NATO SANS CLASSIFICATION

25 novembre 2020

DOCUMENT
AC/35-D/2001-REV3

COMITÉ DE SÉCURITÉ

DIRECTIVE SUR LA SÉCURITÉ PHYSIQUE

Note du président par intérim

1. On trouvera en annexe 1 la troisième version révisée de la directive sur la sécurité physique, qui est publiée à l'appui du C-M(2002)49-REV1, intitulé « La sécurité dans l'Organisation du Traité de l'Atlantique Nord ». Elle a un caractère contraignant et obligatoire. Elle remplace l'AC/35-D/2001-REV2, qui doit être détruite.

2. La présente directive est le résultat de la revue globale de la politique de sécurité de l'OTAN (voir l'AC/35-N(2015)0025-AS1, du 21 décembre 2015).

3. Ce document a été approuvé par le Comité de sécurité (AC/35-N(2020)0004-AS1, du 4 novembre 2020) et fera l'objet de revues périodiques

(signé) Marco Criscuolo

1 annexe

Responsable : R. Grumberg, NOS, poste 9182
Original : anglais

ANNEXE 1
AC/35-D/2001-REV3

DIRECTIVE SUR LA SECURITE PHYSIQUE

TABLE DES MATIERES

ANNEXE 1
AC/35-D/2001-REV3

DIRECTIVE SUR LA SÉCURITÉ PHYSIQUE

INTRODUCTION

1. Le présent document, intitulé « Directive sur la sécurité physique », est publié par le Comité de sécurité (AC/35) à l'appui de la pièce jointe « D » à la politique de sécurité de l'OTAN (C-M(2002)49). Il contient des dispositions obligatoires ainsi que des informations qui clarifient leur sens. Il porte sur les points suivants :

(a) principes de base ;

(b) impératifs généraux liés à la sécurité physique ;

(c) mesures spécifiques à la sécurité physique ;

(d) impératifs liés au stockage des informations OTAN classifiées ;

(e) protection physique des systèmes d'information et de communication ;

(f) protection contre les attaques techniques.

PRINCIPES DE BASE

2. Tous les locaux, bâtiments, bureaux, pièces et autres zones où des informations OTAN classifiées sont stockées, manipulées et/ou examinées sont protégés par des mesures de sécurité physique appropriées. Pour déterminer le degré de sécurité physique nécessaire, tous les facteurs pertinents sont pris en considération, notamment :

(a) le niveau de classification de sécurité et la catégorie des informations ;

(b) le volume et la forme (copie papier et/ou support électronique) des informations classifiées stockées et/ou manipulées ;

(c) le contrôle de l'accès et l'application du principe du besoin d'en connaître ;

(d) la menace que constituent les services de renseignement hostiles ayant pour cible l'OTAN et/ou les pays membres de l'OTAN, et l'évaluation locale de la menace que représentent les actes de terrorisme, d'espionnage, de subversion, de sabotage et de criminalité (organisée) ;

(e) le mode de stockage des informations classifiées (copie papier ou support électronique avec chiffrement).

3. Les mesures de sécurité physique sont conçues pour :

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

(b) décourager, empêcher et détecter toute action pouvant émaner d'une menace intérieure ;

(c) opérer, au sein du personnel, une distinction dans les accès aux informations OTAN classifiées en fonction du niveau d'habilitation de sécurité (PSC) et du besoin d'en connaître ;

(d) permettre de détecter le plus tôt possible tout incident de sécurité et d'y donner suite.

4. Les autorités nationales de sécurité/autorités de sécurité désignées (ANS/ASD) et autres autorités de sécurité compétentes ainsi que les organes civils et militaires de l'OTAN sont chargés de veiller à ce que des dispositifs de sécurité soient en place afin d'éviter qu'en situation d'urgence, des informations OTAN classifiées ne tombent entre les mains de personnes non autorisées ou hostiles (plans d'évacuation et/ou de destruction d'urgence des informations classifiées). Au minimum, ces plans :

(a) couvrent les situations d'urgence dans lesquelles il convient d'évacuer et/ou de détruire des informations classifiées ;

(b) prévoient des procédures d'évacuation/destruction d'urgence désignant les autorités (principale et de remplacement) chargées d'ordonner leur exécution ;

(c) prévoient des méthodes de communication ;

(d) précisent les moyens de destruction ou méthodes d'évacuation ;

(e) désignent différents sites de stockage de repli en cas d'évacuation ;

(f) désignent les éléments à détruire ou évacuer en priorité.

