



Secrétariat

16 août 2021

Circulaire du Secrétaire général

Destinataires : Fonctionnaires de l'Autorité

Objet : **Classification et utilisation des informations sensibles**

1. La présente circulaire vient définir les procédures de classification et de traitement voulues des données et informations confidentielles confiées à l'Autorité internationale des fonds marins ou émanant de cette dernière, l'objectif étant de mettre en œuvre l'article 168 de la Convention des Nations Unies sur le droit de la mer ainsi que les règles, règlements et procédures de l'Autorité relatifs aux activités de prospection et d'exploration dans la Zone (ci-après, les Règlements).

Section 1

Portée

2. Les dispositions de la présente circulaire s'appliquent en principe à toutes les données et informations confiées à l'Autorité ou émanant de cette dernière, quels qu'en soient la source ou le destinataire.
3. Conformément aux Règlements, le Secrétaire général a pour mission de sauvegarder la confidentialité des données et informations présentées ou communiquées à l'Autorité ou à toute personne participant à un programme ou activité de l'Autorité en application des Règlements ou d'un contrat émis en vertu des Règlements. À cette fin, il arrête, dans le respect des dispositions de la Convention, des procédures appelées à régir le traitement des informations confidentielles. Des procédures complémentaires sont décrites à l'annexe II à la présente circulaire.

Section 2

Gestion des documents et archives de l'Autorité

Définitions

4. Aux fins de la présente circulaire, les définitions ci-après trouvent application :
 - a) Archives : Documents devant être conservés indéfiniment en raison de leur intérêt administratif, budgétaire, juridique ou historique ou de leur valeur d'information ;
 - b) Déclassement : Mesure prise en ce qui concerne tous documents non courants après évaluation, y compris leur transfert dans un local de stockage secondaire ou leur destruction ;



c) Données informatiques ou télématiques : Toutes données ou informations, quels qu'en soient la forme et le support, qui sont ou ont été produites, acheminées, reçues, traitées ou représentées par des moyens informatiques ou télématiques, notamment par courrier électronique ou télécopie ;

d) Document non courant : Tout document ou pièce renfermant des données ou informations qui ne sont plus utilisées quotidiennement pour les activités du service, mais doivent être conservées pour une durée déterminée ;

e) Exploitation pour les besoins du service : Exploitation de moyens informatiques ou télématiques par tout(e) utilisateur(trice) autorisée dans l'exercice de ses fonctions et dans les limites autorisées ;

f) Document (ou document officiel) : Pièce renfermant des données ou informations, quels qu'en soient la forme et le support, conservées par l'Autorité comme preuve de ses activités ;

g) Gestion des documents : Constitution et gestion d'un ensemble de documents renfermant des informations exhaustives, exactes et fiables comme preuve des activités menées ;

h) Plan d'archivage : Directives détaillées établies par un bureau et fixant les modalités de déclasserment des documents, l'idée étant de les conserver aussi longtemps que nécessaire eu égard à leur intérêt administratif, budgétaire, juridique ou historique ou à leur valeur d'information ;

i) Activité : Acte accompli dans l'exercice de ses fonctions par tout fonctionnaire au moyen d'un outil informatique ou télématique ;

j) Document temporaire : Document renfermant des données ou informations d'utilité limitée aux fins de l'exécution de telle ou telle activité ordinaire ou de l'établissement d'un autre document ;

k) Document essentiel : Pièce renfermant des données ou informations essentielles à la bonne marche de l'Autorité et sans lesquelles cette dernière ne pourrait continuer à fonctionner efficacement ou assurer la continuité de ses activités en cas de sinistre ; document contenant des informations nécessaires à la protection des droits et intérêts de l'Autorité, de son personnel et de ses interlocuteurs.

Responsabilités du (de la) fonctionnaire

5. Tous documents, y compris les documents et les messages électroniques établis ou reçus par le (la) fonctionnaire dans l'exercice de ses fonctions à l'Autorité sont la propriété de celle-ci.

6. Le (la) fonctionnaire ne doit pas altérer, détruire, égarer ou rendre inutilisable les pièces, documents ou dossiers censés demeurer dans les archives de l'Autorité. Il (Elle) est autorisé(e) à détruire les pièces et documents conformément aux directives portant délais de conservation arrêtées par le Secrétaire général.

