussi inclure les avaries (scotch manquant ou déchiré, découpage ou toute autre ouverture supposant un vol ou une spoliation)*	✔	✔	✔
Enlèvements frauduleux				
7.4.33	Avant chaque chargement, l'identité du conducteur, les documents de transport ou tout autre document transmis par le chargeur doivent être vérifiés	✔	✔	✔

Section	Systèmes de sécurité : installation, poste de surveillance et suivi	A	B	C
7.5				
Poste de surveillance				

Section	Systèmes de sécurité : installation, poste de surveillance et suivi	A	B	C
7.5.1	Les déclenchements d'alarme doivent être suivis 24X7X366 via un poste de surveillance interne, voire un poste externe protégé contre les accès non autorisés. *A noter : Le poste de surveillance peut se situer dans l'enceinte ou à l'extérieur du site et peut appartenir à l'entreprise ou à un tiers. Dans tous les cas, les accès doivent être contrôlés par un système de contrôle d'accès électronique (badges), par des serrures ou par un dispositif biométrique*	✔	✔	✔
7.5.2	Tous les systèmes d'alarme doivent être suivis en permanence 24X7X366	✔	✔	✔
7.5.3	Le poste de surveillance identifie l'alarme et intervient en moins de 3 minutes	✔	✔	✔
7.5.4	Les rapports de suivi des alarmes doivent être disponibles	✔	✔	✔
7.5.5	Procedure de suivi documentée	✔	✔	✔
Système d'alarme intrusion				
7.5.6	Tous les systèmes d'alarme activés en dehors des heures d'ouverture et reliés au système d'alarme principal	✔	✔	✔
7.5.7	60 jours d'enregistrements du système d'alarme conservés	✔	✔	
7.5.8	Les enregistrements du système d'alarme sécurisés et sauvegardés	✔		
7.5.9	Les enregistrements du système d'alarme sécurisés		✔	
7.5.10	Procédure documentée qui s'assure que les systèmes de sûreté (équipements et données) sont uniquement accessibles par du personnel autorisé. Cela inclut les serveurs, baie informatique réseau, logiciel, base de données) Suppression/modification immédiate des codes d'alarme en cas de départ d'un employé ou si les fonctions de ce dernier ne nécessitent plus de les conserver	✔	✔	✔
7.5.11	Alarme transmise en cas de panne/perte d'alimentation électrique. *Note : Pour les systèmes équipés d'un onduleur, Une alarme est transmise quand les batteries de l'onduleur sont en défaut (ex : batteries faibles)*	✔	✔	✔
7.5.12	Vérification de la programmation de l'alarme Note : Procédure documentée qui confirme l'activation de l'alarme pendant les heures de fermeture	✔	✔	✔
7.5.13	Transmission de l'alarme en cas de défaut de l'appareil ou de la ligne	✔	✔	
7.5.14	Système de communication secondaire en place en cas de défaut de l'appareil ou de la ligne.	✔	✔	
Système de contrôle d'accès électronique (SCAA)				
7.5.15	90 jours d'enregistrements des données disponibles. Enregistrements sécurisés et sauvegardés pour sauvegarde.	✔	✔	

Section	Systèmes de sécurité : installation, poste de surveillance et suivi	A	B	C
7.5.16	Procédure documentée qui s'assure que les systèmes de contrôle d'accès sont uniquement accessibles par du personnel autorisé. Suppression/modification immédiate des codes d'accès en cas de départ d'un employé ou si les fonctions de ce dernier ne nécessitent plus de les conserver	✔	✔	
7.5.17	Contrôle trimestriel, au minimum, des rapports du système afin d'identifier les irrégularités ou abus (plusieurs tentatives infructueuses, carte invalide, partage de la carte pour permettre un accès non autorisé…) Procédure documentée.	✔	✔	
CCTV système de vidéosurveillance				
7.5.18	Enregistrement numérique.	✔	✔	✔
7.5.19	Enregistrement avec un minimum 8 images par seconde (ips) par caméra *Note : TAPA permettra aux titulaires de la certification actuels qui n'ont pas la capacité de passer à 8 ips de continuer avec les 3 ips existants jusqu'à la révision de 2023. Les nouveaux titulaires de certificat doivent satisfaire à la nouvelle exigence*	✔	✔	✔
7.5.20	Vérification quotidienne (période d'activité) des enregistrements via une procédure documentée. Documentation disponible	✔	✔	✔
7.5.21	Conservation des enregistrements pendant un minimum de 30 jours si cela est autorisé par la loi locale. Fournir les preuves de la loi locale si moins de 30 jours	✔	✔	✔
7.5.22	Accès restreint au système vidéo (le matériel, les logiciels, les données/enregistrements)	✔	✔	✔
7.5.23	Pour des raisons de sûreté, les images sont uniquement accessibles par du personnel autorisé	✔	✔	✔
7.5.24	Procédure documentée détaillant la politique de protection des données concernant l'utilisation en temps réel des images et des enregistrements en conformité avec la loi locale	✔	✔	
Eclairage extérieur et intérieur				
7.5.25	Les niveaux d'éclairage intérieurs et extérieurs sont suffisants pour avoir une qualité d'image permettant de mener une enquête	✔	✔	
7.5.26	Les niveaux d'éclairage extérieur et intérieur sont suffisants pour reconnaître clairement tous les véhicules et les individus	✔		