IMPÉRATIFS GÉNÉRAUX LIÉS À LA SÉCURITÉ PHYSIQUE

5. Les mesures de sécurité physique ne représentent qu'un aspect de la sécurité de protection et doivent être étayées par de solides mesures de sécurité concernant le personnel, les informations et les systèmes d'information et de communication (SIC), qui sont traitées respectivement en détail dans les pièces jointes C, E et F au C-M(2002)49 et dans les directives complémentaires. Une gestion rationnelle des risques de sécurité implique la détermination des méthodes les plus adaptées, les plus efficaces et les plus rentables pour contrer les menaces et compenser les éventuelles vulnérabilités par une combinaison de mesures de protection appartenant à chacun de ces domaines. Dans un souci d'efficacité et de rentabilité, les impératifs de sécurité physique sont définis dès l'étape de la planification et de la conception des projets de locaux, et l'avis des autorités de sécurité compétentes est sollicité, le but étant d'éviter par la suite des travaux de rénovation coûteux.

6. Les programmes de sécurité physique reposent sur le principe de la défense en profondeur et font appel à différentes mesures de sécurité physiques complémentaires offrant un degré de protection qui correspond aux impératifs associés au niveau de criticité et de vulnérabilité de l'organisme visé et des informations en sa possession. Bien que les mesures de sécurité physiques soient spécifiques à chaque site et dépendantes d'un certain nombre de facteurs (tels que l'évaluation locale de la menace, la structure et l'architecture du bâtiment, les considérations environnementales ou encore l'emplacement du site), les principes généraux suivants s'appliquent :

(a) il est avant tout nécessaire d'identifier les moyens qui exigent une protection. On crée ensuite des mesures de sécurité à plusieurs niveaux pour assurer une « défense en profondeur » et retarder les intrusions ;

(b) les mesures de sécurité physique les plus extérieures définissent la zone protégée et découragent l'accès non autorisé ;

(c) les mesures du niveau suivant détectent tout accès non autorisé ou toute tentative d'accès et alertent les services de gardiennage ;

(d) les mesures se situant le plus à l'intérieur retardent suffisamment l'action de l'intrus pour qu'il puisse être arrêté par les services de gardiennage. Il existe donc un lien entre le délai de réaction des services de gardiennage et les mesures de sécurité physique destinées à retarder l'action d'un intrus.

7. Les équipements qui permettent d'assurer la sécurité physique (vidéosurveillance, système de détection des intrusions (IDS), armoires fortes, etc.) font l'objet d'une maintenance régulière afin de garantir des performances maximales. L'efficacité de chacune des mesures de sécurité et celle de l'ensemble du système de sécurité sont en outre réévaluées périodiquement. Une telle réévaluation est particulièrement importante si un changement intervient dans l'utilisation du site ou dans certains éléments spécifiques du système de sécurité. Cela peut se faire en mettant régulièrement (en principe chaque année) en pratique les plans de réaction aux incidents dans le cadre d'exercices.

8. L'autorité de sécurité locale analyse minutieusement toute installation de systèmes électroniques ou d'appareils mobiles disposant de fonctions d'enregistrement et/ou de transmission (p. ex. téléphone mobile, smartphone, montre connectée, tablette, ordinateur portable, objet connecté) dans des zones où des informations OTAN classifiées sont stockées, manipulées ou examinées. Le document complémentaire sur l'utilisation des appareils mobiles dans les installations de l'OTAN (AC/35-D/1042) peut être utilisé comme référence pour l'élaboration des exigences de sécurité et des règles locales régissant l'utilisation des appareils mobiles.

Zones de sécurité

9. Une zone de sécurité est une zone dans laquelle des informations classifiées NATO CONFIDENTIEL (NC) ou d'un niveau de classification supérieur sont stockées, manipulées ou examinées. Les dispositions ci-après s'appliquent aux zones de sécurité tant permanentes que temporaires. L'organisation et la structure des différentes zones sont précisées ci-dessous :

(a) zone de sécurité OTAN de classe I : zone particulièrement sensible dans laquelle des informations classifiées NC ou d'un niveau de classification supérieur sont stockées, manipulées ou examinées de telle façon que le fait de pénétrer dans cette zone équivaut en pratique à avoir accès à des informations classifiées et que tout accès non autorisé constitue dès lors une infraction de sécurité. Ces zones, qui peuvent par exemple comprendre les salles d'opérations, les centres de communications ou les locaux d'archives, nécessitent :

(i) d'établir de façon précise un périmètre protégé dont toutes les entrées et sorties sont contrôlées ;

(ii) de mettre en place un système de contrôle des entrées laissant pénétrer uniquement les personnes dûment habilitées et expressément autorisées[1] à y accéder ;

(iii) de déterminer le niveau de classification de sécurité et la catégorie des informations (p. ex. ATOMAL, BOHEMIA) qui y sont stockées habituellement, c'est-à-dire des informations auxquelles on a accès en pénétrant dans la zone ;

[1] Par personne expressément autorisée, on entend un membre du personnel pour lequel il a été officiellement reconnu qu'il a le besoin d'en connaître et doit accéder auxdites zones concernées en raison de la nature de ses fonctions, et dont le nom figure sur les listes de contrôle d'accès, ainsi que toute personne qui a été officiellement autorisée, sur une base ad hoc, par le chef de l'organisation concernée à remplir un rôle ou une fonction spécifique.