7. Avant de quitter le service de l'Autorité, le (la) fonctionnaire prend toutes dispositions nécessaires pour transférer au bureau dont il (elle) relève tous documents en sa possession qui ne sont plus requis pour les besoins du service et n'emporte aucun document hors des locaux de l'Autorité. Le (La) chef du bureau concerné peut donner conseils et avis au sujet des documents du (de la) fonctionnaire avant sa cessation de service. Le (La) fonctionnaire est autorisé(e) à conserver un nombre raisonnable de documents d'accès non restreint reproduits à ses propres frais ainsi qu'à conserver ses documents privés.

8. Sont considérés comme privés les documents relevant des catégories suivantes :

- a) Notes et journaux personnels ;
 - b) Exemplaires excédentaires de documents imprimés, non classifiés, de l'Autorité ;
 - c) Correspondance personnelle n'ayant pas trait aux fonctions de l'intéressé(e), même si les éléments qui la composent sont conservés dans un bureau du Secrétariat, notamment les invitations à des manifestations mondaines, les lettres de remerciement, les listes de correspondance et autres documents de caractère strictement personnel.
9. Lors de son départ à la retraite, le (la) fonctionnaire peut emporter les documents privés visés au paragraphe 7 ci-dessus.

Responsabilités des bureaux

10. Chaque bureau établit et applique des directives touchant la conservation de leurs documents, y compris temporaires, conformément à des plans d'archivage préalablement approuvés par le Secrétaire général. Ces plans doivent pourvoir à la gestion responsable et transparente des documents, les délais de conservation minimums à respecter pour satisfaire aux prescriptions administratives, budgétaires et juridiques étant précisés, et répertorier les documents à conserver dans les archives de l'Autorité. Les documents de l'Autorité qui ne sont pas visés par des directives de conservation approuvées ne doivent pas pour autant être détruits.
11. Avant de transférer ses documents aux archives de l'Autorité, tout bureau doit les mettre au format fixé par le Secrétaire général.
12. Le bureau n'est pas autorisé à détruire des documents en sa possession sans autorisation expresse consignée dans un plan d'archivage ou autorisation signée par le Secrétaire général, à l'exception de documents temporaires.
13. Tout bureau autorisé à conserver des documents non courants au-delà de la période réglementaire pour s'acquitter de ses fonctions doit en assurer la gestion et la conservation conformément aux normes arrêtées par le Secrétaire général.
14. Tout bureau établit des procédures pour recenser et gérer les documents essentiels dans le cadre du plan global de continuité des opérations et reprise après sinistre du Secrétariat, conformément aux directives arrêtées par le Secrétaire général concernant la définition des documents essentiels.

Documents électroniques

15. Les documents électroniques créés ou gérés au moyen d'un outil informatique ou télématique appartenant à l'Autorité sont soumis aux règles de gestion des documents énoncées dans la présente circulaire. Ils doivent notamment être saisis dans un système d'archivage électronique ou, en l'absence d'un tel système, saisis et gérés à l'aide d'un autre système d'archivage, par exemple sur support papier.
16. Nombre de messages électroniques produits ou reçus par l'Autorité ont valeur documentaire car ils attestent et rendent compte de ses activités. Tout bureau veille à répertorier, gérer et stocker les messages électroniques conformément aux règles de gestion des documents énoncées dans la présente circulaire. Le directeur de l'informatique élabore et diffuse, eu égard aux méthodes de travail et aux pratiques en vigueur, des directives venant définir les utilisations indiquées des systèmes de messagerie électronique comme moyens de communication officiels.

Consultation par le (la) fonctionnaire des archives et documents non courants de l'Autorité

17. Tout fonctionnaire doit avoir accès aux archives et aux documents non courants dont il a besoin pour s'acquitter de ses fonctions, selon les modalités fixées par le Secrétaire général.

18. Les documents autres que ceux contenant des données et informations communiquées en application des Règlements et devant être traités conformément aux dispositions des Règlements et de l'annexe II à la présente circulaire, qui sont classifiés par le Secrétaire général ou tout(e) représentant(e) à ce habilité(e), peuvent être déclassifiés à tout moment par la même autorité.

