Transported Asset Protection Association

FSR 2026

TAPA Global Standard

Copyright © TAPA Not Copy

TAPA Americas

1353 Riverstone Pkwy,
Ste 120-320
Canton, GA 30114 USA

www.tapaonline.org

TAPA Asia Pacific

Oxley BizHub 2
62 Ubi Road 1, #06-11
Singapore 408734

www.tapa-apac.org

TAPA EMEA

Kanaalpark 140
2321 JV Leiden
The Netherlands

www.tapaemea.org

© TAPA 2026

Table de Matière

1.0 Introduction *4*

1.1 Objet du présent document FSR 4

1.2 Ressources pour la mise en œuvre du TAPA FSR 4

1.3 Protection des politiques et procédures des fournisseurs de services logistiques 4

2.0 À propos de TAPA *5*

2.1 Objectif de TAPA 5

2.2 Mission de TAPA 5

3.0 Normes TAPA *6*

3.1 Normes de Sûreté TAPA 6

3.2 Mise en œuvre 6

4.0 Conseils juridiques *7*

4.1 Portée 7

4.2 Traduction 7

4.3 La marque TAPA 7

4.4 Limites de responsabilité 7

5.0 Contrats et sous-traitance *8*

5.1 Contrats 8

5.2 Sous-traitance 8

5.3 Enquête et résolution des plaintes de TAPA 8

6.0 Dérogations *9*

7.0 Exigences de Sûreté des installations *10*

S1. Exigences générales 10

S2. Périmètre 12

2.1 Entrepôt - Manutention, expédition et réception des marchandises à l'extérieur 12

2.2 Barrières physiques 13

2.3 Zones de quai extérieures 13

2.4 Accès aux véhicules personnels 14

S3. Murs extérieurs, toit et portes 15

3.1 Côtés extérieurs de l'établissement : vidéosurveillance/VSS 15

3.2 Murs extérieurs et toiture 16

S4. Points d'entrée et de sortie des bureaux et des entrepôts 19

4.1 Point(s) d'entrée visiteurs de la zone de bureaux 19

4.2 Point(s) d'entrée de la main-d'œuvre 20

4.3 Identification du conducteur et du véhicule 20

S5. Entrepôt et bureaux intérieurs 22

5.1 Zone d'entrepôt : Murs multi-locataires 22

5.2 Zones internes de l'entrepôt 22

TAPA Copyright © Do Not Copy

5.3 Portes de quai intérieures et zones de quai ... 23
5.4 Contrôle d'accès entre le bureau et le quai/entrepôt ... 23
5.5 Zone de fret de grande valeur (HVC) ... 24
5.6 Inspection des déchets de l'entrepôt ... 25
5.7 Préchargement et préparation ... 25
5.8 Fouilles des contenants personnels et fouilles à la sortie ... 26
5.9 Contrôle des équipements de manutention de cargaison ... 26
5.10 Intégrité du conteneur ou de la remorque : inspection en 7 points ... 26
5.11 Processus de remise des marchandises ; scellés de Sûreté ... 27
5.12 Intégrité du chargement ; processus de validation du chargement/déchargement ... 28
5.13 Collectes frauduleuses ... 28

S6. Systèmes de Sûreté : conception, surveillance et intervention ... 29
6.1 Poste de surveillance ... 29
6.2 Système de détection d'intrusion (IDS) ... 29
6.3 Système de contrôle d'accès automatique (AACS) ... 30
6.4 CCTV/VSS ... 31
6.5 Éclairage extérieur et intérieur ... 32

S7. Formation et procédures ... 33
7.1 Procédures d'escalade ... 33
7.2 Engagement de la direction ... 33
7.3 Entraînement ... 33
7.4 Accès aux biens de l'acheteur ... 34
7.5 Contrôle de l'information ... 34
7.6 Signalement des incidents de Sûreté ... 34
7.7 Programmes de maintenance ... 35
7.8 Management des sous-traitants/fournisseurs ... 35
7.9 Expédition et réception des dossiers ... 35
7.10 Processus de pré-alerte en place ... 36

S8. Intégrité de la main-d'œuvre ... 37
8.1 Vérification des antécédents (conformément à la législation locale) ... 37
8.2 Licenciement ou réembauche du personnel ... 37

S9. Exigences relatives aux fonctions centrales (applicables uniquement à la certification multisite) ... 39
9.1 Générale ... 39
9.2 Politiques et procédures ... 40
9.3 Rapport d'audit d'auto-évaluation réalisé pour tous les sites ... 40
9.4 Comptes rendus d'inspections, registres (registres des visiteurs/conducteurs), inspections en 7 points 41
9.5 Évaluation des risques de tous les sites ... 41
9.6 Plan d'implantation du site : système de vidéosurveillance/d'alarme et de surveillance vidéo. 41
9.7 Enregistrements d'alarmes et de contrôle d'accès ... 41
9.8 Dossiers de formation ... 42
9.9 Dossiers de sélection/vérification ... 42
9.10 Revue de direction pour évaluer les auto-audits ; les SCAR (actions correctives et préventives) soulevées ; les pertes et vols ; les évaluations des risques ... 42

8.0 Menaces informatiques et de cybersécurité – Option améliorée ... 44

E8. Exigences obligatoires ... 44

TAPA Copyright © Do Not Copy

1.0 Introduction

1.1 Objet du présent document FSR

Ce document relatif aux exigences de Sûreté des installations (FSR) constitue la norme officielle TAPA pour l'entreposage sécurisé. Il s'agit d'une norme internationale commune pouvant être utilisée dans les accords commerciaux et de Sûreté conclus entre les acheteurs et les prestataires de services logistiques (PSL) et/ou autres candidats à la certification.

Lors de l'élaboration de cette norme, TAPA a pris en compte les nombreuses différences dans la manière dont les services d'entreposage sont fournis à l'échelle mondiale, régionale et même au sein d'une même entreprise, et a reconnu que les exigences FSR peuvent s'appliquer à tout ou partie des services fournis par un PSL/candidat. Selon la complexité et la taille de la chaîne d'approvisionnement, la conformité aux normes TAPA peut être assurée par un seul PSL/candidat ou par plusieurs PSL/candidats et sous-traitants qualifiés.

Portée

TAPA propose trois options pour faciliter la certification :

• Certification monosite par un organisme d'audit indépendant (OAI).

• Certification multisite par un OAI.

• Auto-audit réalisé par des auditeurs agréés (AA) pour le compte du prestataire de services linguistiques/demandeur ou d'un OAI (réalisant un auto-audit pour le compte du prestataire de services linguistiques/demandeur).

Public

Les utilisateurs types des normes TAPA sont notamment :

• Acheteurs

• Prestataires de services logistiques/Demandeurs

• Forces de l'ordre ou autres organismes gouvernementaux

• Organisations professionnelles de la chaîne d'approvisionnement

• Assureurs

1.2 Ressources pour la mise en œuvre du TAPA FSR

Les ressources nécessaires pour répondre aux exigences du FSR seront à la charge du PLS/Demandeur et à ses propres frais, sauf négociation ou autre accord entre l'Acheteur et le PLS/Demandeur.

1.3 Protection des politiques et procédures des fournisseurs de services logistiques

Les copies des documents relatifs aux politiques et procédures de Sûreté ne seront soumises à l'acheteur que conformément aux accords de divulgation signés entre le prestataire de services logistiques/demandeur et l'acheteur et seront traitées comme des informations confidentielles.

TAPA Copyright © Do Not Copy

2.0 À propos de TAPA

2.1 Objectif de TAPA

Le vol de marchandises représente l'un des plus grands défis pour la chaîne d'approvisionnement des fabricants de produits de valeur et à haut risque, ainsi que pour leurs prestataires logistiques.

La menace ne provient plus seulement de criminels opportunistes. Aujourd'hui, des réseaux criminels organisés opèrent à l'échelle mondiale et utilisent des attaques de plus en plus sophistiquées contre les véhicules, les locaux et le personnel pour atteindre leurs objectifs.

TAPA est une plateforme unique qui réunit des fabricants internationaux, des prestataires logistiques, des transporteurs, les forces de l'ordre et d'autres acteurs clés autour d'un objectif commun : réduire les pertes liées aux chaînes d'approvisionnement internationales. La priorité de TAPA est la prévention du vol grâce à l'utilisation de renseignements en temps réel et des mesures préventives les plus novatrices.

2.2 Mission de TAPA

La mission de TAPA est de contribuer à la protection des actifs de ses membres en minimisant les pertes de marchandises tout au long de la chaîne d'approvisionnement. TAPA y parvient grâce à l'élaboration et à l'application de normes de Sûreté internationales, de pratiques sectorielles reconnues, de technologies de pointe, de formations, d'analyses comparatives, de collaborations réglementaires et à l'identification proactive des tendances criminelles et des menaces pesant sur la Sûreté de la chaîne d'approvisionnement.

TAPA Copyright © Do Not Copy

3.0 Normes TAPA

3.1 Normes de Sûreté TAPA

Les normes de Sûreté TAPA internationales suivantes ont été créées pour garantir le transport et le stockage sécurisés des marchandises de grande valeur, particulièrement vulnérables au vol :

• Les exigences de Sûreté des installations (FSR) définissent les normes minimales applicables à l'entreposage sécurisé, ou au stockage en transit, au sein d'une chaîne d'approvisionnement.

• Les exigences de Sûreté du transport routier (TSR) concernent exclusivement le transport par camion et définissent les normes minimales applicables au transport routier de produits au sein d'une chaîne d'approvisionnement.

• Les exigences de Sûreté des parkings sécurisés (PSR) concernent exclusivement la sécurisation des parkings destinés au stationnement des véhiucles routier.