(iv) d'indiquer clairement que l'entrée dans les zones concernées nécessite une autorisation spéciale de l'autorité de sécurité locale. Le niveau de classification de sécurité et/ou la sensibilité de la zone concernée peut figurer sur l'indication en question ;

(b) zone de sécurité OTAN de classe II : zone dans laquelle des informations classifiées NC ou d'un niveau de classification supérieur sont stockées, manipulées ou examinées de telle façon qu'elles peuvent être protégées au moyen de contrôles internes contre l'accès de personnes non autorisées. Ces zones, qui peuvent par exemple comprendre les bureaux ou les salles de réunion dans lesquels des informations OTAN classifiées sont stockées, manipulées ou examinées, nécessitent :

(i) d'établir de façon précise un périmètre protégé dont toutes les entrées et sorties sont contrôlées ;

(ii) de mettre en place un système de contrôle des entrées n'y laissant pénétrer sans escorte que les personnes titulaires d'une habilitation de sécurité et autorisées à y accéder ;

(iii) de prévoir un dispositif d'escorte ou un mécanisme de contrôle équivalent pour les personnes qui ne satisfont pas aux critères énoncés à l'alinéa (b) (ii) ci-dessus, afin de les empêcher d'accéder à des informations OTAN classifiées et de pénétrer librement dans des zones qui ont été spécifiquement désignées comme étant des zones protégées contre les attaques techniques ainsi que contre l'écoute active et passive.

10. Toutes les zones de sécurité (par exemple, les bureaux, salles de réunion et salles de conférences, zones techniquement protégées, etc.) dans lesquelles des informations OTAN classifiées sont débattues font l'objet d'une évaluation périodique afin de déterminer le risque d'écoute passive. Lorsque l'autorité de sécurité compétente estime qu'un tel risque existe, il convient d'interdire toute discussion classifiée ou de prendre des mesures appropriées (par exemple, définir les salles de réunion où des discussions classifiées peuvent avoir lieu) ou encore de prendre des mesures d'ordre technique (par exemple isoler phoniquement les cloisons, portes et plafonds, poser des systèmes d'atténuation sonore, etc.).

11. À moins qu'un système de détection des intrusions soit activé, les zones de sécurité qui ne sont pas occupées 24 heures sur 24 par le personnel de service sont inspectées immédiatement après les heures normales de travail afin de vérifier qu'elles sont bien sécurisées.

12. L'entrée des agents permanents dans les zones de sécurité de classe I ou II est régie par un système de contrôle d'accès approprié (système de laissez-passer ou de reconnaissance personnelle).

Zone administrative

13. Zone entourant ou précédant une zone de sécurité OTAN de classe I ou II. Les informations pouvant être stockées, manipulées ou examinées dans une zone administrative ne peuvent pas être classifiées au-delà de NATO DIFFUSION RESTREINTE (NDR). Ces zones exigent que soit établi de façon visible un périmètre au sein duquel il est possible de contrôler les personnes et les véhicules. Les visiteurs ne sont toutefois pas tenus d'y être escortés.

Zones techniquement sécurisées

14. Les zones techniquement sécurisées sont des zones fixes ou temporaires expressément reconnues comme étant à protéger contre les attaques techniques et les écoutes.

15. Elles font l'objet d'inspections physiques et techniques[2] régulières et l'accès en est strictement contrôlé. Les mesures ci-après sont mises en œuvre pour assurer la protection contre les attaques techniques et les écoutes :

(a) mise en œuvre d'un contrôle d'accès reposant sur des mesures de sécurité physique et technique adaptées au risque. La responsabilité de la détermination du risque est répartie entre les spécialistes techniques compétents et l'autorité de sécurité qui remet des avis au propriétaire du risque pour décision/approbation ;

(b) les zones techniquement sécurisées sont verrouillées et/ou gardées lorsqu'elles ne sont pas occupées, et toutes les clés associées à celles-ci sont considérées comme des clés de sécurité[3]. Ces zones font l'objet d'inspections de sécurité physique et/ou technique à intervalles réguliers, conformément aux exigences de l'autorité de sécurité compétente, ainsi qu'après toute entrée non autorisée, effective ou présumée, ou après tout accès de personnel extérieur (par exemple pour des travaux d'entretien ou de décoration) ;

(c) aucun objet, meuble ou matériel ne peut être introduit dans ces zones avant d'avoir subi une inspection minutieuse, effectuée par du personnel de sécurité formé à cet effet et destinée à détecter les éventuels dispositifs d'écoute. Il y a lieu de tenir un registre des objets, meubles et matériels qui y entrent ou en sortent ;

(d) la présence de tout système électronique ou appareil mobile disposant de fonctions d'enregistrement et/ou de transmission (téléphone portable, smartphone, montre connectée, tablette, ordinateur portable, objet connecté) est interdite ;

(e) les zones techniquement sécurisées ne contiennent en principe aucun téléphone ni dispositif de visioconférence ; toutefois, si leur installation est inévitable, ceux-ci sont physiquement débranchés en cas de discussion classifiée. Cette disposition ne concerne pas les dispositifs de communication dûment homologués et installés, tels que les lignes téléphoniques et équipements de visioconférence classifiés.