Section 3

Classification et exploitation d'informations sensibles

Principes de classification

19. La classification des informations confiées à l'Autorité ou émanant de celle-ci repose sur le principe général que ses activités doivent s'exécuter au grand jour et en toute transparence, sauf le cas d'informations réputées confidentielles en application des directives résultant de la présente circulaire.

20. Sont sensibles toutes informations relevant des catégories suivantes :

a) Documents créés par l'Autorité, reçus d'une tierce partie ou adressés à une tierce partie, considérés confidentiels par les parties concernées ;

b) Documents dont la divulgation risquerait de mettre en danger la sûreté ou la sécurité de toute personne, d'enfreindre ses droits ou de porter atteinte à sa vie privée ;

c) Documents couverts par le secret professionnel ou concernant une enquête interne ;

d) Documents internes inter ou intra-services, y compris à l'état de projet, dont la divulgation risquerait de porter atteinte à la liberté et à l'indépendance de l'Autorité en matière de prise de décisions ;

e) Documents contenant des informations commerciales dont la divulgation serait préjudiciable aux intérêts financiers de l'Autorité ou de toute autre partie concernée ;

f) Données et documents communiqués en application des Règlements ;

g) Autres informations devant être considérées confidentielles du fait de leur teneur ou des circonstances de leur création ou de leur communication.

21. Toute décision de classification doit être prise avec discernement, la classification devant être réservée aux seuls cas où la divulgation risquerait de nuire au bon fonctionnement de l'Autorité, au bien-être ou à la sûreté de son personnel ou de tiers, ou encore de violer les obligations légales de l'Autorité. En pareil cas, on se conformera strictement aux procédures ci-après, afin de ne pas compromettre sciemment ou par inadvertance la confidentialité des informations considérées.

Niveaux de classification

22. Les informations sensibles sont susceptibles de recevoir la classification « confidentiel » ou « strictement confidentiel ».

23. La classification « confidentiel » est réservée aux documents ou informations dont on peut raisonnablement penser que la divulgation non autorisée porterait préjudice aux activités de l'Autorité.

24. La classification « strictement confidentiel » est réservée aux documents ou informations dont on peut raisonnablement penser que la divulgation non autorisée pourrait porter très gravement préjudice ou porter atteinte à tout État membre, à toute partie ayant contracté ou souhaitant contracter avec l'Autorité ou aux activités de celle-ci. Les données et informations réputées confidentielles au regard des Règlements doivent toujours porter la mention « strictement confidentiel », sauf décision contraire du Secrétaire général.

25. La classification « non classifié » est réservée aux documents ou informations dont on peut raisonnablement penser que la divulgation non autorisée ne porterait pas préjudice aux activités de l'Autorité.

Identification et désignation

26. L'auteur(e) de toutes informations ou, si elles émanent d'une source extérieure, leur destinataire, agissant sous la supervision et la direction générales du (de la) chef du bureau concerné, décide si ces informations sont sensibles et leur attribue la désignation appropriée, comme indiqué ci-après.

27. Toutes informations émanant d'une source extérieure et déjà revêtues d'une désignation de confidentialité conservent cette désignation ou en reçoivent une de nature à leur garantir un niveau de protection au moins égal à celui conféré par l'entité dont elles émanent.

28. L'auteur(e) de toutes informations ou, si elles émanent d'une source extérieure, leur destinataire, agissant sous la supervision et la direction générales du (de la) chef du bureau concerné, précise si possible si les informations classifiées ne représentent qu'une petite partie du document, le reste n'étant pas classifié.

Déclassification

29. L'auteur(e) de toutes informations ou, si elles émanent d'une source extérieure, leur destinataire, agissant sous la supervision et la direction générales du (de la) chef du bureau concerné, indique, s'il y a lieu, sur le document la date ou l'événement qui en emportera déclassification. La date ou l'événement venu, le document est automatiquement déclassifié. Le délai indiqué ne doit pas dépasser celui fixé au paragraphe 30 de la présente circulaire.

30. S'il n'est pas spécifié de date ou d'événement, les informations pourront être déclassifiées à tout moment par leur auteur(e) ou leur destinataire, si elles émanent d'une source extérieure, par le Secrétaire général ou par tout(e) fonctionnaire à ce habilité(e).

