INSTRUCTION DE TRAITEMENT 7[1]

SÉCURITÉ PHYSIQUE

1. INTRODUCTION

1) La sécurité physique signifie l'application de mesures physiques et techniques de protection pour empêcher l'accès non autorisé aux informations confidentielles et mettre en place des barrières contre le vol ou l'agression.

2) Pour protéger les informations classifiées, ainsi que développer et protéger les activités du Parlement européen dans les domaines qui requièrent un certain degré de confidentialité, un certain nombre de mesures minimales de sécurité sont établies et des installations sécurisées sont créées.

2. PRINCIPES

2.1 Protection des informations classifiées de l'UE (ICUE)

3) Des mesures physiques de sécurité sont mises en place dans tous les locaux où des informations et des documents classifiés sont stockés et/ou traités. Il est tenu compte des mesures de sécurité physique dès le stade de la planification.

2.2 Degré de sécurité physique pour les ICUE

4) Les mesures physiques de sécurité sont choisies en tenant compte de tous les facteurs pertinents, y compris:

   a) le niveau de classification des informations et/ou des documents;

   b) le volume et la forme (par exemple copie papier/support de données informatiques) des informations classifiées détenues;

   c) l'environnement et la structure des bâtiments dans lesquels se trouvent des informations classifiées;

   d) l'évaluation locale, par les services de gestion des risques, des menaces visant l'UE et/ou ses États membres, ainsi que des actes de sabotage, du terrorisme et des autres activités subversives ou criminelles.

2.3 Objectifs des mesures de sécurité

5) Les mesures physiques de sécurité sont conçues pour:

   a) empêcher toute intrusion par la ruse ou par la force;

[1] Décision du Bureau du Parlement européen du 15 avril 2013 concernant les règles applicables au traitement des informations confidentielles par le Parlement européen.

b) décourager, empêcher et détecter les actes commis par du personnel déloyal (espion de l'intérieur);

c) permettre l'identification du personnel pour l'accès aux informations classifiées conformément aux autorisations nécessaires; ainsi que

d) détecter toute infraction à la sécurité et y réagir le plus rapidement possible.

2.4 Principes de la sécurité physique

6) La sécurité physique repose sur le principe de la "défense en profondeur", à savoir l'application d'un vaste éventail de mesures de sécurité organisées en plusieurs niveaux de défense, et sur des éléments retardateurs.

7) Bien que les mesures physiques de sécurité soient spécifiques à chaque site, les principes généraux ci-après s'appliquent:

a) les locaux nécessitant une protection sont identifiés;

b) des mesures de sécurité sont mises en place pour assurer la "défense en profondeur" et fournir des éléments retardateurs;

c) à la périphérie, les mesures physiques de sécurité délimitent la zone protégée et empêchent l'accès non autorisé;

d) le niveau suivant de mesures permet de détecter l'accès ou les tentatives d'accès non autorisé et d'alerter le personnel de sécurité;

e) à l'intérieur, les mesures retardent les intrus jusqu'à ce qu'ils puissent être appréhendés par le personnel de sécurité;

f) le temps d'intervention dont dispose le personnel de sécurité est directement lié aux mesures physiques de sécurité destinées à retarder les intrus;

g) les mesures physiques de sécurité sont conçues de façon à retarder les intrus pendant un temps supérieur à celui nécessaire à l'intervention en profondeur du personnel de sécurité.

8) L'unité des technologies et de la sécurité des informations de la Direction générale de la sécurité (DG Sécurité) est chargée de l'application des normes techniques de sécurité et gère un registre de ces normes, qui peut être consulté par les services compétents des autres institutions et par l'unité Informations classifiées ("UIC") du Parlement.

2.5 Installations sécurisées

9) Deux types de zones protégées physiquement sont créées pour la protection physique des informations classifiées:

a) une zone sécurisée;

b) des salles de lecture sécurisées.

10) Pour chaque installation sécurisée, des procédures d'exploitation de sécurité établissent:

a) le niveau de classification des informations classifiées qui y sont traitées ou stockées;

b) les mesures de surveillance et de protection qu'il convient de mettre en place;

c) les personnes autorisées à pénétrer sans escorte dans la zone en raison de leur besoin d'en connaître et en fonction de leur habilitation;

d) le cas échéant, les procédures applicables aux escortes ou à la protection des informations classifiées lorsque d'autres personnes sont autorisées à pénétrer dans la zone;

e) les autres mesures et procédures applicables.