• Les normes de cybersécurité (CSS) visent à fournir aux entreprises un outil leur permettant de comprendre les exigences minimales en matière de gestion informatique de leurs opérations de chaîne d'approvisionnement, afin de protéger leurs actifs numériques contre les cyberattaques et les interruptions d'activité.

Les normes de Sûreté mondiales TAPA sont examinées et révisées, le cas échéant, tous les trois (3) ans.

Ce document traite uniquement des exigences FSR !

- Le processus de certification TAPA FSR est documenté dans le document « Cadre de certification TAPA FSR .
- Il est impératif de respecter à la fois les versions actuelles du document TAPA FSR et du cadre de certification TAPA FSR pour obtenir la certification TAPA FSR.

3.2 Mise en œuvre

La réussite de la mise en œuvre des normes de Sûreté TAPA dépend de la collaboration entre les prestataires de services logistiques (PSL)/demandeurs, les acheteurs (propriétaires de la cargaison) et les auditeurs agréés TAPA.

TAPA Copyright © Do Not Copy

4.0 Conseils juridiques

4.1 Portée

La norme FSR est une norme mondiale, et toutes ses sections sont obligatoires, sauf si une exception est accordée par le biais de la procédure de dérogation officielle (voir la section 6 de la norme FSR et la section 7 du document-cadre de certification FSR).

4.2 Traduction

Dans les zones géographiques où l'anglais n'est pas la langue maternelle et où la traduction est nécessaire et applicable, il incombe au prestataire de services linguistiques/demandeur et à ses représentants de veiller à ce que toute traduction du FSR, ou de l'une de ses parties, reflète fidèlement les intentions de TAPA lors de l'élaboration et de la publication de ces normes.

4.3 La marque TAPA

TAPA est une marque déposée de la Transported Asset Protection Association et ne peut être utilisée sans l'autorisation écrite expresse de TAPA dans ses régions officiellement reconnues. Les normes TAPA et les documents associés sont publiés par et pour TAPA et ne peuvent être modifiés, édités ou altérés par quiconque sans son autorisation écrite expresse. Toute utilisation abusive de la marque TAPA peut entraîner le retrait de la certification ou des poursuites judiciaires.

4.4 Limites de responsabilité

La publication de ces normes n'implique aucune garantie de la part de TAPA quant à la prévention de tous les vols de marchandises, même en cas de déploiement et d'application intégrale et correcte des normes. Toute responsabilité découlant d'un vol ou d'une perte de marchandises entreposées, conformément aux normes FSR, incombe au prestataire logistique/demandeur et/ou à l'acheteur, conformément aux termes et conditions de leur contrat et à toute loi ou réglementation applicable dans la juridiction concernée.

TAPA Copyright © Do Not Copy

5.0 Contrats et sous-traitance

5.1 Contrats

Le transport, l'entreposage et la manutention sûrs et sécurisés des biens de l'acheteur relèvent de la responsabilité du PSL/demandeur, de ses agents et sous-traitants tout au long des opérations de collecte, de transit, d'entreposage et de livraison, conformément aux dispositions d'une quittance ou d'un contrat.

Lorsque le référentiel de Sûreté des marchandises (FSR) est mentionné ou inclus dans le contrat entre le prestataire logistique/demandeur et l'acheteur, il doit également être mentionné dans le programme de Sûreté du PSL/demandeur.

Le PSL/demandeur doit fournir à l'acheteur une preuve de certification FSR et, le cas échéant, la preuve que les exigences FSR ont été respectées. En outre, tout manquement avéré du prestataire logistique/demandeur à la mise en œuvre des exigences FSR sera résolu conformément aux termes du contrat négocié entre l'acheteur et le PSL/demandeur.

5.2 Sous-traitance

En cas de recours à des sous-traitants, une clause contractuelle doit stipuler que ces derniers respectent toutes les exigences FSR mentionnées. Les auditeurs internes agréés de PLS doivent confirmer que le sous-traitant satisfait aux exigences FSR de même niveau.

5.3 Enquête et résolution des plaintes de TAPA

Si TAPA reçoit une plainte formelle concernant la performance d'un prestataire de services logistiques(PSL) ou d'un candidat certifié, TAPA peut (sous réserve de validation) exiger que le PSL ou le candidat fasse l'objet d'un nouvel audit à ses frais. Si le PSL ou le candidat échoue à l'audit ou refuse de se conformer à cette procédure, son certificat peut être retiré.

TAPA Copyright © Do Not Copy

6.0 Dérogations

Une dérogation est une autorisation écrite permettant d'exempter un établissement d'une exigence spécifique du TAPA et d'accepter une solution de conformité alternative.

Une dérogation peut être demandée si un PSL / demandeur ne peut satisfaire à une exigence spécifique du FSR et peut justifier des mesures alternatives.

Les dérogations sont valables pour la durée de la certification.

TAPA Copyright © Do Not Copy

7.0 Exigences de Sûreté des installations

S1. Exigences générales

N° de ~~demande~~	Exigences / Contrôles	Niveau applicable		
1.1.1	Toutes les procédures ou politiques requises par la présente norme doivent être documentées et mises à jour au moins tous les deux ans.	Ⓐ	Ⓑ	Ⓒ
1.1.2	La direction doit avoir désigné officiellement un responsable de la Sûreté sur site, chargé du maintien des exigences de Sûreté de la chaîne d'approvisionnement de l'entreprise, notamment en matière de Sûreté des installations (TAPA FSR), de gestion et clôture des non conformités (SCARS), d'évaluation des risques, de rapports de gestion et de Sûreté . Une autre personne (qui peut être la même) sera également responsable du suivi du programme FSR. Cela inclut la planification des contrôles de conformité, la communication avec les responsables de la Sûreté, la recertification, le suivis des modifications apportées à la norme FSR, etc. Ces personnes peuvent être des employés ou des prestataires externes sous contrat.	Ⓐ	Ⓑ	Ⓒ
1.1.3	Les audits internes (réalisés par une équipe interfonctionnelle) du système de management de la Sûreté (SMS), les rapports d'auto-évaluation de l'AA interne et la clôture des SCARS doivent être complétés et documentés.	Ⓐ	Ⓑ	Ⓒ
1.1.4	Une procédure, un registre et/ou un plan de gestion des clés sont nécessaires pour les serrures physiques, les cartes d'accès et/ou les clés permettant de gérer et de contrôler les clés physiques et électroniques. Cette procédure doit inclure les modalités de duplication, de stockage et de gestion des clés perdues ou manquantes.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N° de ~~demande~~	Exigences / Contrôles	Niveau applicable		
1.1.5	Une évaluation des risques documentée, prenant en compte la probabilité et l'impact des menaces à la Sûreté , doit être réalisée et mise à jour au moins une fois par an. La direction doit examiner et confirmer que les risques identifiés ont été évalués et que des mesures de contrôle appropriées ont été mises en œuvre pour les atténuer ou les éliminer à un niveau acceptable. Àu minimun, les événements internes et externes courants suivants doivent être évalués : vol de marchandises ou d'informations, accès non autorisé aux installations ou aux marchandises, altération ou destruction des systèmes de Sûreté , enlèvements frauduleux de marchandises, continuité de la Sûreté en cas de pénurie de personnel ou de catastrophes naturelles, nécessité d'installer des barrières anti-intrusion aux fenêtres ou portes de quai accessibles au niveau du sol, etc. D'autres menaces peuvent être prises en compte en fonction des risques locaux et nationaux.	Ⓐ	Ⓑ	Ⓒ
1.1.6	La personne chargée des audits internes ou annuels pour le PSL / demandeur (appelée auditeur du prestataire de services linguistiques) doit être formée. Il peut s'agir de la même personne que celle mentionnée au point 1.1.2 ou d'un prestataire externe sous contrat pour remplir cette fonction.	Ⓐ	Ⓑ	Ⓒ
1.1.7	Pour comprendre le FSR et être en mesure de mettre en œuvre toutes ses exigences, tous les AA doivent avoir passé et réussi l'examen applicable à la norme TAPA et à la version sur laquelle ils sont tenus d'effectuer l'audit.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S2. Périmètre

2.1 Entrepôt - Manutention, expédition et réception des marchandises à l'extérieur

N° de demande	Exigences / Contrôles	Niveau applicable		
2.1.1	Système de vidéosurveillance (CCTV/VSS) capable de visualiser tout le trafic sur le site de manutention, d'expédition et de réception des marchandises (y compris les points d'entrée et de sortie), garantissant que tous les véhicules et les personnes sont reconnaissables à tout moment, sauf en cas d'obstruction temporaire due aux besoins opérationnels (par exemple, le chargement et le déchargement des camions en temps réel).	Ⓐ	Ⓑ	
2.1.2	Un éclairage adéquat dans les zones de chargement et de déchargement doit être utilisé comme moyen de dissuasion de base contre la criminalité et permettre de visualiser les opérations dans ces zones pendant la nuit. *Remarque : L'éclairage peut être continu ou activé par une alarme, un mouvement, une détection sonore, etc., avec un éclairage immédiat assuré.*	Ⓐ	Ⓑ	Ⓒ
2.1.3	Une procédure décrivant la gestion des véhicules et des personnes non autorisées dans l'aire de manutention, d'expédition et de réception des marchandises doit être mise en place. Cette procédure doit être communiquée aux membres du personnel concernés, y compris aux agents de Sûreté .	Ⓐ	Ⓑ	Ⓒ
2.1.4	La zone de manutention des marchandises, l'expédition et la zone de réception doivent être correctement contrôlées afin d'empêcher tout accès non autorisé.		Ⓑ	Ⓒ
2.1.5	Pour les fenêtres, portes ou portes de quai accessibles au niveau du sol, l'évaluation annuelle des risques doit déterminer la nécessité d'installer des barrières anti-intrusion. Elle doit également évaluer l'utilisation de rideaux ou de stores pour empêcher les regards indiscrets à l'intérieur des bâtiments (voir l'évaluation des risques, exigence 1.1.5).	Ⓐ		

