Statut UPU: **2**

Date d'adoption de ce statut: **16 février 2016**

Date d'approbation de cette version: **19 avril 2021**

Sécurité postale – Mesures de sûreté générales

Les normes de sûreté de l'UPU sont actualisées dans leur intégralité. **Chaque mise à jour donne lieu à une nouvelle version, dont le numéro suit celui de la norme**. **Avant d'utiliser ce document, merci de vous assurer de sa validité en consultant le Catalogue des normes de l'UPU, disponible gratuitement sur le site Web de l'UPU (www.upu.int)**.

Clause de non-responsabilité

Le présent document contient les informations les plus récentes disponibles au moment de la publication. L'UPU n'offre aucune garantie, expresse ou implicite, concernant l'exactitude, le caractère suffisant, la valeur commerciale ou l'adéquation des informations contenues dans le présent document. Toute utilisation en étant faite est donc entièrement aux risques et pour le compte de l'utilisateur.

Avertissement – Propriété intellectuelle

L'UPU souligne que la mise en œuvre de cette norme pourrait donner lieu à l'utilisation d'un droit de propriété intellectuelle revendiqué. Les destinataires du présent document sont invités à présenter, avec leurs commentaires, toute information concernant des droits de propriété intellectuelle dont ils auraient connaissance, et à fournir des justificatifs.

A la date d'approbation de la norme, l'UPU n'avait reçu aucune information concernant de tels droits de propriété intellectuelle, à l'exception des indications fournies dans la présente publication. Toutefois, l'UPU rejette toute responsabilité découlant de l'existence de droits de propriété intellectuelle détenus par des tiers et matérialisés dans leur totalité ou en partie dans les normes de l'UPU.

Avis concernant les droits d'auteur

Union postale universelle
Programme «Normalisation»
Weltpoststrasse 4
3015 BERNE
SUISSE

Téléphone: (+41 31) 350 31 11
Télécopie: (+41 31) 350 31 10
Adresse électronique: standards@upu.int

Table des matières Page

Avant-propos

Les services postaux font partie de la vie quotidienne des habitants du monde entier. L'Union postale universelle (UPU) est l'institution spécialisée des Nations Unies chargée de réglementer le service postal universel. Les services postaux de ses 192 Pays-membres constituent le plus vaste réseau de distribution physique du monde. Plus de 5 millions d'employés postaux, travaillant dans plus de 660 000 bureaux de poste dans le monde entier, traitent un total de 434 milliards d'envois de la poste aux lettres au niveau national et plus de 5,5 milliards de ces envois au niveau international chaque année. En outre, plus de 6 milliards de colis sont expédiés par la poste tous les ans. Suivant le rythme des changements sur le marché des communications, les opérateurs désignés utilisent de plus en plus les nouvelles technologies de l'information et de la communication pour aller au-delà de ce que l'on considère traditionnellement comme leur secteur d'activité essentiel. Elles répondent aux exigences accrues des clients avec une gamme élargie de produits et de services à valeur ajoutée.

La normalisation est une importante condition préalable à une exploitation postale efficace et à l'interconnectivité du réseau postal universel. Le Groupe «Normalisation» de l'UPU élabore et gère un nombre croissant de normes pour améliorer les échanges d'informations entre les opérateurs désignés. Il s'assure également de la compatibilité des initiatives de l'UPU et des autres entités postales internationales. Il travaille en étroite collaboration avec les postes, les clients, les fournisseurs et d'autres partenaires, y compris différentes organisations internationales. Le Groupe «Normalisation» veille à la mise en place de normes cohérentes dans des domaines tels que l'échange de données informatisé (EDI), le codage du courrier, les formules postales et l'oblitération.

Les normes de l'UPU sont rédigées conformément aux règles énoncées dans la partie V du document «Informations générales sur les normes de l'UPU» et sont publiées par le Bureau international conformément à la partie VII de ce document.

L'UPU reconnaît que la sécurité et la sûreté du secteur postal sont essentielles pour permettre le commerce, les communications et la sûreté des transports au niveau international. Afin de faciliter l'élaboration de normes de sûreté et de pratiques recommandées pour adoption par les opérateurs désignés, l'UPU a créé le Groupe «Sécurité postale» (GSP).