Section	Formation et procédures	A	B	C
7.6				
Procédures d'intervention				

Section	Formation et procédures	A	B	C
7.6.1	Procédure locale documentée concernant la manutention des marchandises incluant les délais d'information au chargeur en cas de perte, manquant ou vol. Les incidents doivent être signalés aux chargeurs dans les 24 heures, immédiatement pour les vols. Procédure constamment suivie	✔	✔	✔
7.6.2	Liste des contacts chargeurs/PSL disponible en cas d'urgence (incidents sûreté). Liste mise à jour au minimum tous les 6 mois incluant les autorités (police…)	✔	✔	✔
Engagement de la direction				
7.6.3	Le PSL/candidat doit avoir une personne officiellement nommée pour la sûreté sur le site, qui est responsable du maintien des exigences de sûreté de TAPA FSR et de la chaine d'approvisionnement de la société. Le PSL/candidat doit également avoir une personne (qui peut être la même) en charge du suivi du programme FSR. Cela comprend le délai de mise en conformité, les communications avec les auditeurs, le renouvellement, les évolutions/modifications de la norme. *A noter : cette personne peut être un employé ou une ressource externe sous contrat pour assurer ce rôle*	✔	✔	✔
7.6.4	La direction doit développer, communiquer et maintenir une politique de sûreté qui assure que toutes les personnes concernées (employés et sous-traitants) sont clairement conscientes des attentes du PSL/candidat	✔	✔	✔
7.6.5	Une évaluation des risques concernant la probabilité et l'impact des évènements liés à la sûreté doit être effectuée/mise à jour au moins une fois par an. L'évaluation doit être documentée et exige de la direction de prendre des décisions qui diminueraient les risques de sûreté. Au minimum, les évènements internes/externes suivants doivent être évalués : le vol de marchandise ou d'information, l'accès non autorisé aux installations, la manipulation/destruction des systèmes de sûreté, la sûreté pendant la manipulation des marchandises, les pénuries ou catastrophes naturelles, etc... D'autres évènements liés aux risques locaux peuvent être pris en considération	✔	✔	✔
Formation				
7.6.6	Formation/sensibilisation à la sûreté et aux menaces dispensée à tous les employés et répétée tous les 2 ans qui comprend à la fois des risques généraux et des risques spécifiques locaux	✔	✔	✔
7.6.7	Formation/sensibilisation axée sur la protection des données des dossiers des chargeurs (électronique et papier) dispensée à tous les employés ayant accès à ces informations	✔	✔	
Accès aux marchandises des chargeurs				
7.6.8	Procédure documentée qui restreint l'accès aux marchandises (employés, visiteurs…)	✔	✔	
Contrôle de l'information				
7.6.9	Accès aux informations sur les envois et les chargeurs contrôlés et basés sur le principe du « qui doit savoir »	✔	✔	✔