11) Pour chaque installation sécurisée:

a) un périmètre défini et protégé est établi de façon visible et toutes les entrées et sorties sont contrôlées par un système de laissez-passer ou d'identification individuelle;

b) seules les personnes dûment autorisées sont autorisées à pénétrer sans escorte dans une installation sécurisée. Toutes les autres personnes sont escortées en permanence ou font l'objet de contrôles équivalents;

c) les dispositifs de communication électroniques et les équipements électriques ou électroniques sont interdits.

12) L'autorité responsable de la sécurité certifie qu'une zone répond aux conditions requises pour être désignée comme installation sécurisée.

2.5.1 Zone sécurisée

13) Une zone sécurisée est une zone où les informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et au-dessus ou équivalent sont traitées et conservées de telle façon que l'entrée dans la zone constitue, à toutes fins pratiques, l'accès à des informations classifiées. La zone sécurisée est une zone dont le périmètre est clairement défini et protégé et dont toutes les entrées et sorties sont contrôlées.

14) La zone sécurisée comprend les installations suivantes:

a) sas de sécurité ("SAS"): une zone de réception qui permet la vérification, l'identification et l'inspection de tous les occupants et visiteurs;

b) salle de lecture: une zone où l'on applique la procédure de consultation des documents classifiés, prévue pour préserver la confidentialité des informations qui y sont déposées;

c) salle d'enregistrement: la zone d'enregistrement des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et au-dessus (zone de gestion);

d) archives sécurisées: une zone composée d'espaces d'archivage des informations classifiées répondant à des normes différentes selon le niveau de classification des documents;

e) salle de communication: un espace destiné à recevoir des équipements spéciaux de communication (transmission et réception) ainsi qu'à héberger les équipements hardware des systèmes informatiques (CIS et autres) nécessaires pour la protection des informations classifiées.

15) La salle de lecture, la salle d'enregistrement et la salle de communication sont également protégées contre les écoutes et les radiations électromagnétiques, et toutes les personnes et tous les matériels, y compris le matériel de communication crypté entrant dans la zone, sont contrôlés et font l'objet, à intervalles réguliers, d'inspections physiques ou d'enquêtes, selon les exigences de l'autorité de sécurité compétente.

2.5.2 Salles de lecture sécurisées

16) Les salles de lecture sécurisées sont des espaces dans lesquels des informations classifiées jusqu'au niveau de classification RESTREINT UE/EU RESTRICTED et autres informations confidentielles peuvent être consultées et gardées temporairement conformément aux instructions de traitement 4 et 5 et conservées de telle façon qu'elles puissent être protégées contre tout accès non autorisé au moyen de contrôles internes.

3. PRATIQUES

17) La zone sécurisée répond à des normes de protection spécifiques. La sécurité physique des installations sécurisées repose sur des niveaux de sécurité:

a) niveau 1: périmètre;

b) niveau 2: bâtiments;

c) niveau 3: chambres fortes.

3.1 Niveau 1: périmètre

18) Ce niveau comprend:

a) la définition du périmètre;

b) l'accès au périmètre et le système de détection des intrusions dans le périmètre;

c) un système de télévision en circuit fermé (CCTV);

d) l'éclairage de sécurité;

e) le personnel de sécurité pour intervenir en cas d'incidents, pour les patrouilles, le contrôle des visiteurs, les fouilles menées aux entrées et sorties.

19) Toutes les constructions sont réalisées de manière à ce que toute tentative d'accès non autorisé soit manifeste.

3.2 Niveau 2: bâtiments

20) Ce niveau comprend:

a) la définition des éléments structurels: murs, sols, plafonds, fenêtres, portes (y compris l'application de normes pour la résistance aux attaques);

b) un système de télévision en circuit fermé (CCTV);

c) le contrôle d'accès et la politique en matière de déplacements (accréditation);

d) le système de détection des intrusions (SDI):

e) le personnel de sécurité pour intervenir en cas d'incidents, pour les patrouilles, le contrôle des visiteurs, les fouilles menées aux entrées et sorties.

21) Les murs, les cloisons, les plafonds et les sols constituent des constructions permanentes et sont connectés sans interruption et sans possibilité de démontage ou de retrait non destructifs.