Ce groupe réunit des experts en matière de sûreté issus d'un certain nombre de Pays-membres de l'UPU et est chargé d'élaborer des stratégies de sûreté mondiales et régionales pour aider les opérateurs désignés à remplir leur mission en la matière. Le GSP s'efforce, par des actions de formation, des missions de conseil et des programmes de prévention, de protéger les employés et les avoirs des opérateurs désignés, ainsi que de prévenir toute forme de fraude, de spoliation ou d'utilisation abusive du courrier.

Il s'agit de la quatrième version du document. La modification apportée à la version précédente, indiquée par une barre verticale dans la marge, correspond à l'ajout d'informations sur le Cadre de normes SAFE de l'Organisation mondiale des douanes (OMD) pour refléter le fait que les normes de l'UPU en matière de sécurité sont conformes audit cadre.

Introduction

L'un des objectifs du Groupe «Sécurité postale» (GSP) est d'améliorer la sûreté de toutes les opérations au sein du secteur postal. Le GSP, en collaboration avec d'autres interlocuteurs de l'UPU, a défini un ensemble minimal d'exigences en matière de sûreté applicables à tous les aspects du secteur. Le fait d'élaborer des normes de sûreté quantifiables pour le secteur postal contribue à la protection des employés, des biens et des envois postaux en général, participe à la sûreté du transport utilisé pour acheminer les envois et permet aux autorités nationales et internationales d'utiliser des outils d'évaluation des risques.

Les normes de sûreté physique et de sûreté des opérations élaborées dans le cadre du GSP sont applicables aux installations principales du réseau postal. Lors de la publication de ce document, les normes sont les suivantes:

– Norme S58 (Normes de sûreté postale – Mesures de sûreté générale) (présent document): définit les exigences minimales en matière de sûreté physique et de sûreté des opérations applicables aux installations principales du réseau postal.
– Norme S59 (Normes de sûreté postale – Sûreté des bureaux d'échange et du courrier-avion international): définit les exigences minimales relatives aux opérations de sûreté pour le transport du courrier-avion international.

Remarque: pour que l'application de la norme S59 soit obligatoire, la norme S58 doit également être mise en œuvre. Seuls des agents habilités, au sens de l'Organisation de l'aviation civile internationale (OACI) dans l'annexe 17 de la Convention relative à l'aviation civile internationale, peuvent procéder à des inspections.

Normes de sûreté postale – Sécurité postale. Mesures de sûreté générales

1. Champ d'application

Le présent document définit les exigences minimales en matière de sûreté physique et de sûreté des opérations applicables aux installations principales du réseau postal.

Remarque 1: les opérateurs désignés sont chargés de vérifier la conformité par rapport à l'ensemble de la législation nationale, de la réglementation, etc.

Les opérateurs désignés et les parties de la chaîne logistique peuvent apporter des preuves du fait qu'ils respectent le Programme national de sûreté de l'aviation civile ou les programmes de certification de sûreté reconnus à l'échelle internationale, tels que le Cadre de normes SAFE de l'OMD, considérés comme respectant les exigences des normes S58 et S59 de l'UPU.

Remarque 2: le Cadre de normes SAFE établit les principes et les normes à adopter comme seuil minimal par les membres de l'OMD. Les lignes directrices en matière de sûreté et de sécurité applicables aux opérations postales et contenues dans les normes S58 et S59 de l'UPU sont cohérentes avec le Cadre de normes SAFE.

2. Références normatives

Les documents référencés ci-dessous sont indispensables à l'application des présentes. Pour les références comportant une date ou un numéro de version, seule l'édition citée s'applique. Pour les références sans date et ne comportant pas de numéro de version, la dernière édition du document référencé (y compris ses éventuelles modifications) s'applique.

Organisation de l'aviation civile internationale, Instructions techniques pour la sécurité du transport aérien des marchandises dangereuses (Doc 9284).

Remarque: les demandes de copies des publications de l'OACI doivent être adressées directement au Groupe de la vente des documents de l'OACI: sales@icao.int.

3. Termes et définitions

Un certain nombre de termes communément utilisés dans le présent document sont définis dans le glossaire des normes de l'UPU et dans des documents cités dans les normes de référence et dans la bibliographie. Les définitions des termes fréquemment utilisés ou particulièrement importants, ainsi que celles d'autres termes figurant dans le présent document, sont indiquées ci-après.