Section	Formation et procédures	A	B	C
7.6.10	Accès aux informations sur les envois contrôlés/surveillés et enregistrés	✔	✔	✔
7.6.11	Accès aux informations sur les envois et information sur les chargeurs sauvegardés jusqu'à leur destruction	✔	✔	✔
Signalement des incidents de sûreté				
7.6.12	Enregistrement des incidents de sûreté avec un système de suivi qui permet la mise en œuvre de mesures proactives	✔	✔	
Programmes de Maintenance				
7.6.13	Programmes de maintenance documentés qui s'assurent du bon fonctionnement permanent de tous les systèmes/installations électroniques/physiques de sûreté (ex : vidéosurveillance, contrôle d'accès, alarme, éclairage)	✔	✔	✔
7.6.14	La maintenance préventive doit être effectuée au moins une fois par an ou en concordance avec les spécificités des fabricants	✔	✔	✔
7.6.15	Vérification hebdomadaire et documentée des fonctionnalités de tous les systèmes sauf si les défaillances sont immédiatement/automatiquement remontées	✔	✔	
7.6.16	Une demande d'intervention/réparation doit être formulée dans les 48 heures suivant la découverte du défaut. Pour toute réparation supérieure à 24 heures, des mesures alternatives doivent être mises en œuvre	✔	✔	
Maitrise de la sous-traitance				
7.6.17	Le PSL/candidat s'assure que tous les sous-traitants / prestataires connaissent et respectent les programmes de sûreté	✔	✔	✔
Documents d'expédition et de réception				
7.6.18	Documents lisibles, complets et exacts (exemple: date, heure, signature, conducteur, détail des envois et quantité…)	✔	✔	✔
7.6.19	Le PSL/candidat doit conserver tous les documents des envois ainsi que les preuves de livraisons au moins deux ans et les garder à disposition en cas d'investigation ultérieure par exemple pour perte	✔	✔	✔
7.6.20	La preuve de livraison doit être fournie conformément à l'accord écrit entre Le chargeur et le PSL/candidat. En cas d'exigence du chargeur, les arrivages doivent être notifiés au chargeur dans les délais de réception convenus, recoupant les détails pré-annoncés de l'expédition	✔	✔	✔
Procédures de pré-avis				

Section	Formation et procédures	A	B	C
7.6.21	En cas d'exigence du chargeur, la procédure de pré-avis s'applique aux envois expédiés et reçus. Les détails doivent être convenus par le chargeur et le PSL/candidat. Suggestion de détails : heure de départ, heure d'arrivée, nom du transporteur, nom du conducteur, plaque d'immatriculation, informations sur l'envoi (quantité, poids, N° lettre de voiture/CMR, numéro de plomb/scellé)	✔	✔	✔

Section	Intégrité du personnel	A	B	C
7.7				
7.1	Procédures de recrutement (selon les lois en vigueur)			
7.7.1	Le PSL/candidat doit avoir une procédure de recrutement incluant au minimum le contrôle des antécédents professionnels et criminels. Cette procédure s'applique à tous les candidats incluant les employés et les sous-traitants. Le PSL/candidat exigera des sociétés d'intérim et des sociétés sous-traitantes une procédure équivalente	✔	✔	✔
7.7.2	Les intérimaires et les sous-traitants doivent signer une déclaration comme quoi ils n'ont pas de condamnation pénale en cours et qu'ils se conformeront bien aux procédures de sûreté du PSL/candidat	✔	✔	✔
7.7.3	Le PSL/candidat aura les accords des sociétés d'intérim et des sociétés sous-traitantes pour récupérer les informations concernant les intérimaires et les sous-traitants ou devra conduire lui-même les vérifications incluant les antécédents criminels et professionnels	✔	✔	✔
7.7.4	Procédure de traitement des fausses déclarations pré/post embauche des candidats/employés	✔	✔	✔
Fin d'emploi (volontaire et involontaire) ou réembauche du personnel				
7.7.5	Procédure documentée fin d'emploi. La procédure doit inclure la remise des clés, badges et autres équipements ou informations sensibles	✔	✔	✔
7.7.6	Procédure documentée pour la protection des données des chargeurs (informations et activités). Tous les moyens physiques et/ou électroniques (codes, clés, mots de passe…) doivent être récupérés/désactivés	✔	✔	✔
7.7.7	Registre du personnel à disposition pour contrôle	✔	✔	✔
7.7.8	Procédure afin d'éviter la réembauche d'un employé si les critères de fin d'emploi/refus d'un poste sont toujours valables. Note : Les dossiers sont systématiquement contrôlés avant la réembauche (motif de fin d'emploi/refus d'un poste)	✔	✔	✔