22) Une distinction est établie entre les points d'entrée désignés (portes) et les passages réservés exclusivement aux urgences (sortie de secours).

23) Tous les points d'entrée et de sortie sont équipés de SDI et de CCTV, en fonction du type d'utilisation décidé, et protégés contre toute autre forme d'utilisation.

3.3 Niveau 3: chambres fortes

24) Ce niveau comprend:

a) les normes de verrous;

b) les normes de chambres fortes.

3.4 Mesures techniques de sécurité

25) Le détail des éléments structurels, y compris la détermination des normes de résistance aux attaques à appliquer en fonction des normes européennes en vigueur en la matière, concerne:

a) les murs;

b) les sols et plafonds;

c) les fenêtres;

d) les portes;

e) les verrous;

f) autres.

26) La protection de tous les espaces techniques et ouvertures diverses (service) est assurée avec les techniques suivantes:

a) contrôle d'accès;

b) système de détection des intrusions (SDI):

c) contrôle des visiteurs:

– escortés/sans escorte,

– registre des visiteurs,

– système de télévision en circuit fermé (CCTV).

3.4.1 Murs

27) Tous les murs sont réalisés en briques pleines et construits à partir du plancher et jusqu'au plafond.

3.4.2 Fenêtres

28) Toutes les fenêtres dans la zone, ainsi que leurs châssis, répondent à des normes spécifiques.

3.4.3 Porte d'accès

29) L'ensemble se compose d'un châssis, d'un bloc central et de la quincaillerie. Il répond aux certifications demandées ci-dessous.

3.4.4 Système de contrôle d'accès

30) Les personnes pénétrant dans une zone sécurisée ou la quittant sont identifiées au moyen d'un système de contrôle d'accès (sauf en cas d'urgence). Ce système se compose des éléments suivants:

a) PC de contrôle, niveaux programmables des accès, mémoires des événements et imprimante;

b) logiciel protégé par mot de passe;

c) connaissance d'un seul progiciel par les opérateurs;

d) aperçu complet possible de toute l'installation à tout moment;

e) production intégrée de rapports d'alarme/d'événement;

f) logiciel de gestion comprenant des calendriers, un enregistreur de temps, un fichier journal d'événement et des fonctions de production de rapports.

31) Le contrôle d'accès comprend également:

a) des lecteurs de badge, avec clavier numérique (code PIN);

b) mode de badge: entrant et sortant.

32) Les lecteurs de badge sont compatibles avec la technologie utilisée au Parlement.

33) Tous les points d'entrée et de sortie sont repérés. Une distinction est établie entre les points d'entrée désignés (portes) et les passages réservés exclusivement aux urgences:

a) principal point d'accès;

b) point d'accès secondaire;

c) point de sortie de secours.

34) Tous les points d'entrée et de sortie sont équipés exclusivement en vue de l'utilisation qui est la leur, et protégés contre toute utilisation à d'autres fins.

35) Le mode de fonctionnement du contrôle d'accès est "fail secure", à savoir:

a) en fonctionnement normal, l'entrée et la sortie ne sont possibles qu'à l'aide du badge/lecteur de badge;

b) en cas d'urgence à l'intérieur de la pièce, un dispositif de déblocage permet le déverrouillage de la porte pour quitter la pièce;

c) en cas de coupure électrique, la porte de la pièce reste verrouillée mais une clé dédiée permet un actionnement continu du verrou depuis l'extérieur.

36) Un cylindre sécurisé est installé dans le verrou. Les clés du cylindre sécurisé sont gérées exclusivement par le service de sécurité. Un bouton facile à actionner, avec reset à clé, permet le déclenchement de la serrure motorisée.

37) Tous les boîtiers de contrôle, de commande et de gestion sont installés à l'intérieur de la zone protégée, et couplés au SDI (dispositifs anti-sabotage).

38) Le système de contrôle d'accès est conçu de manière à empêcher l'accès physique non autorisé (vandalisme par exemple) et l'accès logique (par exemple via le réseau) aux équipements (lecteurs de badges, contrôleurs, etc.).

39) Tout accès au système de contrôle d'accès est contrôlé et enregistré, et toutes les informations et données générées par le système sont surveillées depuis la salle de contrôle de sécurité.

40) Il pourrait être possible d'augmenter le niveau de sécurité lors de l'accès dans les zones sécurisées par l'ajout d'un contrôle d'accès basé sur des éléments biométriques qui garantissent l'identité d'une personne en mesurant une de ses caractéristiques physiques.