MESURES DE SÉCURITÉ PHYSIQUE SPÉCIFIQUES

16. La présente section contient des informations sur diverses mesures de sécurité physique (périmètre, portes, serrures, etc.) et technique (système de détection des intrusions, de vidéosurveillance, etc.) et procédures apparentées (contrôle des visiteurs, contrôle des clés,

[2] Une inspection technique désigne la conduite d'une opération de recherche et détection d'appareils électroniques ou l'examen d'une zone en vue d'y déceler la présence de dispositifs de collecte d'informations (microphones, caméras, etc.) ou de brouillage des communications.

[3] Par clés de sécurité, on entend les dispositifs permettant d'actionner les serrures montées sur les armoires fortes destinées au stockage d'informations classifiées, sur les portes des pièces ou des zones sécurisée, sur les portes des pièces ou des zones sécurisées qui ont été soumises à des inspections de sécurité technique, ou sur les coffrets de sécurité destinés au transport de documents classifiés. Toute clé de sécurité doit être manipulée et protégée de la même manière que les informations classifiées auxquelles elles donnent accès.

cloisonnement des espaces de bureaux) ainsi que sur la manière dont elles peuvent contribuer au cadre de sécurité d'une organisation ou d'un site.

Périmètre

17. Un périmètre est une barrière physique qui délimite une zone à protéger.

18. Il sert :

(a) à assurer une dissuasion physique et psychologique destinée à empêcher tout accès involontaire dans une zone ;

(b) à empêcher tout accès non autorisé par des moyens visibles ou dissimulés ;

(c) à retarder toute intrusion dans une zone afin de laisser aux gardes ou aux forces de sécurité le temps de réagir ;

(d) à faciliter les procédures d'identification et de contrôle en canalisant le flux des personnes et des véhicules autorisés vers des points d'entrée fixes.

19. Le degré de protection qu'apporte une clôture périmétrique dépend de sa conception, du matériau utilisé, de sa hauteur, du type et de la profondeur de ses fondations, ainsi que des mesures de sécurité mises en œuvre pour accroître ses performances et son efficacité (protections supérieures, système de détection périmétrique des intrusions, éclairage, vidéosurveillance). Certains bâtiments peuvent être dépourvus de clôture périmétrique mais tirer parti d'autres obstacles ou infrastructures servant de barrières physiques.

20. Une barrière périmétrique ne retarde un intrus déterminé que pendant un court laps de temps ; il convient donc de la compléter par un système de détection des intrusions (IDS), un système de vidéosurveillance (CCTV), un éclairage de sécurité et des rondes effectuées à intervalle périodique mais variable par des gardes ou des forces de sécurité.

21. L'efficacité d'un périmètre dépend également du niveau de sécurité assuré aux points d'accès. Les grilles d'entrée sont dès lors construites selon les mêmes normes de sécurité que le périmètre et font l'objet d'un contrôle d'accès.

Systèmes de détection des intrusions

22. Il est possible d'accroître le niveau de sécurité offert par une clôture périmétrique en lui adjoignant un système de détection périmétrique des intrusions (PIDS). Il peut s'agir d'un dispositif dissimulé (bien que ce soit habituellement pour des raisons esthétiques) ou visible faisant office d'élément de dissuasion. Les fausses alertes étant fréquentes avec ce type de système, les PIDS doivent, en principe, n'être utilisés qu'avec un système de vérification des alarmes (par exemple, CCTV).

23. Conformément au principe de la « défense en profondeur », des systèmes de détection des intrusions (IDS) peuvent être installés dans les locaux et les bâtiments en lieu et place des gardes, ou pour aider ceux-ci dans leur tâche. Pour être efficace, un IDS doit être assorti de personnel prêt à réagir dans un délai raisonnable si l'alarme est donnée.

Contrôle d'accès

24. Le terme « contrôle d'accès » englobe les systèmes de laissez-passer ou de reconnaissance personnelle, y compris les dispositifs de contrôle et d'escorte des contractants et des visiteurs.

25. Un contrôle d'accès peut être exercé sur un site, dans un ou plusieurs bâtiments faisant partie d'un site, ou dans des sections, zones ou locaux spécifiques d'un bâtiment. Le mécanisme de contrôle peut être électronique, électromécanique ou physique. Il peut également être exercé par un garde ou un réceptionniste. Un système de laissez-passer ou de reconnaissance personnelle est instauré pour contrôler l'entrée des agents permanents dans les zones de sécurité de classe I ou II.

26. Si le site est équipé d'un système de reconnaissance des laissez-passer, ces derniers sont portés de manière visible en permanence afin de permettre leur reconnaissance et l'identification de leur détenteur.