TAPA Copyright © Do Not Copy

2.2 Barrières physiques

N° de demande	Exigences / Contrôles	Niveau applicable		
2.2.1	Une barrière physique entoure la zone de manutention, d'expédition et de réception des marchandises	Ⓐ		
2.2.2	La barrière physique entourant la zone de manutention, d'expédition et de réception des marchandises doit avoir une hauteur minimale de 1,8 mètre (6 pieds). Remarque : Cette barrière physique, conçue pour empêcher tout accès non autorisé, doit avoir une hauteur de 1,8 mètre (6 pieds) sur toute sa longueur, y compris aux endroits où le niveau du sol est plus bas.	Ⓐ		
2.2.3	Barrière physique autour de la zone de manutention, d'expédition et de réception des marchandises doit être maintenue en bon état.	Ⓐ		
2.2.4	Les porte(s) à l'intérieur de la zone de manutention, d'expédition et de réception des marchandises, doivent être gardées ou contrôlées électroniquement.	Ⓐ		
2.2.5	La barrière physique entourant la zone de manutention, d'expédition et de réception des marchandises est inspectée au moins une fois par semaine afin de vérifier son intégrité et l'absence de dommages.	Ⓐ		

TAPA Copyright © Do Not Copy

2.3 Zones de quai extérieures

N° de demande	Exigences / Contrôles	Niveau applicable		
2.3.1	Les zones de quai extérieures sont couvertes par des caméras de vidéosurveillance/VSS extérieures couleur ou « jour/nuit ».	Ⓐ	Ⓑ	Ⓒ
2.3.2	Des caméras de vidéosurveillance/VSS sont installées pour permettre de visualiser en permanence toutes les opérations et les mouvements autour de la zone de quai extérieure, sauf en cas d'obstruction temporaire due aux besoins opérationnels (par exemple, le chargement et le déchargement de camions en temps réel).	Ⓐ	Ⓑ	Ⓒ

N° de demande	Exigences / Contrôles	Niveau applicable		
2.3.3	Tous les véhicules et les personnes se trouvant aux abords des zones de quai extérieures doivent être couverts par des caméras de vidéosurveillance (CCTV/VSS) capables d'afficher clairement les informations d'identification des véhicules et de discerner les traits du visage du personnel.	Ⓐ		
2.3.4	Les véhicules et les personnes se trouvant aux abords des zones de quai extérieures doivent être couverts et visibles par des caméras de vidéosurveillance/VSS dans au moins 75 % des cas sur une journée.		Ⓑ	Ⓒ
2.3.5	Toutes les zones extérieures autour des portes de quai sont entièrement éclairées.	Ⓐ	Ⓑ	Ⓒ

2.4 Accès aux véhicules personnels

N° de demande	Exigences / Contrôles	Niveau applicable		
2.4.1	Les véhicules personnels ne sont autorisés dans les zones de manutention, d'expédition et de réception des marchandises que sur autorisation préalable, conformément à une politique documentée.	Ⓐ	Ⓑ	Ⓒ
2.4.2	Aucun parking privé à moins de 25 m / 82 pi de distance à pied des zones de quai extérieures.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S3. Murs extérieurs, toit et portes

3.1 Côtés extérieurs de l'établissement : vidéosurveillance/VSS

N° de demande.	Exigences / Contrôles	Niveau applicable		
3.1.1	Des caméras de vidéosurveillance extérieures couleur ou « jour/nuit » doivent être installées, permettant de couvrir tous les côtés extérieurs de l'établissement.	Ⓐ		
3.1.2	Un système de caméras de vidéosurveillance/VSS extérieures couleur ou « jour/nuit » doit être en place, permettant de couvrir les côtés extérieurs de l'établissement comportant des portes, des fenêtres ou d'autres ouvertures.		Ⓑ	
3.1.3	Toutes les vues du système de caméras de vidéosurveillance/VSS extérieures sont dégagées en permanence, sauf en cas d'obstruction temporaire due aux besoins opérationnels (par exemple, le chargement et le déchargement de camions en temps réel).	Ⓐ		
3.1.4	Tous les véhicules et les personnes se trouvant aux abords des installations doivent être couverts par des caméras de vidéosurveillance (CCTV/VSS) capables d'afficher clairement les informations d'identification des véhicules et de discerner les traits du visage du personnel.	Ⓐ		
3.1.5	Les véhicules et les personnes sont visibles dans au moins 75 % des enregistrements quotidiens des caméras de vidéosurveillance extérieures.		Ⓑ	

TAPA Copyright © Do Not Copy

3.2 Murs extérieurs et toiture

N° de demande	Exigences / Contrôles	Niveau applicable		
3.2.1	Les murs extérieurs et la toiture doivent être construits et entretenus de manière à résister aux intrusions et à offrir une protection physique robuste. Les matériaux utilisés doivent présenter une résistance et une durabilité suffisantes pour empêcher toute tentative d'effraction (par exemple : briques, blocs de béton, panneaux de béton préfabriqués ou panneaux sandwich haute résistance d'au moins 7 mm d'épaisseur). *Remarque : Lorsque des matériaux légers ou non structuraux sont utilisés, des mesures de Sûreté supplémentaires (telles que des treillis métalliques internes ou des systèmes de détection d'intrusion) doivent être mises en œuvre pour garantir un niveau de Sûreté équivalent.*	Ⓐ	Ⓑ	Ⓒ
3.2.2	Toutes les fenêtres ouvrantes, les aérations ou autres ouvertures dans les murs extérieurs de l'établissement, ou toute fenêtre scellée installée à moins de 3 mètres / 9 pieds 10 pouces du sol de travail dans les murs extérieurs de l'établissement, doivent être munies d'une barrière physique ou être équipées d'une alarme et reliées au système d'alarme principal.	Ⓐ	Ⓑ	
3.2.3	Toutes les fenêtres ouvrantes, les puits de lumière, les aérations, les trappes de toit et toute autre ouverture de toiture doivent être sécurisées soit par : a) une barrière physique robuste (par exemple, des barres de Sûreté , des grilles ou des couvercles renforcés), soit par : b) un dispositif de détection d'intrusion intégré au système d'alarme principal du bâtiment. Remarque : Les barrières physiques doivent être conçues pour empêcher leur retrait ou leur manipulation, et les ouvertures équipées d'alarmes doivent déclencher des alertes immédiates en cas d'accès non autorisé.	Ⓐ		
3.2.4	L'accès extérieur au toit (échelle ou escalier) doit être : verrouillé physiquement et couvert par un système de vidéosurveillance (caméras couleur ou « jour/nuit ») ou verrouillé physiquement et équipé d'une alarme.	Ⓐ		
3.2.5	L'accès extérieur au toit (échelle ou escalier) est physiquement verrouillé.		Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N° de demande	Exigences / Contrôles	Niveau applicable		
3.2.6	Toutes les portes piétonnes extérieures de l'entrepôt et des bureaux sont équipées d'alarmes anti-ouverture et reliées au système d'alarme principal. Remarque : Les portes de quai ne sont pas concernées par cette exigence ; voir la spécification 3.2.12 pour les exigences relatives aux alarmes des portes de quai.	Ⓐ	Ⓑ	Ⓒ
3.2.7	Chaque porte extérieure d'entrepôt, porte de bureau ou autre ouverture de l'établissement doit être identifiée de manière unique, porte par porte ou zone par zone, au sein du système d'alarme principal.	Ⓐ		
3.2.8	Toutes les portes extérieures de l'entrepôt sont systématiquement fermées et verrouillées lorsqu'elles ne sont pas utilisées. Le cas échéant, un système de clés/codes est mis en place.	Ⓐ	Ⓑ	
3.2.9	Les portes piétonnes donnant accès à l'extérieur de l'entrepot, ainsi que leur cadres, ne doivent pas être facilement franchissables. Si les charnières sont extérieures, elles doivent être goupillées ou soudées par points. Les portes d'entrepôt entièrement ou partiellement vitrées sont inacceptables, sauf si elles sont équipées de détecteurs de bris de verre, ou si un autre dispositif de détection local assure la protection (par exemple, infrarouge passif) et transmet une alarme directement au centre de surveillance, OU si le verre est protégé par des barreaux ou un grillage. TAPA autorisera les titulaires de certification actuels qui ne sont pas en mesure de se conformer à cette exigence à conserver leur installation actuelle jusqu'à la prochaine révision. Les nouveaux titulaires de certification ou les nouveaux sites devront se conformer à la nouvelle exigence.	Ⓐ	Ⓑ	Ⓒ
3.2.10	Les sorties de secours réservées aux situations d'urgence (ex : sorties de secours incendie) sont équipées en permanence d'un avertisseur sonore individuel ou par zone.	Ⓐ	Ⓑ	
3.2.11	Toutes les portes de quai doivent être suffisamment robustes pour dissuader et/ou retarder toute effraction à l'aide de petits outils manuels électriques/à piles.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

N° de demande	Exigences / Contrôles	Niveau applicable		
3.2.12	Portes de quai Horaires de non-utilisation : Les portes de quai sont fermées et sécurisées (désactivées électroniquement ou verrouillées physiquement). Un système d'alarme est activé pour détecter toute intrusion et déclencher une alarme reliée au système d'alarme principal. Horaires d'utilisation : Les portes de quai doivent être fermées lorsqu'elles ne sont pas utilisées. Le cas échéant, les portes à ciseaux doivent être sécurisées par un verrou mécanique coulissant et avoir une hauteur minimale de 2,4 mètres (8 pieds).	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S4. Points d'entrée et de sortie des bureaux et des entrepôts