41) Le boîtier de raccordement est installé à l'intérieur de la zone et au-dessus de la porte. Tous les câbles de la porte (contact magnétique, boîtier vert, buzzer) y sont branchés sur un bornier qui est connecté au câble principal qui va vers le boîtier de raccordement de zone.

42) L'armoire technique principale comporte l'unité de détection des intrusions, les contrôleurs de porte, l'extension, l'alimentation, les relais, le contact incendie, le réseau pour la télégestion, les borniers numérotés et tous les autres éléments nécessaires au bon fonctionnement de l'installation, le tout monté sur une platine de montage. Tous les câbles et fils sont repérés. Ces armoires sont équipées de passe-câbles et d'une aération. L'armoire est fermée à clé et équipée d'un dispositif contre le sabotage. Le boîtier de raccordement de zone est alimenté par le réseau 230V/50Hz/16A (source principale), ou en cas de défaut de ce dernier, par des batteries placées dans un second tableau réservé uniquement pour les batteries (sources secondaires).

43) Les batteries sont constituées d'éléments étanches, sont au cadmium nickel ou au plomb, ne demandent aucun entretien et ont une durée de vie de 5 ans. Leur capacité est calculée de manière à assurer le fonctionnement intégral du système; l'autonomie des batteries à prévoir est de 30 heures pour les portes d'accès.

44) Les batteries sont maintenues en état de charge permanente par des chargeurs appropriés. Un dispositif de commutation assure le passage d'une source à l'autre. L'une des alimentations ainsi que sa batterie sont propres à l'alimentation de la centrale. L'autre alimentation et sa batterie alimentent les asservissements. Les batteries de secours peuvent être installées dans une armoire séparée à côté de l'armoire technique principale. Les batteries ne sont pas superposées. Ces armoires sont équipées de passe-câbles et d'aération. Elles sont fermées à clé et équipées d'un dispositif contre le sabotage.

3.4.5 Système de détection des intrusions (SDI)

45) La zone sécurisée est protégée par un système indépendant de détection des intrusions. Sur ce système de détection sont connectés tous les périphériques nécessaires, avec gestion de l'état, des tentatives de sabotage ou de la déconnexion.

46) Le SDI est connecté au local de télégestion centralisé. La transmission de données entre les deux se fait au moyen de la suite IP, c'est-à-dire les protocoles utilisés pour le transfert de données par internet: le protocole de contrôle de transmission (TCP) et le protocole internet (IP). Le SDI est relié aux détecteurs de mouvements et aux contacts magnétiques de la porte. Il comprend tout l'équipement nécessaire à la détection d'un intrus dans la zone contrôlée et réagit en conséquence lorsqu'il est en mode surveillance.

47) Les contacts anti-sabotage sont en place; les claviers, les détecteurs de mouvements, le boîtier de dérivation et la centrale sont protégés par un dispositif anti-arrachement, et les circuits reliant les diverses composantes et le SDI sont connectés en permanence à la boucle de surveillance.

48) Le SDI répond aux critères suivants:

a) Confidentialité

Les informations relatives à la conception de la mise à niveau de l'installation et à la mise en service sont considérées comme confidentielles.

b) Transmission des signaux

La transmission est assurée au moyen d'une transmission numérique vers une centrale de surveillance répondant aux normes du secteur et en direct vers le local de télégestion centralisé de la Direction de la sécurité. Les informations suivantes sont obligatoirement transmises:

i) alarme intrusion;

ii) mise en surveillance totale ou partielle;

iii) sabotage;

iv) dérangement technique des alimentations batteries et secteur;

v) mise en surveillance et mise hors surveillance totale ou partielle (ON/OFF passif);

vi) test de transmission au moins une fois par 24 heures;

vii) mise en surveillance tardive et mise hors surveillance prématurée avec indentification de l'utilisateur auprès de la centrale de surveillance (ON/OFF actif).

c) Clavier de commande

Le clavier de commande numérique permet de commander toutes les fonctions du SDI. Il permet notamment de visualiser la nature de chaque événement et sa localisation. Le clavier est également muni d'un signal d'alarme local (buzzer). Ce dernier émet des signaux sonores lorsque certaines fonctions sont utilisées, pendant la temporisation de sortie et d'entrée et lorsque les touches numériques sont pressées (validation).