Cloisonnement des espaces de bureaux

27. Les mesures nécessaires sont prises pour éviter que des personnes non autorisées puissent accéder à des informations OTAN classifiées que ce soit par l'observation ou par une proximité physique. Les facteurs tels que le nombre de personnes travaillant dans une zone ou y ayant accès, la position des fenêtres, les possibilités de voir l'intérieur des locaux depuis l'extérieur ou encore les conditions d'éclairage (lumière naturelle ou artificielle) sont dès lors pris en considération. Des précautions sont également prises contre l'écoute passive et active.

Gardes

28. Le recours à des gardes peut constituer un bon moyen de dissuasion à l'égard des individus qui pourraient envisager une intrusion subreptice. Les tâches des gardes et la fréquence des rondes sont définies en tenant compte du niveau de risque ainsi que des autres systèmes ou équipements de sécurité déjà en place. Les gardes reçoivent des instructions écrites appropriées afin que les tâches qui leur sont spécifiquement confiées soient exécutées comme il se doit. Ils ont besoin d'un moyen de communication avec leur centre de contrôle.

29. Lorsqu'il est fait appel à des gardes pour assurer l'intégrité de zones de sécurité et d'informations OTAN classifiées, ils sont dûment habilités, qualifiés et supervisés.

30. Tout incident de sécurité se produisant sur le site entraîne obligatoirement la réaction d'une force d'intervention. Celle-ci se compose d'un nombre adapté d'agents de sécurité (en principe, deux gardes au minimum), déterminé par l'autorité de sécurité compétente. La réponse à un incident ne se fait pas au détriment de la protection d'une autre zone du site. Le temps de réaction des gardes aux signaux d'alarme ou d'urgence est testé et ne dépasse pas le délai considéré comme permettant d'empêcher un intrus d'accéder à des informations OTAN classifiées.

Vidéosurveillance

31. La vidéosurveillance (CCTV) est d'une aide précieuse pour les gardes de sécurité dans les vérifications consécutives à un incident ou à une alerte déclenchée par le système de détection des intrusions (IDS) sur des sites ou des périmètres de grande étendue. Pour qu'un tel système soit

efficace, il est toutefois nécessaire de sélectionner et d'installer un équipement approprié, et d'assurer une surveillance depuis le centre de contrôle. Il convient de demander l'avis d'experts pour la conception du système de vidéosurveillance (caractéristiques techniques et emplacement des caméras, redondances du système, disposition intérieure et ergonomie des postes de surveillance du centre de contrôle). Il y a également lieu de faire en sorte que les informations OTAN classifiées pouvant figurer dans les données audiovisuelles recueillies par le système de vidéosurveillance soient protégées des regards indiscrets.

Éclairage de sécurité

32. En plus d'assurer l'illumination nécessaire pour une surveillance efficace exercée directement par les gardes ou par l'intermédiaire d'un système CCTV, un éclairage de sécurité peut fortement décourager les intrus. Son installation doit être adaptée aux conditions locales et le niveau d'éclairage répondre aux besoins minimums du système CCTV.

Armoires fortes et mobilier de bureau

33. Dans une approche de la sécurité de type « défense en profondeur », les armoires fortes et le mobilier de bureau constituent la dernière ligne de défense pour les informations OTAN classifiées qui y sont stockées. La durée de protection qu'ils offrent est déterminée par des essais complets qui permettent de calculer leur capacité de résistance aux tentatives d'ouverture non décelées et aux formes d'attaque dont ils sont vraisemblablement susceptibles de faire l'objet. Ces équipements sont dûment homologués en fonction du niveau de classification des informations qu'ils contiennent (voir paragraphes 50 à 54 de la présente directive). Le choix des équipements utilisés pour stocker des informations OTAN classifiées est effectué d'après les critères suivants :

(a) la menace pesant sur la sécurité dans la zone où seront stockées les informations ;

(b) le niveau de classification des informations à stocker ;

(c) le niveau de protection qu'offrent l'armoire ou le meuble et sa serrure ;

(d) la combinaison de mesures auxiliaires mises en place pour protéger l'environnement de l'armoire ou du mobilier.

Serrures

34. Les systèmes de serrures et de clés sont sélectionnés de manière à assurer un degré de protection correspondant au niveau de contrôle d'accès requis, aux informations à protéger et au type de structure et de matériau dans lesquels ils seront installés.

35. Les cylindres mécaniques de serrure doivent être résistants aux clés de frappe, aux attaques physiques (p. ex. perçage, cisèlement, torsion, extraction) et à la duplication non autorisée des clés. Dans les systèmes de gestion des clés du site, les groupes de clés principales doivent être en nombre limité. Les serrures extérieures doivent avoir une résistance à la corrosion adaptée aux conditions locales.