31. Sous réserve des dispositions de tout autre texte administratif ou de tout engagement juridique souscrit par l'Autorité en la matière, il sera procédé à la déclassification de documents transférés au Secrétaire général sous leur désignation originelle comme suit :

a) La classification des documents marqués « strictement confidentiel » est revue au cas par cas par le Secrétaire général ou par tout(e) fonctionnaire à ce habilité(e) à l'expiration d'un délai de 10 ans. Les documents qui ne sont pas déclassifiés à cette occasion font l'objet d'un nouvel examen tous les cinq ans par le Secrétaire général ou par tout(e) fonctionnaire à ce habilité(e), sous réserve des dispositions pertinentes des Règlements, s'agissant de données et informations communiquées en vertu d'un contrat d'exploration ;

b) Les documents marqués « confidentiel » sont automatiquement déclassifiés par le Secrétaire général à l'expiration d'un délai de 10 ans, sous réserve des dispositions pertinentes des Règlements, s'agissant de données et informations communiquées en vertu d'un contrat d'exploration.

32. Avant de déclassifier toutes informations émanant d'une source extérieure, l'Autorité tient dûment compte de la classification décidée par cette source et sollicite, le cas échéant, son consentement.

Traitement d'informations classifiées

33. Le (La) chef de bureau veille à ce que toutes informations classifiées reçues par son bureau ou en émanant soient traitées conformément aux normes minimales ci-après :

a) Toutes informations classifiées doivent être acheminées sous pli ou colis scellés, faisant clairement apparaître leur classification ;

b) Toutes informations classifiées entrantes ou sortantes doivent être consignées dans un registre spécial désignant les fonctionnaires habilités à les traiter ;

c) Toutes informations classifiées ne peuvent être copiées qu'avec l'autorisation de leur(e) auteur(e) ou du (de la) chef du bureau dont elles émanent ou qui les a reçues, constat devant être dressé de toutes copies dans le registre tenu à cet effet ;

d) Toutes informations classifiées doivent être rangées et conservées en lieu sûr, sous clef, dans les locaux du bureau concerné, seuls les fonctionnaires habilités par le (la) chef du bureau pouvant y accéder ;

e) Toutes informations classifiées reçues sous forme électronique doivent être imprimées sur papier dès réception, puis rangées et conservées comme indiqué à l'alinéa d). Le fichier électronique doit être archivé selon les modalités sécurisées indiquées au paragraphe 35 ci-après ;

f) La transmission électronique d'informations classifiées s'opère uniquement par des voies sécurisées, conformément au paragraphe 35.

34. Lorsque des informations classifiées sont communiquées à titre périodique (rapports de situation, points opérationnels, évaluations politiques périodiques, par exemple), le bureau concerné établit un système vérifiable de diffusion et de contrôle desdites informations.

35. Les normes minimales susindiquées sont sans préjudice du pouvoir du (de la) chef de bureau d'instituer des contrôles plus stricts du traitement d'informations classifiées, pour autant que ces contrôles soient compatibles avec les dispositions de la présente circulaire.

36. Le (La) chef de bureau institue, avec le concours du directeur de l'informatique, des procédures propres à garantir que les systèmes informatiques et télématiques, notamment les réseaux et les systèmes de télécommunication, servant à la collecte, à la création, à la transmission, au calcul, à la diffusion, au traitement et au stockage des données classifiées, soient pourvus de moyens de contrôle permettant d'en interdire l'accès à toutes personnes non habilitées et d'en préserver l'intégrité.

37. La destruction par des moyens autorisés de documents classifiés non courants ne présentant plus d'intérêt administratif, budgétaire, juridique ou historique et n'ayant plus valeur d'information doit être autorisée par leur auteur(e) ou par le (la) chef du bureau concerné.