4.1 Point(s) d'entrée visiteurs de la zone de bureaux

N° de demande	Exigences / Contrôles	Niveau applicable		
4.1.1	Les points d'entrée des visiteurs sont contrôlés par un employé/agent de Sûreté /réceptionniste formé à la délivrance des badges, aux contrôles, à l'enregistrement des entrées, à l'accueil des visiteurs, aux exigences d'escorte, etc. Une procédure doit être en place lorsque les employés enregistrent leurs propres invités et lorsque les visites ont lieu en dehors des heures d'ouverture.	Ⓐ	Ⓑ	Ⓒ
4.1.2	Les point(s) d'entrée des visiteurs dans la zone des bureaux doivent être couvert(s) par vidéosurveillance ; (caméras couleur ou « jour/nuit »). Les personnes doivent être clairement reconnaissables à tout moment.	Ⓐ	Ⓑ	
4.1.3	Alarme anti-agression (bouton panique ou alarme de contrainte) présente aux points d'entrée des visiteurs dans les bureaux et testée chaque semaine.	Ⓐ	Ⓑ	
4.1.4	Tous les visiteurs des bureaux doivent s'identifier au moyen d'une pièce d'identité officielle avec photo (permis de conduire, passeport, carte nationale d'identité, etc.). Si l'établissement accepte les identités numériques et que la législation locale l'autorise, une procédure de vérification rigoureuse (incluant l'infrastructure technique nécessaire) doit être mise en place.	Ⓐ	Ⓑ	Ⓒ
4.1.5	Tous les visiteurs des locaux doivent être enregistrés et un registre est tenu pendant au moins 30 jours. Les détails de chaque visite, tels que l'identité de la personne visitée et le motif de la visite, doivent être traçables grâce aux informations consignées dans ce registre.	Ⓐ	Ⓑ	Ⓒ
4.1.6	Tous les badges visiteurs doivent être vérifiés au moment où le visiteur quitte les lieux et le registre complet doit être contrôlé quotidiennement.	Ⓐ	Ⓑ	
4.1.7	Tous les visiteurs portent un badge ou un laissez-passer visible et sont escortés par le personnel de l'entreprise.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

4.2 Point(s) d'entrée de la main-d'œuvre

N° de demande	Exigences / Contrôles	Niveau applicable		
4.2.1	Tous les points d'entrée du personnel sont contrôlés 24h/24 et 7j/7.		Ⓑ	Ⓒ
4.2.2	Tous les points d'entrée du personnel sont contrôlés 24h/24 et 7j/7 par un dispositif de contrôle d'accès électronique. Les accès sont enregistrés.	Ⓐ		
4.2.3	Point(s) d'entrée du personnel sont couvert(s) par vidéosurveillance (caméras couleur ou « jour/nuit »).	Ⓐ	Ⓑ	
4.2.4	Tous les employés doivent recevoir un badge d'identification avec photo de l'entreprise une fois le processus de vérification terminé.	Ⓐ	Ⓑ	
4.2.5	Tous les autres employés doivent recevoir un badge d'identification de l'entreprise afin d'être identifiables au sein de l'établissement.	Ⓐ	Ⓑ	
4.2.6	Tous les badges des employés sont clairement visibles.	Ⓐ	Ⓑ	
4.2.7	Les badges d'accès pour le personnel ne doivent en aucun cas être partagés, et une politique de délivrance des badges doit être mise en place.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

4.3 Identification du conducteur et du véhicule

N° de demande	Exigences / Contrôles	Niveau applicable		
4.3.1	Tous les conducteurs doivent être identifiés au moyen d'une pièce d'identité officielle avec photo (permis de conduire, passeport, carte nationale d'identité, etc.) et un registre des conducteurs doit être tenu. Si l'établissement accepte les identités numériques et que la législation locale l'autorise, un processus de vérification rigoureux (incluant toute l'infrastructure technique requise) doit être mis en place.	Ⓐ	Ⓑ	Ⓒ

N° de demande	Exigences / Contrôles	Niveau applicable		
4.3.2	Vérification de la validité du permis de conduire et de son adéquation avec le conducteur. Si l'établissement accepte les permis de conduire numériques et que la législation locale l'autorise, une procédure de vérification rigoureuse (incluant toute l'infrastructure technique requise) doit être mise en place.	Ⓐ	Ⓑ	Ⓒ
4.3.3	Les identifiants des véhicules sont enregistrés manuellement (par écrit) ou par caméra. Il faut au minimum inclure la plaque d'immatriculation et le type de véhicule.	Ⓐ		

TAPA Copyright © Do Not Copy

S5. Entrepôt et bureaux intérieurs

5.1 Zone d'entrepôt : Murs multi-locataires

N° de demande	Exigences / Contrôles	Niveau applicable		
5.1.1	Les murs intérieurs et le toit des zones/batiments multilocataires, du sol au plafond, sont construits/conçus et entretenus pour résister à la pénétration (Exemple : murs en brique, en bloc, en dalle de béton préfabriquée, en panneaux multi-épaisseur d'une largeur minimale de 7 mm).	Ⓐ	Ⓑ	Ⓒ
5.1.2	Si les cloisons intérieures des zones/batiments multilocataires, allant du sol au plafond, sont constituées de treillis métallique de Sûreté ou d'une autre barrière de Sûreté reconnue dans le secteur, elles doivent également être équipées d'un système d'alarme anti-intrusion. Remarque 1 : Les filets, les clôtures de qualité inférieure ou les treillis non sécuritaires ne sont pas acceptables. Remarque 2 : Si les cloisons des zones/batiments multilocataires sont construites en matériau plein du sol au plafond, cette exigence ne s'applique pas.	Ⓐ	Ⓑ	Ⓒ

5.2 Zones internes de l'entrepôt

N° de demande	Exigences / Contrôles	Niveau applicable		
5.2.1	Un système de détection d'intrusion (par exemple, infrarouge, mouvement, son ou vibration) est requis pour surveiller les zones internes de l'entrepôt. Les alarmes doivent être activées et reliées au système d'alarme principal en dehors des heures d'ouverture (c'est-à-dire lorsque l'entrepôt est fermé). Remarque 1 : Si l'entrepôt fonctionne 24 h/24 et 7 j/7, cette exigence peut ne pas s'appliquer si les risques et les mesures d'atténuation sont documentés dans l'évaluation des risques locale. (Voir l'exigence 1.1.5) Remarque 2 : Quelles que soient les heures d'ouverture, un système de détection d'intrusion périmétrique ou des barrières physiques sont toujours requis sur les portes extérieures et les fenêtres du rez-de-chaussée des bureaux et de l'entrepôt. (Voir les exigences 3.2.2 et 3.2.6)	Ⓐ		

TAPA Copyright © Do Not Copy

5.3 Portes de quai intérieures et zones de quai

N° de demande	Exigences / Contrôles	Niveau applicable		
5.3.1	Toutes les portes et zones de quai internes sont couvertes par des caméras de vidéosurveillance (caméras couleur ou « jour/nuit »).	Ⓐ	Ⓑ	Ⓒ
5.3.2	Vue dégagée en permanence sur les opérations de chargement/déchargement de marchandises à toutes les portes et zones de quai internes, sauf en cas d'obstruction temporaire due aux besoins opérationnels (par exemple, chargement et déchargement de camions en temps réel).	Ⓐ	Ⓑ	Ⓒ
5.3.3	Les biens de l'acheteur sont sous surveillance vidéo à 100 % dans les zones de mouvement ou de préparation des marchandises (c.-à-d. les zones de déchargement/assemblage des palettes, les trajets vers et depuis les rayonnages de stockage, les quais, les allées de transit).	Ⓐ	Ⓑ	
5.3.4	Une analyse des angles morts pour une couverture CCTV à 100 % des mouvements de marchandises doit être effectuée au moins une fois par an, sauf en cas de modifications opérationnelles et/ou structurelles de l'entrepôt.	Ⓐ		

TAPA Copyright © Do Not Copy

5.4 Contrôle d'accès entre le bureau et le quai/entrepôt

N° de demande	Exigences / Contrôles	Niveau applicable		
5.4.1	Contrôle d'accès entre le bureau et le quai/entrepôt.	Ⓐ	Ⓑ	
5.4.2	Les alarmes des portes à badge ou à interphone, pour les portes entre le bureau et le quai/entrepôt, sont audibles localement et génèrent une alarme pour intervention lorsqu'elles sont maintenues ouvertes pendant plus de 60 secondes ou immédiatement si elles sont forcées.	Ⓐ		
5.4.3	Les alarmes de porte pour les portes entre le bureau et le quai/entrepôt sont audibles localement ou envoient une alarme pour intervention lorsqu'elles sont maintenues ouvertes pendant plus de 60 secondes ou forcées.		Ⓑ	
5.4.4	Le personnel autorisé du prestataire de services logistiques/demandeur et les visiteurs accompagnés ont accès aux zones de quai/d'entrepôt en fonction des besoins de l'entreprise et de manière restreinte.	Ⓐ	Ⓑ	Ⓒ
5.4.5	La liste des accès aux zones de quai/d'entrepôt est révisée au moins trimestriellement afin de limiter/vérifier que l'autorisation d'accès n'est accordée qu'au personnel désigné/autorisé.	Ⓐ	Ⓑ	