8. Exigences relatives aux fonctions centrales (applicable uniquement pour la certification multi-site

Section	Fonction centrale	A	B	C
8.1	**Généralités**			
8.1.1	Une fonction centrale supervise le système de gestion de la sûreté pour tous les sites tels que définis dans le cadre de la certification multi-sites.	✔	✔	✔
8.1.2	Tous les sites ont un lien juridique ou contractuel avec la fonction centrale	✔	✔	✔
8.1.3	Un système unique de gestion de la sûreté est mis en place pour s'assurer que tous les sites répondent aux exigences du référentiel sûreté TAPA.	✔	✔	✔
8.1.4	La fonction centrale et son système de gestion font l'objet d'audits internes visant à assurer la conformité continue du référentiel sûreté TAPA	✔	✔	✔
8.1.5	La fonction centrale effectue des audits de tous les sites concernés afin de s'assurer que le système de gestion de la sûreté de chaque site répond aux exigences du référentiel. Les vérifications doivent être effectuées à l'aide des modèles de vérification TAPA appropriés	✔	✔	✔
8.1.6	La fonction centrale doit avoir le pouvoir et les droits d'exiger que tous les sites se conforment au référentiel de sûreté requises par TAPA et de mettre en œuvre des mesures correctives et préventives au besoin. *Note : Le cas échéant, cela devrait être précisé dans l'accord formel entre la fonction centrale et les sites.*	✔	✔	✔
8.2	**Politique et Procédures**			
8.2.1	La fonction centrale doit maintenir des politiques et des procédures documentées pour ses systèmes de gestion de la sûreté qui s'appliquent à tous ses sites.	✔	✔	✔
8.2.2	La fonction centrale veille à ce que les politiques et procédures soient mises à jour, communiquées, déployées et mises en œuvre par tous les sites.	✔	✔	✔
8.2.3	Les politiques et procédures doivent être suivies et facilement accessibles par tous les sites.	✔	✔	✔
8.3	**Rapport d'auto-évaluation réalisé pour tous les sites**			
8.3.1	La fonction centrale donne mandat à tous les sites de procéder à l'auto-évaluation et tous les rapports d'auto-évaluation sont soumis à la fonction centrale aux fins d'enregistrement et d'examen.	✔	✔	✔
8.3.2	La fonction centrale veille à ce que tous les écarts constatés lors de l'auto-évaluation et des audits soient fermés de manière appropriée afin d'améliorer le système de gestion de la sûreté.	✔	✔	✔
8.3.3	Tous les sites soumettent à la fonction centrale des rapports d'étape et des rapports sur tous les écarts en suspens. La fonction centrale doit remonter à la direction du LSP/candidat si les écarts ne sont pas achevés avant les dates d'échéance.	✔	✔	✔
8.4	**Registres des inspections, registres (registres des visiteurs, registres des conducteurs), inspections en 7 points**			

Section	Fonction centrale	A	B	C
8.4.1	La fonction centrale à en place des procédures en place pour s'assurer que tous les sites tiennent des registres des inspections, des visiteurs et des conducteurs et des inspections des 7 points, etc.	✔	✔	✔
8.5	**Évaluation des risques de tous les sites**			
8.5.1	La fonction centrale met en place des procédures pour s'assurer que des évaluations et une gestion appropriées des risques sont effectuées sur tous les sites et que des registres sont tenus.	✔	✔	✔
8.6	**Mise en place de caméras de surveillance et d'alarmes sur les sites**			
8.6.1	La fonction centrale à des procédures en place pour s'assurer que tous les sites examinent et tiennent à jour des documents sur tous les systèmes de sûreté physique comme la vidéosurveillance et la disposition des alarmes.	✔	✔	✔
8.7	**Alarme et enregistrement des contrôles d'accès**			
8.7.1	La fonction centrale à des procédures en place pour s'assurer que tous les systèmes d'alarme et de contrôle d'accès sont entretenus et testés pour assurer leur efficacité opérationnelle.	✔	✔	✔
8.7.2	La fonction centrale à des procédures en place pour que tous les sites tiennent des registres de tous les tests et incidents de détection d'intrusion et de contrôle d'accès.	✔	✔	✔
8.8	**Enregistrements de formations**			
8.8.1	La fonction centrale à des procédures en place pour s'assurer que tous les sites tiennent des dossiers de formation appropriés sur la formation en gestion de la sûreté de ses employés	✔	✔	✔
8.8.2	La fonction centrale à des procédures en place pour s'assurer que tous les sites tiennent des dossiers de formation en matière de sûreté pour tout le personnel du site.	✔	✔	✔
8.9	**Contrôle / vérification des antécédents**			
8.9.1	La fonction centrale à des procédures en place pour s'assurer que tous les sites effectuent l'examen et le contrôle des antécédents à intervalles réguliers afin d'assurer l'intégrité et l'efficacité des systèmes de gestion de la sûreté.	✔	✔	✔
8.9.2	La fonction centrale à des procédures en place pour s'assurer l'enregistrement des dossiers, y compris ses constatations et les mesures correctives/préventives 8.1.6 qui sont tenus.	✔	✔	✔
8.10	**Examen par la direction pour évaluer les auto-vérifications; SCRA relevées; pertes, vols; évaluations des risques.**			
8.10.1	La fonction centrale procède régulièrement à une revue de direction pour s'assurer de la conformité, de l'efficacité et de l'amélioration de ses systèmes de gestion de la sûreté.	✔	✔	✔
8.10.2	Les revues de la direction portent, entre autres, sur l'efficacité des auto-évaluations, les fermetures des écarts, les évaluations des risques, les incidents ainsi que les mesures d'amélioration	✔	✔	✔
8.10.3	La fonction centrale tient des registres de toutes les revues de direction	✔	✔	✔

9.0. Menace informatique et cybersécurité – Option améliorée

Le FSR intègre des améliorations facultatives des menaces liées à la cybersécurité qui sont considérées comme un niveau de protection plus élevé et qui peuvent être utilisées en plus des modules. Cette amélioration facultative est destinée à être sélectionnée par le LSP/candidat et/ou le chargeur comme exigences supplémentaires pour des besoins de sûreté opérationnelle.