Section 4
Obligations fondamentales du (de la) fonctionnaire et mesures disciplinaires en cas de manquement

Obligations fondamentales

38. Le (La) fonctionnaire est tenu(e) d'obligations fondamentales de respect de la confidentialité de toutes informations et données tel que prescrit par la Convention, le Statut et le Règlement du personnel ainsi que les Règlements :

a) Le (La) fonctionnaire ne doit pas utiliser sa qualité officielle ou des informations dont il (elle) a eu connaissance à l'occasion de ses fonctions pour son intérêt personnel – financier ou autre – ou pour l'intérêt personnel de tiers quels qu'ils soient, y compris les membres de sa famille, ses amis ou protégés ;

b) Le (La) fonctionnaire doit observer la plus stricte réserve sur toutes questions relevant de ses fonctions. Sauf, le cas échéant, dans l'exercice normal de ses fonctions ou avec l'autorisation du Secrétaire général, il (elle) ne doit communiquer à qui que ce soit, gouvernement, entité, personne ou toute autre source, aucun renseignement dont il (elle) a eu connaissance à raison de sa qualité officielle et dont il (elle) sait ou devrait savoir qu'il n'a pas été rendu public. La cessation de service ne dégage pas le (la) fonctionnaire de ces obligations ;

c) Conformément au paragraphe 2 de l'article 168 de la Convention et, sous réserve de leurs obligations envers l'Autorité, le Secrétaire général et le personnel ne doivent divulguer, même après la cessation de leurs fonctions, aucun secret industriel, aucune donnée qui est propriété industrielle et qui a été transférée à l'Autorité en application de l'article 14 de l'annexe III de la Convention, ni aucun autre renseignement confidentiel dont ils ont connaissance à raison de leurs fonctions ;

d) Tout(e) chef de bureau ou fonctionnaire doit informer sans tarder le Secrétaire général de tout manquement aux dispositions de la présente section.

39. Le fait pour tout(e) fonctionnaire de manquer aux obligations résultant de la présente circulaire peut être qualifié de conduite ne donnant pas satisfaction au sens de l'article 10.2 du Statut du personnel, passible d'instance disciplinaire et de sanction disciplinaire pour faute.

40. Sans préjudice des dispositions du chapitre X du Règlement du personnel, les procédures ci-après s'appliquent à tout manquement présumé aux dispositions de la présente circulaire relatives à la confidentialité.

Enquête préliminaire et établissement des faits

41. S'il y a lieu de croire que tel(le) fonctionnaire a manqué à quelque obligation résultant de la présente circulaire, le (la) chef ou le (la) responsable du bureau dont il (elle) relève ouvre une enquête préliminaire.

42. Si cette enquête semble indiquer que l'allégation est fondée, le (la) chef ou le (la) responsable du bureau en informe immédiatement le Secrétaire général en lui communiquant un exposé détaillé des faits établis et en y joignant tous éléments de preuve documentaires utiles.

43. Si la nature et la gravité de la faute sont propres à justifier le congé administratif du (de la) fonctionnaire en cause, le (la) chef ou le (la) responsable du bureau concerné fait une recommandation motivée dans ce sens. En règle générale, le congé administratif est envisagé si la faute en question est de nature à nuire à autrui ou à l'Autorité ou s'il existe un risque que des éléments de preuve soient détruits ou dissimulés, et s'il n'est pas possible de réaffecter le (la) fonctionnaire.

44. Au vu des éléments de preuve produits, le Secrétaire général apprécie s'il y a lieu à suivre et, dans l'affirmative, s'il y a lieu à congé administratif. Conformément à la disposition 10.4 du Règlement du personnel, le (la) fonctionnaire en congé administratif continue de percevoir son traitement, sauf circonstances exceptionnelles appelant une décision contraire du Secrétaire général.

Contrôle et enquête du directeur de l'informatique

45. Il est systématiquement procédé au suivi technique de l'utilisation des moyens informatiques et télématiques aux fins du dépannage, de l'établissement de diagnostics, de l'analyse statistique et du réglage du fonctionnement desdits moyens, ce qui peut donner lieu à la production de données agrégées aux fins du suivi général de leur utilisation.

46. À la demande du Secrétaire général, le directeur de l'informatique ouvre une enquête.

a) Toutes demandes d'enquête concernant l'utilisation des moyens informatiques et télématiques sous l'empire de la présente section doivent être adressées au Secrétaire général. Faites par écrit, elles décrivent brièvement les données recherchées, le nom du (de la) fonctionnaire ou de la personne en cause et le nom du (de la) fonctionnaire habilitée à recevoir les informations au sein du bureau demandeur ;

b) L'enquête ne commence qu'après que la demande a été approuvée par le Secrétaire général.