5.5 Zone de fret de grande valeur (HVC)

N° de demande	Exigences / Contrôles	Niveau applicable		
5.5.1	La taille et l'utilisation de la zone HVC peuvent être définies par un accord entre l'acheteur, le PSL / demandeur. En l'absence d'un tel accord, la zone HVC doit pouvoir stocker un volume minimal de 6 mètres cubes de produit.	Ⓐ	Ⓑ	
5.5.2	La zone HVC doit être grillagé ou avoir des parois rigides sur tous les côtés, y compris le dessus/toit.	Ⓐ	Ⓑ	
5.5.3	La porte/portail de la zone HVC doit être équipée d'un dispositif de verrouillage de Sûreté.	Ⓐ	Ⓑ	
5.5.4	L'entrée et l'interieure de la zone HVC doivent être entièrement couvertes par des caméras (couleur ou « jour/nuit »). Remarque : Si la zone est trop petite pour installer une caméra à l'intérieur, la couverture de l'entrée est suffisante.	Ⓐ		
5.5.5	Couverture CCTV/VSS (caméras couleur ou « jour/nuit ») à l'entrée de la zone HVC.		Ⓑ	
5.5.6	Si l'accès à la zone HVC est requis par plus de 10 personnes, le système de contrôle de son accès doit être contrôlé électroniquement par carte ou badge. Si l'accès est requis par 10 personnes ou moins, un système de verrouillage renforcé (cadenas ou serrure) associé à un système de distribution de clés contrôlé doit être mis en place. Les clés peuvent être empruntées pour assurer la relève, mais leur transfert est interdit sans autorisation préalable et doit être consigné dans le registre des clés. Toutes les clés doivent être restituées et leur présence vérifiée après chaque utilisation.	Ⓐ		
5.5.7	Les portes et portails de la zone HVC sont équipés d'alarmes pour détecter toute intrusion. Ces alarmes peuvent être déclenchées par des contacteurs de porte et/ou par un système de vidéosurveillance/détection de mouvement afin de détecter les accès non autorisés.	Ⓐ		
5.5.8	Le périmètre de la zone HVC est maintenu en bon état et inspecté mensuellement afin de vérifier son intégrité et l'absence de dommages.	Ⓐ		

TAPA Copyright © Do Not Copy

N° de demande	Exigences / Contrôles	Niveau applicable		
5.5.9	Le PSL / demandeur doit s'assurer que l'accès au système de vidéosurveillance est réservé au personnel désigné et autorisé. La liste des personnes autorisées à accéder au système de vidéosurveillance est révisée mensuellement et mise à jour en temps réel lorsqu'un employé quitte l'entreprise ou n'a plus besoin d'y accéder. Une procédure d'accès au système de vidéosurveillance est en place.	Ⓐ	Ⓑ	

5.6 Inspection des déchets de l'entrepôt

N° de demande	Exigences / Contrôles	Niveau applicable		
5.6.1	Les conteneurs à déchets principaux/zones de compactage internes et/ou externes de l'entrepôt sont surveillés par vidéosurveillance/VSS.	Ⓐ		
5.6.2	Les sacs poubelles utilisés à l'intérieur de l'entrepôt sont transparents, lorsqu'ils sont employés..		Ⓑ	Ⓒ

5.7 Préchargement et préparation

N° de demande	Exigences / Contrôles	Niveau applicable		
5.7.1	Aucun préchargement ni stationnement de camions FTL/dédiés de l'acheteur n'est autorisé à l'extérieur de l'entrepôt en dehors des heures d'ouverture, sauf accord mutuel entre l'acheteur et le PSL / demandeur. Des mesures de Sûreté alternatives doivent être mises en œuvre (par exemple, dispositifs de Sûreté supplémentaires sur les véhicules/compartiments de chargement). Remarque : « À l'extérieur de l'entrepôt » désigne les zones séparées de l'entrepôt, mais situées à l'intérieur de la cour/clôture périmétrique du PSL / demandeur.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

5.8 Fouilles des contenants personnels et fouilles à la sortie

N° de demande	Exigences / Contrôles	Niveau applicable		
5.8.1	Des procédures de Sûreté écrites définissent les modalités de contrôle des « contenants personnels » à l'intérieur de l'entrepôt. Les contenants personnels comprennent les boîtes à lunch, les sacs à dos, les glacières, les sacs à main, etc.	Ⓐ	Ⓑ	
5.8.2	Si la législation locale le permet, le PSL / demandeur doit élaborer et tenir à jour une procédure documentée relative aux contrôles de sortie. L'activation de cette procédure est à la discrétion du PSL / demandeur et/ou conformément à l'accord conclu avec l'acheteur. La procédure doit au minimum définir les critères de droit du PSL / demandeur à effectuer des contrôles en cas de nécessité, notamment en cas de suspicion de vol par le personnel. Les employés, les prestataires temporaires, les sous-traitants et les visiteurs doivent être informés de cette politique avant leur entrée dans l'entrepôt.	Ⓐ		

TAPA Copyright © Do Not Copy

5.9 Contrôle des équipements de manutention de cargaison

N° de demande.	Exigences / Contrôles	Niveau applicable		
5.9.1	Une procédure exigeant la mise hors service de tous les chariots élévateurs et autres engins de manutention motorisés en dehors des heures d'exploitation doit être en place. Remarque : Ceci n'inclut pas les transpalettes manuels.	Ⓐ	Ⓑ	

5.10 Intégrité du conteneur ou de la remorque : inspection en 7 points

N° de demande.	Exigences / Contrôles	Niveau applicable		
5.10.1	Inspection physique en 7 points réalisée sur tous les conteneurs ou remorques destinés à l'expédition et appartenant à l'acheteur : paroi avant, côtés gauche et droit, plancher, plafond/toit, portes intérieures et extérieures et mécanisme de verrouillage, châssis extérieur et dessous de caisse. Remarque : Ceci s'applique à tous les types de remorques et conteneurs sous scellés (y compris, et pas seulement, les conteneurs de fret maritime).	Ⓐ	Ⓑ	Ⓒ

5.11 Processus de remise des marchandises ; scellés de Sûreté

N° de demande	Exigences / Contrôles	Niveau applicable		
5.11.1	Sauf exemption expresse de l'acheteur, des scellés de Sûreté inviolables sont apposés sur tous les envois directs. Ces scellés doivent être certifiés conformes à la norme ISO 17712 (classification I, S ou H). Remarque : Les scellés ne sont pas requis pour les envois comportant plusieurs arrêts, compte tenu de la complexité et des risques liés au transport de plusieurs scellés par les chauffeurs.	Ⓐ	Ⓑ	Ⓒ
5.11.2	Le PSL / demandeur doit disposer de procédures documentées pour la gestion et le contrôle des scellés de Sûreté , des serrures de porte de remorque (conteneur), des verrous à goupille et autres équipements de Sûreté .	Ⓐ	Ⓑ	Ⓒ
5.11.3	Seul le personnel autorisé, c'est-à-dire les employés de l'entrepôt, est habilité à apposer ou à retirer les scellés de Sûreté . Ces derniers sont formés pour reconnaître et signaler tout scellé compromis. Le chauffeur ne doit en aucun cas apposer ou retirer les scellés, sauf dérogation accordée par l'acheteur.	Ⓐ	Ⓑ	Ⓒ
5.11.4	Procédures en place pour identifier et signaler les scellés de Sûreté compromis.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

5.12 Intégrité du chargement ; processus de validation du chargement/déchargement

N° de demande	Exigences / Contrôles	Niveau applicable		
5.12.1	Des procédures rigoureuses sont en place pour garantir le contrôle de tous les biens de l'acheteur expédiés et reçus, par un comptage manuel et/ou électronique. Le processus doit garantir que les anomalies sont systématiquement identifiées, documentées et signalées au PSL/demandeur et/ou à l'acheteur. Les enregistrements manuels et/ou électroniques doivent être recevables comme preuves. Si les chauffeurs ne sont pas présents pour assister à cette opération, l'acheteur/le PSL/le demandeur doit mettre en œuvre une méthode alternative de vérification du comptage, telle que des scans et/ou des images de vidéosurveillance/VSS, collectées et conservées spécifiquement à cette fin. Remarque : Outre les pièces manquantes, les anomalies peuvent inclure des dommages, des sangles ou des rubans adhésifs manquants, des coupures ou d'autres ouvertures évidentes, indiquant un possible vol ou un détournement.	Ⓐ	Ⓑ	Ⓒ

5.13 Collectes frauduleuses

N° de demande	Exigences / Contrôles	Niveau applicable		
5.13.1	L'identité du chauffeur routier, les documents de chargement et les informations de pré-alerte spécifiées par l'acheteur sont vérifiés avant le chargement. Une procédure doit être mise en place. Si l'établissement accepte les identités numériques et que la législation locale l'autorise, un processus de vérification rigoureux (incluant toute l'infrastructure technique requise) doit être mis en place.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S6. Systèmes de Sûreté : conception, surveillance et intervention

6.1 Poste de surveillance

N° de demande	Exigences / Contrôles	Niveau applicable		
6.1.1	Surveillance des alarmes 24h/24, 7j/7, 366j/an doit être en place via un poste de surveillance interne ou externe, protégé contre les accès non autorisés. Remarque : Les postes de surveillance peuvent être situés sur site ou hors site et appartenir à l'entreprise ou à un tiers. Dans tous les cas, l'accès doit être contrôlé par un système de contrôle d'accès électronique (badges), des serrures ou des lecteurs biométriques..	Ⓐ	Ⓑ	Ⓒ
6.1.2	Poste de surveillance pour répondre en temps réel à toutes les alarmes du système de Sûreté , 24h/24 et 7j/7, 366j/an.	Ⓐ	Ⓑ	Ⓒ
6.1.3	Le poste de surveillance accuse réception de l'activation de l'alarme et déclenche une intervention en moins de 3 minutes.	Ⓐ	Ⓑ	Ⓒ
6.1.4	Les rapports de surveillance des alarmes sont disponibles.	Ⓐ	Ⓑ	Ⓒ
6.1.5	Les procédures de réponse mises en place doivent être contrôlées.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