3.1 Contrôle d'accès

En matière de sûreté physique, le terme «contrôle d'accès» fait référence à la pratique consistant à limiter l'entrée d'une propriété, d'un bâtiment ou d'une salle à un certain nombre de personnes autorisées.

Remarque: le contrôle de l'accès physique peut s'effectuer par l'intermédiaire d'une personne (un agent de sûreté ou un réceptionniste), par des moyens mécaniques (serrures et clés) ou par des moyens technologiques (système de carte).

3.2 Installation principale

Bureau d'échange; centre aéropostal; installations postales où ont lieu les contrôles de sûreté aérienne; dernière installation postale par laquelle transitent les envois postaux avant d'être expédiés par voie aérienne.

3.3 Opérateur désigné

Toute entité gouvernementale ou non gouvernementale désignée officiellement par le Pays-membre pour assurer l'exploitation des services postaux et remplir les obligations y relatives découlant des Actes de l'Union sur son territoire.

3.4 Exigence minimale en matière de sûreté

Technique, méthode, processus ou activité composés des mesures minimales à prendre pour sécuriser les opérations au sein de l'installation principale en ce qui concerne la législation locale, les politiques internes et les procédures.

3.5 Inspection

Examen du courrier par des moyens techniques ou d'autres moyens non intrusifs afin d'identifier ou de déceler des explosifs.

3.6 Système d'accès unique

Caractéristiques physiques des systèmes de contrôle d'accès limitant l'entrée des personnes non autorisées en permettant l'accès d'une seule personne à la zone contrôlée avant la fermeture des portes. Ce système doit permettre d'éviter l'accès par usurpation d'identité ainsi que le passage des employés non autorisés, et ce sans intervention humaine.

Remarque: pour ce faire, des tourniquets sont généralement utilisés, ou encore des portes à doubles battants ou des capteurs spécialisés.

4. Sigles et abréviations

CCTV	Système de télévision en circuit fermé
OD	Opérateur désigné
OACI	Organisation de l'aviation civile internationale
PNSAC	Programme national de sûreté de l'aviation civile
GSP	Groupe «Sécurité postale»

5. Normes de sûreté des installations principales

5.1 Informations générales concernant les mesures de sûreté physique

Les mesures de sûreté physique relatives aux installations postales principales devraient comprendre, selon les cas, une combinaison de différentes mesures de sûreté (barrières périmétriques, éclairage, dispositifs de verrouillage et systèmes de contrôle des clés, agents de sûreté en uniforme et reconnaissables, système de télévision en circuit fermé et systèmes d'alarme/de détection d'intrus).

5.1.1 Évaluation des risques et plans de sûreté des installations

Une évaluation des risques doit avoir lieu tous les ans pour identifier chaque installation principale. Cette évaluation doit tenir compte des avoirs de la poste, des opérations menées dans l'installation concernée, du taux de criminalité général dans la zone considérée et d'autres facteurs susceptibles de renforcer les possibilités de délits.

Pour chaque installation principale, un plan de sûreté détaillé doit être rédigé et tenu à jour. Le plan de sûreté d'une installation contient toutes les mesures de contrôle suivantes:

– Normes de conception de l'installation principale.
– Barrières périmétriques.
– Fenêtres, portes ou autres ouvertures périmétriques.
– Éclairage.
– Dispositifs de verrouillage et systèmes de contrôle des clés.
– Mesures de contrôle d'accès.

5.1.2 Normes de conception de l'installation principale

Toutes les installations doivent être construites selon les normes nationales de sûreté relatives à la conception des bâtiments. Des matériaux résilients doivent être utilisés afin d'empêcher tout accès non autorisé.

Un programme spécial d'inspection et de réparations annuelles doit être mis en place pour assurer l'intégrité des structures; il doit comprendre les délais de réalisation des éventuelles réparations. L'inspection annuelle doit également comprendre une évaluation des risques des environs, le profil du produit postal traité dans l'installation ainsi que les éventuelles autres modifications de fonctionnement pouvant avoir des conséquences sur la sûreté du bâtiment et de ses employés.