Le clavier de commande numérique pour armer/désarmer la zone est installé à l'intérieur ou à l'extérieur (mais à proximité) de la porte d'entrée de la zone.

Le système d'alarme installé dans la zone sécurisée est distinct du système général d'avertissement antieffraction du bâtiment.

L'UIC est informée immédiatement de toute alarme dans la zone sécurisée.

d) Détecteur à double technologie

La zone est équipée de détecteurs à double technologie ou bivolumétriques, combinant dans un même boîtier une hyperfréquence et un infrarouge passif contrôlé par un microprocesseur qui s'adapte à n'importe quel environnement. Ils sont activés ou désactivés par l'enlèvement ou l'installation de pontages: mémoire d'alarme, nombre d'impulsions comptées, détection IRP ou micro-ondes.

49) Le système de détection des intrusions (SDI) comprend:

a) un tableau de commande du système d'alarme: commandes locales, commandes à distance;

b) la gestion du code PIN;

c) la détection volumétrique: technologie double avec anti-masquage;

d) les contacts magnétiques pour:

i) les portes,

ii) les fenêtres,

iii) les ouvertures diverses,

iv) les armoires, les éléments de rangement sécurisés;

e) les détecteurs sismiques sur les fenêtres et les murs;

f) les détecteurs de bris de glace sur les fenêtres;

g) le buzzer (signal d'alarme local).

50) Tous les boîtiers de contrôle, de commande et de gestion sont installés à l'intérieur de la zone protégée et couplés au SDI (dispositifs anti-sabotage).

51) Le SDI est conçu de manière à empêcher l'accès physique non autorisé (vandalisme par exemple) et l'accès logique (par exemple via le réseau) à la caméra et aux images enregistrées.

52) Tout accès au SDI est contrôlé et enregistré et toutes les informations et données générées par le SDI sont surveillées depuis la salle de contrôle de sécurité.

3.4.6 Système de télévision en circuit fermé (CCTV)

53) La porte d'accès à la zone sécurisée est surveillée par CCTV; l'image est relayée à l'accueil du bâtiment et au local de télégestion centralisé de la Direction de la sécurité. La camera est connectée à un système d'enregistrement des images, consultable ultérieurement par les personnes autorisées. Elle est placée à un endroit jugé sensible d'un point de vue sécurité. Chaque ouverture de la porte, de l'intérieur ou de l'extérieur, déclenche l'enregistrement d'une séquence.

54) Les caméras satisfont aux normes et caractéristiques nécessaires et résistent au vandalisme.

55) Les enregistrements respectent le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

56) L'accès à l'enregistreur est protégé par nom d'utilisateur et mot de passe associé. La lecture des enregistrements ne peut s'effectuer que par des personnes dûment autorisées par l'UIC, et seul l'administrateur désigné peut supprimer des séquences vidéo.

57) Le système de CCTV:

a) couvre le périmètre extérieur, les points d'accès et de sortie, les points de contrôle;

b) couvre les points d'accès et de sortie intérieurs, les points de contrôles, les pièces, les installations et équipements essentiels;

c) définit le type de caméra pour chaque lieu: caméra statique, caméra PTZ, caméra à infrarouges;

d) par caméra: à des fins de paramétrage, définit le niveau d'identification requis: visage, personne, activité, décor global;

e) fournit les équipements de fonctionnement et de visualisation (ordinateur, écrans);

f) fournit des équipements d'enregistrement et de stockage et des capacités de sauvegarde;

g) dispose d'une lumière appropriée pour garantir une observation optimale (au moins 1 lux).

58) Tous les boîtiers de contrôle, de commande et de gestion sont installés à l'intérieur de la zone protégée et couplés au SDI (dispositifs anti-sabotage).

59) Le système de CCTV est conçu de manière à empêcher l'accès physique non autorisé (vandalisme par exemple) et l'accès logique (par exemple via le réseau) à la caméra et aux images enregistrées.

60) Tout accès au système de CCTV est contrôlé et enregistré et toutes les informations et données générées par le système de CCTV sont surveillées depuis la salle de contrôle de sécurité.

3.5 Surveillance

61) La surveillance des équipements de sécurité est assurée par la Direction de la sécurité:

a) sur place;

b) horaire/calendrier d'activité: 24/7/365;

c) les moyens de communication sont établis;

d) procédures opérationnelles d'intervention en cas d'incident;

e) procédures opérationnelles pour le fonctionnement des équipements techniques.