6.2 Système de détection d'intrusion (IDS)

N° de demande	Exigences / Contrôles	Niveau applicable		
6.2.1	Tous les systèmes IDS sont activés en dehors des heures opérationnelles et reliés au système d'alarme principal.	Ⓐ	Ⓑ	Ⓒ
6.2.2	Les enregistrements des alarmes IDS sont conservés pendant 90 jours.	Ⓐ	Ⓑ	
6.2.3	Les enregistrements des alarmes IDS sont stockés en toute sécurité et sauvegardés au moins une fois par semaine.	Ⓐ	Ⓑ	

N° de demande	Exigences / Contrôles	Niveau applicable		
6.2.4	Une procédure doit être en place pour garantir que l'accès au système de détection d'intrusion (IDS) est limité aux personnes autorisées ou aux administrateurs système. Ceci inclut les serveurs, les consoles, les contrôleurs, les panneaux de contrôle, les réseaux et les données. Les droits d'accès à l'IDS doivent être mis à jour sans délai lorsque des personnes quittent l'organisation ou changent de rôle et n'ont plus besoin d'y accéder.	Ⓐ	Ⓑ	Ⓒ
6.2.5	Une alarme doit être déclenchée en cas de coupure de courant ou de perte du système IDS. Remarque : Pour les systèmes équipés d'un système d'alimentation sans coupure (UPS), l'alarme est déclenchée en cas de défaillance de la batterie de l'UPS.	Ⓐ	Ⓑ	Ⓒ
6.2.6	Une vérification du système d'alarme IDS doit être effectuée. Remarque : Procédures de validation de l'activation des alarmes en dehors des heures de service.	Ⓐ	Ⓑ	Ⓒ
6.2.7	Alarme IDS transmise par ligne fixe ou sans fil et/ou défaillance du mode de communication.	Ⓐ	Ⓑ	
6.2.8	Système de communication de secours en place sur le dispositif IDS et/ou en cas de panne de ligne.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

6.3 Système de contrôle d'accès automatique (AACS)

N° de demande	Exigences / Contrôles	Niveau applicable		
6.3.1	Historique des transactions AACS disponible sur 90 jours. Données stockées en toute Sûreté et sauvegardées.	Ⓐ	Ⓑ	
6.3.2	Une procédure doit être en place pour garantir que l'accès à AACS soit limité aux personnes autorisées ou aux administrateurs système. Les droits d'accès doivent être mis à jour sans délai lorsque des personnes quittent l'organisation ou changent de rôle et n'ont plus besoin d'y accéder.	Ⓐ	Ⓑ	

N° de demande	Exigences / Contrôles	Niveau applicable		
6.3.3	Les rapports du système de contrôle d'accès sont examinés au moins trimestriellement afin de déceler les irrégularités ou les utilisations abusives (par exemple, tentatives infructueuses multiples, lectures erronées [carte désactivée], preuves de partage de carte permettant un accès non autorisé, etc.). Procédure en place.	Ⓐ	Ⓑ	

6.4 CCTV/VSS

N° de demande	Exigences / Contrôles	Niveau applicable		
6.4.1	Enregistrement numérique des caméras de surveillance/VSS en place.	Ⓐ	Ⓑ	Ⓒ
6.4.2	La vitesse d'enregistrement pour la vidéosurveillance/VSS est fixée à un minimum de 8 images par seconde (ips) par caméra.	Ⓐ	Ⓑ	Ⓒ
6.4.3	La fonctionnalité d'enregistrement numérique est vérifiée quotidiennement les jours d'exploitation selon la procédure établie. Enregistrements disponibles.	Ⓐ	Ⓑ	Ⓒ
6.4.4	Les enregistrements de vidéosurveillance doivent être conservés pendant au moins 30 jours lorsque la législation locale le permet. Le PSL / demandeur doit fournir la preuve de toute législation locale interdisant l'utilisation de la vidéosurveillance et/ou limitant la durée de conservation des données vidéo à moins de 30 jours.	Ⓐ	Ⓑ	Ⓒ
6.4.5	L'accès au système de vidéosurveillance (CCTV/VSS), incluant le matériel, les logiciels et le stockage des données/vidéos, est strictement contrôlé. Cette pièce doit être verrouillée si le système de stockage CCTV/VSS est installé sur site et que des contrôles d'accès sont en place.	Ⓐ	Ⓑ	Ⓒ
6.4.6	Les images des caméras de surveillance/VSS, à des fins de Sûreté , ne sont visionnées que par le personnel autorisé.	Ⓐ	Ⓑ	Ⓒ
6.4.7	Des procédures sont en place détaillant la politique de protection des données de vidéosurveillance/VSS concernant l'utilisation des images en temps réel et archivées conformément à la législation locale.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

6.5 Éclairage extérieur et intérieur

N° de demande	Exigences / Contrôles	Niveau applicable		
6.5.1	Les niveaux d'éclairage extérieur et intérieur sont suffisants pour permettre l'enregistrement d'images de vidéosurveillance/VSS de qualité suffisante pour les enquêtes et les preuves.	Ⓐ	Ⓑ	
6.5.2	L'éclairage extérieur et intérieur est suffisant pour permettre de reconnaître clairement tous les véhicules et toutes les personnes.	Ⓐ		

TAPA Copyright © Do Not Copy

S7. Formation et procédures

7.1 Procédures d'escalade

N° de demande	Exigences / Contrôles	Niveau applicable		
7.1.1	Des procédures locales sont en place pour la gestion des biens de l'acheteur, notamment un processus de signalement rapide des pertes, disparitions ou vols de ces biens. Le PSL/demandeur doit signaler tout incident à l'acheteur dans les 24 heures. Les vols manifestes sont signalés immédiatement. Ce processus est systématiquement appliqué.	Ⓐ	Ⓑ	Ⓒ
7.1.2	Une liste des contacts d'urgence est communiquée entre les acheteurs et les PSL/demandeurs pour les cas d'incidents de Sûreté . Elle est mise à jour tous les 6 mois. Elle inclut les contacts d'urgence des forces de l'ordre.	Ⓐ	Ⓑ	Ⓒ

7.2 Engagement de la direction

N° de demande	Exigences / Contrôles	Niveau applicable		
7.2.1	La direction doit élaborer, communiquer et maintenir une politique de Sûreté afin de garantir que toutes les personnes concernées (c'est-à-dire les employés et les sous-traitants) soient clairement conscientes des attentes en matière de Sûreté .	Ⓐ	Ⓑ	Ⓒ

7.3 Entraînement

N° de demande	Exigences / Contrôles	Niveau applicable		
7.3.1	Une formation à la Sûreté et à la sensibilisation aux menaces sera dispensée à tous les membres du personnel au cours des 60 premiers jours d'emploi, puis tous les 2 ans.	Ⓐ	Ⓑ	Ⓒ
7.3.2	Une formation de sensibilisation à la Sûreté de l'information axée sur la protection des données d'expédition électroniques et physiques de l'acheteur est dispensée au personnel ayant accès aux informations de l'acheteur, puis au moins tous les 2 ans, ou conformément à la législation locale si une période de recyclage plus courte est définie.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

7.4 Accès aux biens de l'acheteur

N° de demande	Exigences / Contrôles	Niveau applicable		
7.4.1	Des procédures sont mises en place pour protéger les biens de l'acheteur (c.-à-d. la cargaison) contre tout accès non autorisé par le personnel, les visiteurs, etc.	Ⓐ	Ⓑ	Ⓒ

7.5 Contrôle de l'information

N° de demande	Exigences / Contrôles	Niveau applicable		
7.5.1	L'accès aux documents d'expédition et aux informations relatives aux biens de l'acheteur est limité aux personnes qui en ont besoin. Un processus doit être mis en place pour garantir la protection des informations de l'acheteur.	Ⓐ	Ⓑ	Ⓒ
7.5.2	L'accès aux documents d'expédition et aux informations relatives aux biens de l'acheteur est surveillé et enregistré. Les procédures et les documents associés sont en place.	Ⓐ	Ⓑ	Ⓒ
7.5.3	Les documents d'expédition et tous autres documents, y compris les informations relatives aux biens de l'acheteur, sont conservés en lieu sûr jusqu'à leur destruction.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

7.6 Signalement des incidents de Sûreté

N° de demande	Exigences / Contrôles	Niveau applicable		
7.6.1	Un système de signalement et de suivi des incidents de Sûreté est en place et utilisé pour mettre en œuvre des mesures proactives.	Ⓐ	Ⓑ	

7.7 Programmes de maintenance

N° de demande	Exigences / Contrôles	Niveau applicable		
7.7.1	Des programmes de maintenance sont en place pour toutes les installations/systèmes de Sûreté techniques (physiques) afin d'assurer leur fonctionnement en permanence (par exemple, vidéosurveillance/VSS, contrôle d'accès, détection d'intrusion et éclairage).	Ⓐ	Ⓑ	Ⓒ
7.7.2	La maintenance préventive est effectuée une fois par an, ou conformément aux spécifications du fabricant.	Ⓐ	Ⓑ	Ⓒ
7.7.3	Vérifications fonctionnelles de tous les systèmes une fois par semaine et documentées, sauf en cas de défaillance du système immédiatement/automatiquement signalée ou déclenchée par une alarme.	Ⓐ	Ⓑ	
7.7.4	Une demande de réparation doit être déposée dans les 48 heures suivant la découverte du défaut. Pour toute réparation susceptible de durer plus de 24 heures, des solutions alternatives doivent être mises en œuvre.	Ⓐ	Ⓑ	