Les zones réservées doivent être facilement identifiables, signalées comme il se doit et sécurisées par les mesures de contrôle d'accès qui s'imposent.

5.1.3 Barrières périmétriques

Des barrières physiques, par exemple des grillages, des murs et des portails pour les véhicules, doivent être installées pour empêcher l'accès de personnes ou de véhicules non autorisés aux zones réservées de l'installation principale.

Les clôtures de périmètre ou les murs de séparation doivent être installés à une certaine distance de l'installation pour permettre la surveillance des intrus tentant de pénétrer dans les zones réservées.

Les zones adjacentes aux clôtures de périmètre ne doivent pas être encombrées de débris, d'arbres ni de bosquets, car ces éléments pourraient être utilisés pour pénétrer dans la zone sécurisée.

Des inspections hebdomadaires des barrières périmétriques doivent avoir lieu pour s'assurer de leur intégrité.

5.1.4 Fenêtres, portes ou autres ouvertures périmétriques

Toutes les portes extérieures doivent être suffisamment solides pour empêcher ou retarder un accès par la force à l'aide d'outils manuels ou d'autres moyens d'agression.

Il doit y avoir le moins de portes possible pour assurer un accès adéquat aux zones sécurisées de l'installation, sans oublier les sorties de secours.

Des panneaux et des pancartes doivent être disposés sur les portes extérieures afin d'indiquer quelles sont les zones réservées, sauf si cela représente une obstruction visible ou si la réglementation locale ne le permet pas. Si nécessaire, des panneaux décrivant les responsabilités et les procédures d'information des autorités doivent être bien visibles au cas où des actes criminels seraient commis dans l'installation.

Toutes les fenêtres, portes et autres ouvertures extérieures doivent être sécurisées à l'aide des mécanismes de verrouillage appropriés.

L'évaluation des risques de l'installation peut relever la nécessité de mesures de sûreté supplémentaires, par exemple des fenêtres équipées de barrières, de grillage ou de tout autre dispositif visant à renforcer la sûreté du point d'accès contre toute entrée non autorisée.

5.1.5 Éclairage

Des systèmes d'éclairage adéquats doivent être installés dans toutes les zones piétonnes, dans les zones d'entrée/de sortie des véhicules, sur les aires de travail extérieures, sur les parkings et le long des clôtures ou des murs périmétriques. L'éclairage doit être suffisant pour identifier les personnes ou les véhicules situés à proximité. L'installation de dispositifs d'éclairage dans les zones situées à proximité des aéroports ou des voies de circulation doit respecter les normes de l'aviation civile/de l'aéroport.

Si un système de télévision en circuit fermé est utilisé, il convient d'envisager d'éclairer les zones intérieures, notamment les locaux d'entreposage opérationnel.

Un éclairage d'urgence doit être installé dans les zones opérationnelles essentielles.

5.1.6 Dispositifs de verrouillage et systèmes de contrôle des clés

Tous les dispositifs de verrouillage pour les points d'entrée/de sortie des piétons ou des véhicules doivent être conçus à partir de matériaux renforcés, afin d'empêcher l'accès de personnes non autorisées.

Un système de contrôle des clés doit être mis en place pour assurer une responsabilisation des détenteurs de clés.

Le système doit permettre d'enregistrer les données relatives à la distribution des clés et de protéger l'accès aux clés non distribuées.

Ce système doit être géré par l'unité chargée de la sûreté postale ou par les responsables des établissements postaux concernés.

5.2 Mesures de contrôle d'accès

5.2.1 Informations générales

Les mesures de contrôle d'accès empêchent l'accès non autorisé au courrier et aux véhicules utilisés pour l'acheminement du courrier dans les installations principales. Le contrôle d'accès à toutes les installations principales doit absolument être d'un niveau adéquat afin de protéger les avoirs des postes.