62) La surveillance est assurée par du personnel de sécurité dûment formé, qualifié et titulaire d'une habilitation de sécurité, et les procédures opérationnelles pour l'intervention en cas d'incidents, pour les patrouilles et les inspections sont établies.

3.6 Armoires

63) Prévoir et organiser les armoires ou les éléments de rangement sécurisés pour regrouper tous les équipements de surveillance:

a) système de contrôle d'accès;

b) système de détection des intrusions (SDI);

c) système de télévision en circuit fermé (CCTV);

d) les armoires et les éléments de rangement sécurisés sont reliés au SDI.

3.7 Alimentation électrique

64) Un groupe électrogène d'urgence est installé pour garantir et maintenir la sécurité et la sûreté pendant au moins 24 heures, en cas de coupure de courant électrique sur le réseau électrique normal.

65) Une solution anti-interruption, reposant sur l'utilisation de batteries, stockée dans une armoire distincte et appropriée, couplée au SDI (dispositif anti-sabotage), est mise en place et toute l'alimentation électrique est surveillée.

3.8 Chambres fortes et verrous

66) Les armoires et éléments de rangement sécurisés sont équipés d'un verrou à combinaison mécanique ou électronique ou équivalent et répondent aux normes correspondant au niveau de classification des informations pour lesquelles ils seront utilisés. Ils sont installés à l'intérieur de la zone sécurisée.

67) Les éléments de rangement sont notés en fonction de leur degré de résistance à l'intrusion par la force et par la ruse. Quatre types d'éléments de rangement différents peuvent être utilisés.

a) Éléments de rangement de type 4: ces éléments de rangement sont approuvés pour le stockage de toutes les ICUE, y compris les informations classifiées TRÈS SECRET UE/EU TOP SECRET, au sein de la zone sécurisée. Ils ont un haut degré de résistance à l'intrusion par la force et à l'aide de divers outils mécaniques et électriques ainsi que clandestinement ou par la ruse. Ils offrent une résistance contre les tentatives de forcer les portes, les tiroirs ou les couvercles à des fins de subtilisation ou de sondage.

b) Éléments de rangement de type 3: ces éléments de rangement sont approuvés pour le stockage des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL et SECRET UE/EU SECRET, au sein de la zone sécurisée. Ils ont un certain degré de résistance à l'intrusion par la force et à l'aide d'un nombre limité d'outils mécaniques ainsi que clandestinement ou par la ruse. Ils résistent à la flexion, à la torsion ou aux secousses susceptibles de tordre la structure et de permettre l'insertion de sondes ou de dispositifs pour accéder à l'élément de rangement.

c) Éléments de rangement de type 2: ces éléments de rangement sont approuvés pour le stockage des informations classifiées CONFIDENTIEL UE/EU CONFIDENTIAL, au sein de la zone sécurisée. Ils sont d'une conception et construction solides et offrent une résistance aux intrusions ordinaires ou opportunistes de la part de personnes non préparées pour l'attaque et ne disposant que d'objets facilement accessibles.

d) Éléments de rangement de type 1: ces éléments de rangement sont approuvés pour le stockage d'informations classifiées RESTREINT UE/EU RESTRICTED. Ils n'ont pas de caractéristiques de sécurité particulières mais sont sécurisables et considérés comme offrant un certain niveau d'intégrité de sécurité.

68) Les verrous des éléments de rangement sont notés en fonction de leur degré de résistance à une ouverture non autorisée. Quatre types de verrous différents peuvent être utilisés:

a) Verrous de type 4: ces verrous ont un degré de résistance élevée aux intrusions d'experts et de professionnels disposant de compétences et de ressources développées exclusivement et que l'on estime ne pas être disponibles dans le commerce;

b) Verrous de type 3: ces verrous ont un degré de résistance élevée aux intrusions d'experts et de professionnels à l'aide de compétences et de ressources développées exclusivement et disponibles dans le commerce pour les serruriers professionnels;

c) Verrous de type 2: ces verrous présentent un degré de résistance élevée contre les tentatives d'intrusion d'experts disposant de ressources minimales;

d) Verrous de type 1: ces verrous présentent un degré de résistance modérée aux ouvertures non autorisées.

69) Les verrous des éléments de rangement de type 3 ou 4 peuvent être contrôlés.