Lorsque cette option est sélectionnée dans l'évaluation de pré-certification, toutes les exigences deviennent obligatoires.

.

Section	Menace informatique et cybersécurité – Option améliorée
9.	***Exigences obligatoires***
9.1	Le chargeur ou le PSL/ candidat doit avoir des politiques de sûreté IT et cybermenaces. Les politiques peuvent être distinctes ou regroupées dans un document. Les politiques doivent expliquer : 1. Les mesures prises par le LSP/candidat pour repérer les menaces et y réagir. 2. Les politiques et procédures en place pour protéger, détecter, tester et intervenir en cas d'incident de sûreté. 3. Les méthodes de récupération des systèmes ou des données informatiques. 4. Le protocole de communication avec les chargeurs et les clients pour atténuer l'incidence sur la chaîne d'approvisionnement dans les 24 heures suivant la connaissance de l'incident. 5. La façon dont les politiques sont examinées chaque année et mises à jour au besoin.
9.2	Le PSL/ candidat doit offrir une formation de sensibilisation à l'information à tous les employés. Cette formation doit : 1. Couvrir les rôles et les responsabilités des utilisateurs d'ordinateurs en ce qui concerne le maintien de la sûreté et les avantages connexes. 2. Mettre en place un système qui garantit la conservation des justificatifs de formations pendant au moins une durée de deux ans
9.3	Le PSL/ candidat a en place une politique écrite pour s'assurer que les mesures de cybersécurité sont en place avec les sous-traitants et/ou les fournisseurs qui s'assurent : 1. Les exigences en matière de cybersécurité du PSL/ candidat sont communiquées aux sous-traitants et/ou aux fournisseurs et intégrées aux exigences. 2. Lorsque les sous-traitants et/ou les fournisseurs ne reconnaissent pas ou refusent d'adopter les exigences de cybersécurité des demandeurs, des mesures sont documentées et en place pour atténuer les risques pour les exigences de cybersécurité des PSL/candidat et de leurs chargeurs

Section	Menace informatique et cybersécurité – Option améliorée
9.4	Le PSL/ candidat a un plan d'atténuation des coupures de courant (p. ex., alimentation de rechange ou générateurs de secours) qui garantit que l'alimentation est acheminée vers les systèmes informatiques critiques (identifiés dans l'évaluation des risques locaux) pendant au moins 48 heures.
9.5	Les systèmes d'information du PSL/ candidat sont munis d'un logiciel antivirus et antivirus sous licence. Le logiciel anti-virus doit contenir les dernières mises à jour.
9.6	Le PSL/ candidat dispose d'un plan de continuité après sinistre (DRP) approprié pour la reprise après une attaque système compromise, y compris, mais sans s'y limiter, toutes les sauvegardes de données et de logiciels nécessaires et les arrangements de reprise.
9.7	Les systèmes d'information du PSL/ candidat sont sauvegardés. Ces sauvegardes sont testées régulièrement et les données de sauvegarde chiffrées et transférées à un emplacement secondaire hors site.
9.8	Le PSL/ candidat met en œuvre une politique pour tous les comptes utilisateurs afin de gérer et de contrôler l'accès aux systèmes d'information en utilisant des identifiants individuels uniques et des mots de passe forts. Procédures en place pour assurer : 1. Programme de vérification de la conformité des mots de passe en place. 2. Un premier mot de passe unique doit être attribué à chaque nouveau compte au moment de sa création. 3. Les mots de passe initiaux ne peuvent pas contenir le nom de l'utilisateur, son numéro d'identification ou suivre un modèle standard basé sur les informations de l'utilisateur. 4. Les mots de passe seront communiqués aux utilisateurs de manière sécurisée, et seulement après validation de l'identité de l'utilisateur. 5. Les utilisateurs doivent être tenus de modifier les mots de passe lors de la première ouverture de session. 6. Les mots de passe doivent être changés au moins tous les 90 jours

Publishing and copyright information

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

Publication history

First published in January 2020

First (present) edition published in January 2020

This Publicly Available Specification comes into effect on 1st July 2020