36. Les serrures électroniques doivent être résistantes à la duplication non autorisée des clés électroniques (qu'il s'agisse d'une bande magnétique, d'une puce, d'un jeton de sécurité, etc.) et doivent disposer d'un indicateur actif de batterie faible et de défaut système. Dans les systèmes de gestion des clés électroniques du site, le nombre de passe-partout électroniques (clés électroniques permettant d'ouvrir un grand nombre de serrures électroniques) et la durée de validité des clés

électroniques doivent être limités. Les serrures électroniques enregistrent en mémoire les ouvertures autorisées.

Contrôle des clés et combinaisons

37. Les clés des armoires fortes ne sortent pas du site. De manière générale, elles ne sortent pas du bâtiment où se trouvent les armoires qu'elles permettent d'ouvrir. Les combinaisons des armoires fortes et les codes d'activation/désactivation des IDS sont mémorisés par les personnes qui ont besoin de les connaître. Le nombre des personnes ayant connaissance de ces combinaisons et codes est aussi limité que possible. Les combinaisons et codes sont changés au minimum :

(a) lors de leur mise en service ;

(b) lorsqu'il se produit un changement du personnel qui les connaît ;

(c) dès qu'une compromission a eu lieu ou est suspectée ;

(d) tous les douze mois, sauf autorisation expresse de l'autorité de sécurité compétente, après évaluation du risque de sécurité.

38. Les clés de rechange et un enregistrement écrit de chaque combinaison, à n'utiliser qu'en cas d'urgence, sont conservés par l'autorité de sécurité locale dans une enveloppe opaque scellée.

39. Les clés et leurs doubles sont rangés dans des meubles séparés. L'enregistrement de chaque combinaison est conservé dans une enveloppe séparée.

40. Les clés, les combinaisons et les enveloppes font l'objet d'une protection aussi rigoureuse que celle des informations auxquelles elles donnent accès.

Équipements approuvés

41. L'autorité de sécurité compétente approuve les murs, sols, plafonds et portes des chambres fortes et des zones de rangement ouvertes construites dans une zone de sécurité de classe I ou II dans laquelle des informations classifiées NC ou d'un niveau de classification supérieur sont stockées sur des étagères non fermées ou exposées aux regards, par exemple tableaux, cartes, etc.

42. Les pays de l'OTAN n'utilisent que des équipements approuvés, par une autorité de sécurité compétente, pour la protection des informations OTAN classifiées.

43. Les organismes civils et militaires de l'OTAN s'assurent que tout équipement acheté a été préalablement approuvé par l'un des pays de l'OTAN pour une utilisation dans des conditions similaires. Ils peuvent également acheter des équipements dont l'utilisation a été approuvée par une autorité de sécurité compétente sur la base d'une évaluation des risques réalisée en vue de réduire ou d'atténuer un ou plusieurs risques identifiés.

Contrôle des visiteurs

44. Le système de contrôle des visiteurs permet de déterminer si un visiteur peut être autorisé à accéder à un site, à un bâtiment ou à une zone où sont stockées, manipulées ou examinées des informations OTAN classifiées.

45. Les visites officielles sont normalement notifiées à l'avance par l'organisme d'appartenance du visiteur. La notification officielle comprend au minimum une description du document d'identification officiel, par exemple un passeport ou une carte d'identité.

46. Les visiteurs, qui doivent être soumis à un système de contrôle adapté, peuvent se déplacer avec ou sans escorte (voir paragraphe suivant).

47. Les procédures de contrôle des visiteurs peuvent varier en fonction des exigences de sécurité locales. Dans tous les cas, les exigences minimales ci-dessous s'appliquent aux visiteurs, qu'ils soient escortés ou non :

(a) visiteurs avec escorte : les visiteurs pour lesquels une escorte est nécessaire sont accompagnés en permanence par un membre du personnel ou un garde possédant une PSC du niveau approprié. Ils peuvent être tenus de porter un laissez-passer qui les identifie comme visiteurs. Leurs coordonnées complètes sont enregistrées.

(b) visiteurs sans escorte : les personnes qui sont titulaires d'une PSC du niveau approprié et qui ont le besoin d'en connaître peuvent être temporairement autorisées à accéder sans escorte à une zone ou à certaines parties d'une zone. Toutefois, ces personnes sont tenues de porter un laissez-passer temporaire qui les identifie comme visiteurs, et de le restituer dès que leur tâche au sein de l'organisme est achevée. Leurs coordonnées complètes sont enregistrées, y compris leurs heures d'arrivée et de départ. Les visiteurs sans escorte ne sont pas autorisés à escorter d'autres visiteurs.

Fouilles à l'entrée et à la sortie

48. Des fouilles aléatoires à l'entrée et à la sortie, visant à dissuader toute personne d'introduire des objets prohibés sur un site ou dans un bâtiment ou d'en sortir sans autorisation du matériel classifié ou non classifié, peuvent être conduites dans les sites ou bâtiments dans lesquels sont stockées ou manipulées des informations OTAN.

49. Les fouilles à l'entrée et à la sortie peuvent être une condition pour entrer sur un site ou dans un bâtiment. Une note est affichée pour avertir que des fouilles peuvent être effectuées aléatoirement à l'entrée et à la sortie.