Remarque: les mesures de contrôle d'accès peuvent être manuelles, avec des agents de sûreté fixes postés aux points d'entrée/de sortie pour vérifier l'identité des personnes ou des véhicules entrant dans la zone sécurisée. Les mesures de contrôle d'accès peuvent également être fondées sur des systèmes électroniques simples ou complexes utilisés pour effectuer des vérifications et permettre l'accès aux zones sécurisées. Indépendamment des aspects technologiques liés aux méthodes utilisées, le système doit être capable de filtrer adéquatement les individus à tous les points d'entrée et de différencier les divers types d'accès privilégié selon que les personnes concernées sont des employés, des visiteurs, des prestataires de services ou des fournisseurs. Le système de contrôle d'accès d'une installation principale doit être segmenté afin de garantir que les employés, les visiteurs, les fournisseurs de services et les vendeurs bénéficient uniquement d'un accès aux zones où ils sont appelés à se rendre dans le cadre de leurs fonctions et de leurs activités.

5.2.2 Systèmes de contrôle d'accès pour les employés, les visiteurs, les prestataires de services et les fournisseurs

Une procédure adéquate de contrôle d'accès doit être mise en place dans les zones sécurisées (interdites aux clients) de toutes les installations postales principales. Au moins un des éléments ci-après doit être appliqué:

1º Système de contrôle d'accès manuel:

a) Des agents de sûreté en uniforme, un réceptionniste ou tout autre membre du personnel doivent être postés aux points d'entrée/de sortie afin de vérifier les privilèges d'accès de chaque personne.

b) Le processus manuel doit être documenté sous la forme d'une procédure d'exploitation normalisée.

c) Il faut assurer une formation et donner des instructions au personnel chargé de gérer le système et aux employés placés aux points de contrôle d'accès fixes.

d) Un système d'enregistrement doit être utilisé pour conserver les données relatives à l'accès des personnes autres que les employés dans les zones sécurisées de l'installation principale.

2º Système de contrôle d'accès automatisé (électronique).

Remarque 1: il convient d'envisager de limiter les effets personnels et de mettre en place des procédures de fouille.

Le système doit être conçu pour interdire l'accès non autorisé de personnes par les points d'entrée/de sortie, grâce à un système ou à une procédure d'accès unique. Il doit s'agir d'un système laissant passer uniquement le détenteur du badge qui active le point d'accès.

Remarque 2: le système d'accès unique peut également être mis en place par l'affectation à un poste fixe d'un agent de sûreté en uniforme ou d'un autre employé chargé de contrôler les entrées/sorties au point d'accès. Si le point d'entrée/de sortie n'est pas surveillé, un système de contrôle de l'accès physique (tourniquets, portes et portails d'accès), activé par des lecteurs de badges ou des clés électroniques, doit être utilisé.

Un système d'enregistrement des visiteurs doit être mis en œuvre pour conserver les données relatives à l'accès des personnes autres que les employés dans les zones sécurisées de l'installation principale.

5.2.3 Systèmes de contrôle d'accès pour les véhicules

Seuls les véhicules officiels et les véhicules approuvés des contractants doivent être autorisés dans les zones utilisées pour le chargement/le transport du courrier ou dans les autres zones extérieures sécurisées.

L'accès à ces zones doit être clairement indiqué, notamment grâce à des pancartes, pour faire connaître les limites de la zone réservée.

Un système de contrôle d'accès manuel ou automatisé doit être utilisé pour que les véhicules non autorisés ne puissent pas accéder à la zone extérieure sécurisée.

Si un véhicule non officiel ou tiers doit entrer dans la zone extérieure sécurisée, il faut appliquer une procédure afin de vérifier l'identité du chauffeur et, le cas échéant, inspecter le véhicule avant qu'il ne pénètre dans la zone sécurisée.

Les places de parking des employés doivent se situer dans une zone autre que la zone réservée aux véhicules officiels.

Les places de parking réservées aux visiteurs doivent être séparées des zones sécurisées réservées aux véhicules officiels.

5.2.4 Systèmes d'identification

Un système d'identification des employés et des visiteurs doit être mis en place pour connaître avec certitude l'identité des employés et des visiteurs pénétrant dans l'installation principale.

Le personnel postal (fixe, temporaire ou sous contrat) doit recevoir un badge permettant une identification facile et indiquant le nom juridique de la personne tel qu'il est enregistré dans le système des ressources humaines, une photographie et une date d'expiration. D'autres informations, comme le niveau d'accès, le département ou l'unité, peuvent être ajoutées en fonction de la réglementation et de la législation locales.