TAPA Copyright © Do Not Copy

7.8 Management des sous-traitants/fournisseurs

N° de demande	Exigences / Contrôles	Niveau applicable		
7.8.1	Le prestataire de services/demandeur doit s'assurer que tous les sous-traitants/fournisseurs connaissent et respectent les procédures de Sûreté	Ⓐ	Ⓑ	Ⓒ

7.9 Expédition et réception des dossiers

N° de demande	Exigences / Contrôles	Niveau applicable		
7.9.1	Les documents d'expédition et de réception doivent être lisibles, complets et exacts (date, heure, signatures, nom du chauffeur, du personnel d'expédition et de réception, détails et quantité de l'envoi, etc.). Les noms du chauffeur et de l'expéditeur doivent toujours être parfaitement lisibles.	Ⓐ	Ⓑ	Ⓒ

N° de demande	Exigences / Contrôles	Niveau applicable		
7.9.2	Le PSL / demandeur doit conserver les registres de toutes les collectes et les preuves de livraison pendant une période d'au moins deux ans et les mettre à la disposition des enquêteurs en cas de perte.	Ⓐ	Ⓑ	Ⓒ
7.9.3	Une preuve de livraison doit être fournie conformément à l'accord écrit entre l'acheteur et le PLS/demandeur Lorsque l'acheteur l'exige, le destinataire notifie l'expéditeur, dans le délai convenu, de la bonne réception des biens de l'acheteur. En rapprochant les détails de la réception avec ceux de la pré-alerte.	Ⓐ	Ⓑ	Ⓒ

7.10 Processus de pré-alerte en place

N° de demande	Exigences / Contrôles	Niveau applicable		
7.10.1	Lorsque l'acheteur l'exige, une procédure de pré-alerte est mise en place pour les expéditions entrantes et/ou sortantes. Les modalités de cette pré-alerte doivent être convenues entre l'acheteur et le PSL /demandeur. Les informations suggérées comprennent l'heure de départ, l'heure d'arrivée prévue, le nom du transporteur, le nom du chauffeur, les informations relatives à l'immatriculation, les informations sur l'expédition (nombre de colis, poids, numéro de connaissement, etc.) et les numéros de scellés de la remorque.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S8. Intégrité de la main-d'œuvre

8.1 Vérification des antécédents (conformément à la législation locale)

N° de demande	Exigences / Contrôles	Niveau applicable		
8.1.1	Le PSL/candidat doit se soumettre à une procédure de vérification des antécédents comprenant au minimum une enquête sur les cinq dernières années d'emploi et un casier judiciaire. Cette vérification s'applique à tous les candidats, employés et sous-traitants inclus. Le PSL/candidat devra également s'engager contractuellement à ce qu'une procédure équivalente soit appliquée par les entreprises sous-traitantes fournissant des travailleurs TAS..	Ⓐ	Ⓑ	Ⓒ
8.1.2	Le PSL / demandeur devra conclure des accords prévoyant que l'agence et/ou le sous-traitant fournissant les travailleurs temporaires (TAS) effectuent les vérifications d'antécédents requises, ou procéder lui-même à ces vérifications. Ces vérifications devront inclure un contrôle du casier judiciaire et des antécédents professionnels.	Ⓐ	Ⓑ	Ⓒ
8.1.3	Une procédure doit être en pkace pour le traitement des fausses déclarations des candidats/employés avant et après l'embauche.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

8.2 Licenciement ou réembauche du personnel

Remarque : La cessation d'emploi comprend à la fois les départs volontaires et involontaires — les membres du personnel licenciés et ceux qui ont démissionné.

N° de demande	Exigences / Contrôles	Niveau applicable		
8.2.1	Récupérer les biens matériels des employés ayant quitté l'entreprise, notamment les cartes d'identité, les badges d'accès, les clés, le matériel, les équipements informatiques et les informations sensibles. Une procédure documentée est requise.	Ⓐ	Ⓑ	Ⓒ
8.2.2	Protection des données de l'acheteur : Interdire l'accès des employés ayant quitté l'entreprise aux systèmes physiques ou électroniques, y compris ceux contenant des données de l'acheteur. Une procédure documentée est requise.	Ⓐ	Ⓑ	Ⓒ

N° de demande	Exigences / Contrôles	Niveau applicable		
8.2.3	Liste de contrôle du personnel pour l'intégration et le départ, en place pour vérification.	Ⓐ	Ⓑ	Ⓒ
8.2.4	Réembauche : Des procédures sont en place pour empêcher les PSL/candidats de réembaucher du personnel si les critères de refus ou de licenciement sont toujours valides. Remarque : Les dossiers sont examinés avant toute réembauche (par exemple : antécédents du personnel précédemment licencié ou des candidats rejetés).	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

S9. Exigences relatives aux fonctions centrales (applicables uniquement à la certification multisite)

9.1 Générale

N° de demande	Exigences / Contrôles	Niveau applicable		
9.1.1	Il existe une fonction centrale chargée de gérer le système de gestion de la Sûreté pour tous les sites, conformément au périmètre de la certification multisite.	Ⓐ	Ⓑ	Ⓒ
9.1.2	Tous les sites doivent avoir une relation juridique ou contractuelle avec la fonction centrale. Cette exigence ne s'applique pas aux sites des sous-traitants inclus dans le périmètre de la certification, conformément à la clause 4.2.2 du CFD.	Ⓐ	Ⓑ	Ⓒ
9.1.3	Un système unique de gestion de la Sûreté est mis en place afin de garantir que tous les sites du système répondent aux exigences de la norme de Sûreté TAPA applicable.	Ⓐ	Ⓑ	Ⓒ
9.1.4	La fonction centrale et son système de gestion seront soumis à des audits internes afin de garantir le respect continu des normes TAPA.	Ⓐ	Ⓑ	Ⓒ
9.1.5	La fonction centrale réalisera des audits des sites concernés afin de garantir que chaque site respecte les exigences TAPA FSR applicables. Ces audits devront être effectués à l'aide des modèles d'audit TAPA appropriés. Tous les audits annuels individuels de site devront être réalisés et mis à la disposition de l'auditeur avant le processus de certification.	Ⓐ	Ⓑ	Ⓒ
9.1.6	La fonction centrale est habilitée à exiger de tous les sites qu'ils se conforment aux normes de Sûreté TAPA et à mettre en œuvre les mesures correctives et préventives nécessaires. Remarque : Le cas échéant, ces dispositions doivent figurer dans l'accord formel conclu entre la fonction centrale et les sites.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

9.2 Politiques et procédures

N° de demande	Exigences / Contrôles	Niveau applicable		
9.2.1	La fonction centrale doit maintenir des politiques et des procédures documentées pour ses systèmes de management de la Sûreté , applicables à tous ses sites.	Ⓐ	Ⓑ	Ⓒ
9.2.2	La fonction centrale doit veiller à ce que les politiques et procédures soient correctement mises à jour, communiquées, déployées et mises en œuvre par tous les sites, selon les besoins.	Ⓐ	Ⓑ	Ⓒ
9.2.3	Les politiques et procédures doivent être maintenues et sont facilement accessibles à tous les sites, selon les besoins.	Ⓐ	Ⓑ	Ⓒ

9.3 Rapport d'audit d'auto-évaluation réalisé pour tous les sites

N° de demande	Exigences / Contrôles	Niveau applicable		
9.3.1	La fonction centrale exigera de tous les sites qu'ils procèdent à une auto-évaluation et que tous les rapports d'auto-évaluation lui soient soumis à des fins d'archivage et d'examen. Les documents devront être conservés pendant au moins deux (2) ans.	Ⓐ	Ⓑ	Ⓒ
9.3.2	La fonction centrale doit veiller à ce que toutes les SCAR issues de l'auto-évaluation et des audits soient correctement clôturées afin d'améliorer ses systèmes de management de la Sûreté .	Ⓐ	Ⓑ	Ⓒ
9.3.3	Tous les sites doivent soumettre des mises à jour et des rapports d'avancement concernant tous les SCAR en cours à la fonction centrale. Cette dernière en informera la direction du PSL / demandeur si les SCAR ne sont pas finalisés dans les délais impartis. Les documents doivent être conservés pendant au moins deux (2) ans.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

9.4 Comptes rendus d'inspections, registres (registres des visiteurs/conducteurs), inspections en 7 points

N° de demande	Exigences / Contrôles	Niveau applicable		
9.4.1	La fonction centrale doit mettre en place des procédures pour garantir que tous les sites conservent les registres des inspections, les registres des visiteurs, les registres des conducteurs et l'inspection en 7 points, etc.	Ⓐ	Ⓑ	Ⓒ

9.5 Évaluation des risques de tous les sites

N° de demande	Exigences / Contrôles	Niveau applicable		
9.5.1	La fonction centrale doit mettre en place des procédures pour garantir que des évaluations et une gestion appropriées des risques soient effectuées sur tous les sites, et ses dossiers sont conservés pendant au moins deux (2) ans.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

9.6 Plan d'implantation du site : système de vidéosurveillance/d'alarme et de surveillance vidéo.

N° de demande	Exigences / Contrôles	Niveau applicable		
9.6.1	La fonction centrale doit mettre en place des procédures garantissant que tous les sites examinent et tiennent à jour les documents relatifs à tous les systèmes de Sûreté physique, tels que la vidéosurveillance et l'agencement des alarmes.	Ⓐ	Ⓑ	Ⓒ