NORMES MINIMALES POUR LE STOCKAGE DES INFORMATIONS OTAN CLASSIFIÉES

50. Les informations OTAN classifiées sont stockées dans des zones, des armoires fortes ou du mobilier de bureau permettant de décourager et de détecter tout accès non autorisé aux informations.

51. **COSMIC TRÈS SECRET (CTS) :** Les informations CTS sont stockées dans une zone de sécurité de classe I ou II, de l'une des manières suivantes :

(a) dans un meuble de sécurité approuvé, avec l'un des contrôles supplémentaires suivants :

(i) une protection continue par un garde ou un personnel de service habilité ;

(ii) l'inspection du meuble de sécurité, à intervalles variables mais inférieurs à deux heures, par un garde ou un personnel de service habilité ;

(iii) un système de détection des intrusions (IDS) approuvé, associé à une force d'intervention qui, après un signal d'alarme, arrive sur les lieux dans un délai correspondant à celui estimé nécessaire pour enlever ou ouvrir par effraction le meuble de sécurité ou neutraliser les mesures de sécurité en vigueur ;

(b) une zone de rangement ouverte construite conformément aux dispositions de l'appendice 1 à la présente directive, équipée d'un IDS associé à une force d'intervention qui, après un signal d'alarme, arrive sur les lieux dans un délai correspondant à celui estimé nécessaire pour forcer l'entrée ;

(c) une chambre forte équipée d'un IDS associé à une force d'intervention qui, après un signal d'alarme, arrive sur les lieux dans un délai correspondant à celui estimé nécessaire pour forcer l'entrée.

52. **NATO SECRET (NS) :** Les informations NS sont stockées dans une zone de sécurité de classe I ou II, de l'une des manières suivantes :

(a) de la même manière que les informations classifiées CTS ;

(b) dans une chambre forte ou un meuble de sécurité approuvé, sans contrôles supplémentaires ;

(c) dans une zone de rangement ouverte, auquel cas l'un des contrôles supplémentaires ci-après est nécessaire :

(i) l'endroit où se trouve la zone de rangement ouverte fait l'objet d'une protection continue assurée par un garde ou un personnel de service habilité ;

(ii) un garde ou un personnel de service habilité inspecte la zone de rangement ouverte toutes les quatre heures au minimum ;

(iii) un IDS associé à une force d'intervention qui, après un signal d'alarme, arrive sur les lieux dans un délai correspondant à celui estimé nécessaire pour forcer l'entrée.

53. **NATO CONFIDENTIEL (NC) :** Les informations NC sont stockées dans une zone de sécurité de classe I ou II, dans un meuble de sécurité approuvé.

54. **NATO DIFFUSION RESTREINTE (NDR) :** Les informations classifiées NDR sont stockées dans un meuble fermé à clé (p. ex. armoire ou tiroir) situé dans une zone administrative ou dans une zone de sécurité de classe I ou II. Elles peuvent également être stockées dans une armoire fermée à clé, ou dans une armoire forte, ou dans une zone de rangement ouverte homologuée pour la conservation d'informations classifiées NC ou d'un niveau de classification supérieur.

PROTECTION PHYSIQUE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

55. Les zones dans lesquelles des informations OTAN classifiées sont présentées ou manipulées par des moyens informatiques, ou dans lesquelles l'accès à de telles informations est possible, sont établies de telle façon que l'exigence globale de confidentialité, d'intégrité et de disponibilité soit satisfaite.

56. Les zones dans lesquelles des SIC sont utilisés pour afficher, stocker, traiter ou transmettre des informations classifiées NC ou d'un niveau de classification supérieur, ou dans lesquelles l'accès à de telles informations est virtuellement possible, sont déclarées zones de sécurité OTAN de classe I ou II, ou l'équivalent national.

57. Les zones dans lesquelles des SIC sont utilisés pour afficher, stocker, traiter ou transmettre des informations classifiées NDR, ou dans lesquelles l'accès à de telles informations est virtuellement possible, sont déclarées zones administratives.

58. L'accès aux zones où sont hébergés ou gérés des composants SIC critiques (serveurs, équipements réseau, supports de stockage, équipements cryptographiques, etc.) fait l'objet d'un contrôle spécifique et est limité aux seules personnes autorisées appartenant aux services de sécurité ou aux services d'administration des systèmes, des réseaux ou des équipements cryptographiques.

59. Le niveau de protection à accorder aux SIC manipulant des informations OTAN classifiées est déterminé d'après les dispositions de la pièce jointe F au C-M(2002)49 et de ses directives complémentaires.

Protection physique des imprimantes, copieurs et déchiqueteuses

60. Les imprimantes, copieurs, déchiqueteuses et autres équipements utilisés pour reproduire ou détruire des informations OTAN classifiées font l'objet de mesures de protection physique suffisantes pour que seules les personnes autorisées puissent les utiliser et que les informations OTAN classifiées soient contrôlées suivant les prescriptions de la politique de sécurité de l'OTAN et de ses directives complémentaires.