L'unité chargée de la sûreté postale ou d'autres responsables postaux doivent assurer le contrôle, l'émission et le retrait des badges d'identification destinés aux employés, aux visiteurs et aux contractants. Une procédure doit être suivie pour la déclaration et la communication des informations sur les employés.

Un système doit être utilisé pour inspecter et identifier tous les véhicules avant leur entrée dans les zones extérieures sécurisées.

6. Sûreté et formation du personnel

6.1 Informations générales

Les employés sont indispensables aux opérations postales; il est donc fondamental pour les opérateurs de minimiser les éventuels risques pour la sûreté que représentent de nouveaux employés ou prestataires de services, de même que ceux qui découlent du redéploiement des employés à des postes nécessitant un contrôle ou une formation différents. La sûreté et la formation du personnel doivent être organisées de façon à réduire et à minimiser les risques pour la sûreté des opérations, des clients et des employés.

6.2 Sûreté du personnel et procédures de recrutement

La politique de sélection et de recrutement du personnel doit être documentée pour tous les employés travaillant dans les installations de l'OD ou s'occupant du traitement du courrier sur des sites externes.

La politique de recrutement doit être conforme à la législation nationale afin de veiller à ce que les employés et les contractants actuels et futurs soient suffisamment qualifiés pour remplir leurs tâches postales de manière intègre.

Les employés fixes doivent faire l'objet d'une enquête de fond (vérification des antécédents criminels ou policiers), conformément aux dispositions de la législation nationale.

Une procédure doit être suivie pour la déclaration et la communication des performances et des fautes des employés.

La procédure d'embauche comprend des entretiens, une vérification des données avant l'embauche et d'autres mesures de contrôle, en fonction du poste ou des fonctions à pourvoir.

La résiliation du contrat d'un employé ou d'un contractant doit être bien documentée.

La procédure de résiliation doit veiller au retour en temps opportun des documents d'identification, des dispositifs de contrôle d'accès, des clés, des uniformes et d'autres informations sensibles.

Un système d'enregistrement doit être alimenté afin d'empêcher la réintégration d'un employé ou d'un contractant congédié pour faute.

6.3 Exigences en matière de sûreté concernant les contractants

Les contractants habitués à effectuer des opérations de traitement/de transport du courrier ou à remplir d'autres fonctions délicates doivent mettre en place des mesures de sûreté du personnel analogues à celles de l'OD, conformément au contenu de la section 6.2.

Le contractant doit communiquer à l'OD les éventuelles conclusions ou décisions relatives aux employés pouvant potentiellement représenter un risque pour la sûreté des opérations.

6.4 Mesures de sensibilisation et de formation

Un programme de formation et de sensibilisation aux questions de sûreté doit être documenté et maintenu pour l'ensemble des employés et des contractants.

7. Transport et consignes de sûreté pour les opérateurs désignés et les contractants postaux

L'OD et les contractants autorisés doivent s'appuyer sur des procédures bien documentées permettant de protéger la sûreté du courrier, quel que soit son mode de transport (avion, route, voie maritime et chemin de fer). L'OD doit respecter toutes les dispositions applicables de la législation nationale relatives aux normes de transport.

L'accès au courrier doit être limité, en fonction des besoins, aux employés des postes ou aux contractants chargés de traiter le courrier.

Les véhicules de transport du courrier doivent être conçus avec des matériaux résilients et posséder certaines caractéristiques comme un toit solide, des parois rigides ou des parois souples renforcées, ainsi que des portes de chargement pouvant être verrouillées. Les véhicules doivent être inspectés avant le chargement, et les signes éventuels d'altération doivent être signalés.

Lorsque les véhicules transportant le courrier sont en transit ou sont laissés sans surveillance en dehors des locaux sécurisés des postes ou des contractants, ils doivent être verrouillés, de même que tous les points d'accès au courrier.

Les véhicules ou les moyens de transport doivent si possible porter une mention claire indiquant qu'il s'agit de véhicules postaux autorisés ou de véhicules sous contrat de la poste.

Les opérateurs chargés du transport (qu'il s'agisse d'OD ou de contractants) doivent si possible porter un uniforme des postes et/ou posséder et exposer clairement une identification postale ou du contractant valide, sous quelque forme que ce soit.

La cabine du véhicule et les clés de contact de tous les moyens de transport doivent être protégées pour éviter tout accès non autorisé.