9.7 Enregistrements d'alarmes et de contrôle d'accès

N° de demande	Exigences / Contrôles	Niveau applicable		
9.7.1	La fonction centrale doit mettre en place des procédures garantissant que tous les systèmes d'alarme et de contrôle d'accès sont entretenus et testés afin d'assurer leur efficacité opérationnelle.	Ⓐ	Ⓑ	Ⓒ
9.7.2	La fonction centrale doit mettre en place des procédures garantissant que tous les sites conservent des enregistrements de tous les tests et incidents de détection d'intrusion et de contrôle d'accès.	Ⓐ	Ⓑ	Ⓒ

9.8 Dossiers de formation

N° de demande	Exigences / Contrôles	Niveau applicable		
9.8.1	La fonction centrale doit avoir des procédures en place pour s'assurer que tous les sites tiennent des dossiers de formation appropriés pour le suivi de la formation à la sûreté de leurs employés.	Ⓐ	Ⓑ	Ⓒ
9.8.2	La fonction centrale doit mettre en place des procédures permettant de garantir que tous les sites conservent les dossiers de formation à la Sûreté de l'ensemble du personnel. Ces dossiers doivent être conservés pendant au moins deux (2) ans.	Ⓐ	Ⓑ	Ⓒ

9.9 Dossiers de sélection/vérification

N° de demande	Exigences / Contrôles	Niveau applicable		
9.9.1	La fonction centrale doit mettre en place des procédures permettant de garantir que tous les sites procèdent à un examen régulier du filtrage et de la vérification des dossiers afin d'assurer l'intégrité et l'efficacité des systèmes de management de la Sûreté .	Ⓐ	Ⓑ	Ⓒ
9.9.2	La fonction centrale doit mettre en place des procédures permettant de garantir la conservation des dossiers d'examen, y compris leurs conclusions et les actions correctives/préventives (9.1.6). Ces dossiers seront conservés pendant au moins deux (2) ans.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

9.10 Revue de direction pour évaluer les auto-audits ; les SCAR (actions correctives et préventives) soulevées ; les pertes et vols ; les évaluations des risques

N° de demande	Exigences / Contrôles	Niveau applicable		
9.10.1	La fonction centrale doit, au minimum, procéder à un examen régulier de la direction afin de garantir la conformité, l'efficacité et l'amélioration de ses systèmes de management de la Sûreté .	Ⓐ	Ⓑ	Ⓒ
9.10.2	Les revues de direction doivent notamment porter sur l'efficacité des auto-audits, la clôture des SCAR, les évaluations des risques, les incidents et les actions d'amélioration.	Ⓐ	Ⓑ	Ⓒ

N° de demande	Exigences / Contrôles	Niveau applicable		
9.10.3	La fonction centrale doit conserver les dossiers de toutes les revues de gestion pendant au moins deux (2) ans.	Ⓐ	Ⓑ	Ⓒ

TAPA Copyright © Do Not Copy

8.0 Menaces informatiques et de cybersécurité – Option améliorée

Le référentiel FSR inclut des améliorations optionnelles en matière de sécurité informatique et de cybersécurité , offrant un niveau de protection supérieur et pouvant être utilisées en complément des modules. Ces améliorations optionnelles sont destinées à être sélectionnées par le PSL/demandeur et/ou son acheteur en fonction de leurs exigences supplémentaires en matière de Sûreté opérationnelle. Lorsqu'elles sont sélectionnées lors de l'évaluation préalable à la certification, toutes les exigences deviennent obligatoires.

L'option renforcée du référentiel FSR de TAPA fournit un niveau de contrôle de base en matière de Sûreté informatique et de cybersécurité au niveau du site. Les membres sont fortement encouragés à adopter les normes de cybersécurité (CSS) afin de mettre en place un cadre de cybersécurité plus complet et plus robuste.

TAPA Copyright © Do Not Copy

E8. Exigences obligatoires

N° de demande	Exigences / Contrôles
E8.1.1	Le PSL / demandeur doit disposer de politiques de Sûreté informatique et de cybersécurité . Ces politiques peuvent être présentées séparément ou dans un document unique. Elles doivent préciser : 1. Les actions entreprises par le PSL / demandeur pour identifier les menaces et y répondre. 2. Les politiques et procédures mises en place pour protéger, détecter, tester et gérer les incidents de Sûreté . 3. Les méthodes de restauration des systèmes informatiques et/ou des données. 4. Le protocole de communication avec les acheteurs/clients afin de minimiser l'impact sur la chaîne d'approvisionnement dans les 24 heures suivant la connaissance d'un incident. 5. La manière dont ces politiques sont révisées annuellement et mises à jour le cas échéant.
E8.1.2	Le PSL / le demandeur doit dispenser une formation de sensibilisation à la Sûreté de l'information à tous les employés. Cette formation doit : 1. Couvrir les rôles et responsabilités des utilisateurs d'ordinateurs en matière de Sûreté et les avantages qui en découlent. 2. Mettre en place un système garantissant la conservation des dossiers des personnes ayant suivi la formation pendant au moins deux ans.

E8.1.3	Le PSL / demandeur doit disposer d'une politique écrite garantissant la mise en place de mesures de cybersécurité auprès de ses sous-traitants et/ou fournisseurs, et ce, afin de garantir : 1. La communication des exigences de cybersécurité du PSL / demandeur aux sous-traitants et/ou fournisseurs et leur intégration dans les contrats. 2. La mise en place de mesures documentées et appliquées lorsque les sous-traitants et/ou fournisseurs ne reconnaissent pas ou refusent d'adopter les exigences de cybersécurité, afin d'atténuer les risques pour la Sûreté du PSL / demandeur et pour ses clients.
E8.1.4	Le PSL/demandeur doit disposer d'un plan d'atténuation des interruptions de courant (par exemple, une alimentation électrique alternative ou un générateur de secours) qui garantit l'acheminement de l'énergie vers les systèmes informatiques critiques (identifiés dans l'évaluation des risques locaux) pendant au moins 48 heures.
E8.1.5	Les systèmes d'information du PSL/ demandeur doivent être équipés d'un logiciel antivirus et antimalware sous licence. Ce logiciel doit être à jour.
E8.1.6	Le PSL / demandeur doit disposer d'un plan de reprise après sinistre informatique (PRS) approprié pour se remettre d'attaques de systèmes compromis, y compris, mais sans s'y limiter, toutes les dispositions nécessaires en matière de sauvegarde et de récupération des données et des logiciels.
E8.1.7	Les systèmes d'information du PSL / demandeur doivent être sauvegardés. Ces sauvegardes doivent être testées régulièrement, et les données de sauvegarde doivent être chiffrées et transférées vers un emplacement secondaire hors site.
E8.1.8	Le PSl / demandeur doivent mettre en œuvre une politique de gestion et de contrôle d'accès aux systèmes d'information pour tous les comptes utilisateurs, en utilisant des identifiants uniques et des mots de passe robustes. Les procédures suivantes doivent être mises en place pour garantir : 1. Un programme d'audit de conformité des mots de passe est en place. 2. Un mot de passe initial unique doit être attribué à chaque nouveau compte lors de sa création. 3. Les mots de passe initiaux ne peuvent contenir le nom de l'utilisateur, son numéro d'identification ni suivre un modèle standard basé sur ses informations personnelles. 4. Les mots de passe seront communiqués aux utilisateurs de manière sécurisée, et uniquement après validation de leur identité. 5. Les utilisateurs doivent être tenus de modifier leur mot de passe lors de leur première connexion. 6. Les mots de passe doivent être modifiés au moins tous les 90 jours.

TAPA Copyright © Do Not Copy

À titre d'information : la traduction du Standard dans la langue nationale mise à votre disposition a pour objectif de faciliter la compréhension des exigences TAPA 2026. Cette traduction a été réalisée et validée au mieux de nos connaissances et en tenant compte des éléments de référence nécessaires. Toutefois, la version originale anglaise du Standard concerné demeure la seule version faisant foi aux fins de l'audit.

Informations sur l'édition et le droit d'auteur
Ce document est publié par la Transported Asset Protection Association (TAPA).

© TAPA 2026–2029

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire, transmise sous quelque forme ou par quelque moyen que ce soit — électronique, mécanique, photocopie, enregistrement ou autre — sans l'autorisation écrite préalable de TAPA, sauf dans les conditions prévues par la législation applicable en matière de droit d'auteur.

La mention de droit d'auteur figurant dans ce document indique l'année de sa dernière publication.

Historique de publication
Première publication : septembre 2026

Présente édition publiée en : septembre 2026

Cette spécification accessible au public (PAS) entrera en vigueur le 15 septembre 2026.

Statut de ce document
Ce document représente les exigences de Sûreté des installations (FSR) de TAPA – Révision 2026 et établit les exigences minimales en matière de Sûreté des installations dans le cadre de la certification TAPA.
Ce document reste valide jusqu'à son remplacement, sa révision ou son retrait par TAPA.
TAPA pourra publier ultérieurement des révisions, des mises à jour ou des amendements afin de tenir compte de l'évolution des menaces à la Sûreté , des pratiques du secteur et des développements technologiques..

Utilisation de ce document
La conformité à cette spécification peut être utilisée dans le cadre du processus de certification TAPA pour les installations manipulant des marchandises de grande valeur et sensibles au vol.
Les organisations mettant en œuvre cette spécification sont responsables du respect de toutes les exigences légales, réglementaires et opérationnelles applicables aux exigences décrites dans ce document.

TAPA Copyright © Do Not Copy