PROTECTION CONTRE LES ATTAQUES TECHNIQUES

61. Les bureaux ou les zones dans lesquels se tiennent régulièrement des discussions faisant intervenir des informations classifiées NS ou d'un niveau de classification supérieur doivent être protégés contre les systèmes d'écoute passive et active, au moyen de mesures de sécurité physique et de contrôles d'accès appropriés, quand le risque le justifie. La question de savoir à qui incombe la responsabilité de déterminer le risque fait l'objet d'une coordination avec les spécialistes des questions techniques et est réglée par l'autorité de sécurité compétente.

62. La protection contre l'écoute passive (c'est-à-dire la fuite d'informations OTAN classifiées à cause de communications non sécurisées ou d'émissions électromagnétiques involontaires) peut nécessiter l'obtention d'avis en matière de sécurité technique.

63. La protection contre l'écoute active (c'est-à-dire la captation d'informations OTAN classifiées par microphones avec ou sans fil ou par d'autres dispositifs installés à cet effet) exige une inspection de sécurité technique et/ou physique de la structure de la pièce, de son ameublement, de son équipement et du matériel de bureau, y compris les appareils de bureau (mécaniques et électriques) et les moyens TIC. Ces inspections sont effectuées par un personnel de sécurité qualifié habilité par l'autorité de sécurité compétente.

Examen des équipements électriques et électroniques

64. Avant d'être utilisés dans une zone où les réunions ou les travaux impliquent l'utilisation d'informations classifiées NS ou d'un niveau de classification supérieur et quand, d'après une évaluation des risques de sécurité, les circonstances font entrevoir un risque élevé, les équipements de communications et les appareils de bureau électriques ou électroniques, quel que soit leur type, sont examinés par des spécialistes de la sécurité technique ou TIC, qui veillent à ce qu'aucune information intelligible ne puisse être émise par inadvertance ou illicitement par ces matériels au-delà du périmètre de la zone de sécurité de classe I ou II.

APPENDICE 1
ANNEXE 1
AC/35-D/2001-REV3

ZONES DE RANGEMENT OUVERTES

1. Les zones de rangement ouvertes sont celles désignées par l'autorité de sécurité compétente pour le stockage d'informations OTAN classifiées dans un espace ouvert. Ces zones sont construites selon les normes ci-dessous.

(a) **Construction**

Les murs périmétriques, les planchers et les plafonds sont d'une construction de type définitif, l'ensemble faisant corps. Toute construction doit être réalisée de façon à permettre de vérifier visuellement qu'il n'y a pas eu d'intrusion.

(b) **Portes**

Les portes sont en bois, en métal ou faites d'un autre matériau solide. Les portes d'entrée sont sécurisées au moyen d'une serrure intégrée à combinaison à trois disques approuvée. Dans des circonstances exceptionnelles, l'autorité de sécurité compétente peut autoriser l'installation d'autres serrures sur les portes d'entrée de zones de rangement d'informations NS et NC. Les portes qui ne sont pas sécurisées au moyen des serrures précitées sont sécurisées de l'intérieur au moyen d'un dispositif à pêne dormant avec déverrouillage d'urgence, d'un pêne dormant, d'une barre rigide en bois ou en métal placée en travers de la porte, ou d'un autre dispositif approuvé par l'autorité de sécurité compétente.

(c) **Aérateurs, conduites et ouvertures diverses**

Tous les aérateurs, conduites et ouvertures similaires de plus de 620 cm² (et de plus de 15 cm dans la partie la moins large) qui débouchent sur ou passent par une zone de rangement ouverte sont protégées au moyen de barreaux, de grilles métalliques, d'écrans insonores ou d'un système de détection des intrusions.

(d) **Fenêtres**

(i) Toutes les fenêtres qui pourraient permettre l'observation visuelle des activités classifiées se déroulant à l'intérieur de la zone sont opacifiées, équipées de volets ou de doubles rideaux, ou autrement masquées.

(ii) Les fenêtres situées au niveau du sol et autres fenêtres d'accès facile (par exemple, à partir d'un toit, d'une véranda ou d'un bâtiment annexe) sont construites dans un matériau qui assure une protection contre toute entrée par effraction, ou recouvertes d'un tel matériau. La protection assurée aux fenêtres ne doit pas nécessairement être plus forte que celle des murs contigus. Les zones de rangement ouvertes qui sont situées dans un ensemble contrôlé ou équivalent n'ont pas besoin d'être protégées contre l'entrée par effraction si les fenêtres sont rendues inutilisables, soit par scellement définitif, soit par l'installation, côté intérieur, d'un mécanisme de verrouillage, et si elles sont munies d'un IDS (directement monté sur la fenêtre ou fonctionnant à l'aide de détecteurs de mouvements installés dans la zone).