Un processus de responsabilisation doit être mis en place.

Les itinéraires, les horaires et les arrêts prévus doivent faire l'objet d'une évaluation des risques et, si nécessaire, des mesures de sûreté supplémentaires doivent être prises.

Les véhicules, les moyens de transport ou les conteneurs doivent être correctement vidés.

8. Programme de vérification de la conformité et contrôle

Une vérification de la conformité doit être effectuée tous les ans par du personnel extérieur à l'équipe de gestion de l'installation principale.

Ces personnes doivent disposer de l'autorité nécessaire pour obtenir les informations utiles et pour mettre en œuvre des mesures correctives.

Le programme de vérification de la conformité couvre l'ensemble du programme de sûreté du courrier pour s'assurer du respect des exigences en matière de sûreté. Ce programme doit mettre l'accent, entre autres, sur les éléments suivants:

– Sûreté des installations.
– Sûreté du personnel.
– Sûreté du transport.

L'OD doit veiller à ce que la gestion du programme de vérification de la conformité soit confiée à des personnes n'ayant aucune responsabilité dans l'application des exigences de sûreté.

Il convient de tenir des dossiers des vérifications de la conformité et des recommandations.

Les résultats des vérifications de conformité doivent être transmis à la direction exécutive de l'OD. Les actions de suivi doivent être surveillées et documentées.

9. Unité de sûreté postale pour la prévention et le contrôle

9.1 Unité de sûreté postale pour la prévention et le contrôle (exigence minimale en matière de sûreté)

L'OD doit disposer d'un programme de sûreté documenté couvrant tous les domaines de la prévention et des enquêtes relatives à la protection du courrier, des employés, des partenaires, des clients et des avoirs postaux. Ce programme doit être communiqué à tous les employés.

Exemple: équipement, véhicules, uniformes, technologies de l'information, etc.

L'OD doit pouvoir compter sur une unité de sûreté postale ou sur des employés spécifiquement chargés de prendre des mesures de sûreté. Le nombre d'employés remplissant ces fonctions doit être proportionnel à la taille et aux opérations de l'OD.

L'unité de sûreté postale ou les employés spécifiquement chargés de la sûreté doivent effectuer des examens périodiques de la sûreté des installations et des processus.

9.2 Reprise après sinistre, préparation aux situations d'urgence et planification de la continuité des opérations

Les éléments ci-après doivent être documentés par l'OD et communiqués aux employés concernés:

– Un plan de gestion des crises visant à garantir la sûreté du courrier, des employés, des clients et des avoirs postaux en cas de catastrophe d'origine naturelle ou humaine susceptible de nuire aux échanges de courrier ou aux opérations postales.
– Un plan de poursuite des activités afin de minimiser les interruptions des services postaux en cas d'incident majeur susceptible de nuire aux opérations postales nationales ou internationales.

Bibliographie

Cette bibliographie présente des références et des indications complètes concernant la source de toutes les normes et de tous les autres documents cités dans le texte du présent document. Pour les références comportant une date ou un numéro de version particuliers, les modifications ou révisions ultérieures de ces publications peuvent ne pas être pertinentes. Néanmoins, les utilisateurs du présent document sont invités à s'informer de l'existence et de l'applicabilité d'éditions plus récentes. Pour les références sans date ou sans numéro de version, la dernière édition du document cité s'applique. Rappelons que seuls les documents mentionnés dans le texte sont indiqués ci-après.

1. Organisation de l'aviation civile internationale, Annexe 17 à la Convention relative à l'aviation civile internationale: Sûreté – Protection de l'aviation civile internationale contre les actes d'intervention illicite.

Remarque 1: les demandes de copies des publications de l'OACI doivent être adressées directement au Groupe de la vente des documents de l'OACI: sales@icao.int.

2. Organisation mondiale des douanes, Cadre de normes SAFE visant à sécuriser et à faciliter le commerce mondial.

Remarque 2: l'édition de 2018 du Cadre de normes SAFE est disponible sur le site Web de l'OMD (https://pmnlo-upu-iso01.upu.ch/docview/viewer/docN699ADEFC420185b671ba550de41ffc6552548f8a873aeb7694ba3369974cc652ac1db473843a).