47. En cas d'enquête, il sera procédé comme suit :

a) Le (La) fonctionnaire en cause et son (sa) supérieur(e) hiérarchique sont informé(e)s de l'enquête par la personne qui en est chargée juste avant que celle-ci examine les moyens ou données informatiques ou télématiques du (de la) fonctionnaire, y compris les fichiers et le courrier électroniques ainsi que l'historique de l'accès à Internet et à l'intranet ;

b) Les contrôles matériels portant sur les moyens ou données informatiques ou télématiques sont autant que possible effectués en présence de l'intéressé(e), de son (sa) supérieur(e) hiérarchique et d'un(e) représentant(e) du bureau demandeur ;

c) Si l'intégrité de l'enquête le commande, le (la) fonctionnaire peut se voir interdire l'accès aux moyens ou données informatiques ou télématiques objet de l'enquête, y compris les ordinateurs, fichiers électroniques et comptes de messagerie électronique ;

d) Le (La) fonctionnaire habilité(e) du bureau demandeur doit signer, le cas échéant, un reçu accusant réception de toutes les données récupérées ;

e) Le directeur de l'informatique tient en lieu sûr un dossier spécial dans lequel sont consignés un bref énoncé de la demande d'enquête, le nom du demandeur, le compte rendu des actes accomplis dans le cadre de l'enquête, le nom des fonctionnaires qui y ont procédé et le type d'informations récupérées et remises au demandeur ;

f) Les informations récupérées et remises au demandeur ne restent pas en la possession du directeur de l'informatique. L'original de la demande écrite et signée et les reçus relatifs à toutes informations communiquées au bureau demandeur sont conservés dans un dossier distinct tenu en lieu sûr au Bureau exécutif du Secrétaire général ;

g) Les contrôles et enquêtes ne durent que le temps raisonnablement nécessaire pour déterminer si les faits reprochés au (à la) fonctionnaire sont avérés. S'il n'est pas donné suite s'agissant du manquement présumé, le (la) fonctionnaire en est informé(e) par le bureau qui a demandé les contrôles ou l'enquête.

Notification de l'issue de l'enquête au (à la) fonctionnaire

48. S'il décide de donner suite à l'affaire, le Secrétaire général doit :

a) Informer le (la) fonctionnaire par écrit des allégations portées contre lui (elle) et de son droit de réponse ;

b) Lui faire tenir copie de tous éléments de preuve documentaires relatifs à la faute présumée ;

c) Informer le (la) fonctionnaire de son droit de se faire conseiller par un(e) autre fonctionnaire, en activité ou retraité(e), pour exercer son droit de réponse et lui indiquer comment obtenir cette assistance.

49. Si le Secrétaire général décide de mettre le (la) fonctionnaire en congé administratif, celui-ci (celle-ci) doit être informé(e) du motif et de la durée probable de ce congé et rendre sa carte d'accès. Le (La) fonctionnaire en congé administratif ne peut pénétrer dans les locaux de l'Autorité sans en avoir préalablement demandé l'autorisation et devrait se voir accorder la possibilité d'y entrer, si nécessaire sous escorte, pour préparer sa défense ou pour toute autre raison valable.

50. Il est imparti au (à la) fonctionnaire un délai pour répondre aux allégations et, le cas échéant, présenter tous éléments de preuve à décharge. Ce délai s'apprécie au regard de la gravité et de la complexité des allégations. Toute demande de prorogation du délai de la part du (de la) fonctionnaire doit être faite par écrit et justifier valablement pourquoi il (elle) n'est pas en mesure de respecter ce délai. Faute par le (la) fonctionnaire de présenter une réponse dans le délai imparti, la procédure suivra son cours.

51. L'ensemble du dossier, composé des pièces énumérées au paragraphe 47, de la réponse du (de la) fonctionnaire et, le cas échéant, des éléments de preuve produits, est soumis au Secrétaire général.

52. Au vu du dossier complet, le Secrétaire général peut décider de :

a) Clore l'affaire et informer immédiatement le (la) fonctionnaire que les allégations ont été abandonnées et qu'il ne sera donné aucune suite à l'affaire, sans préjudice, le cas échéant, des mesures énoncées aux points i) et ii) de l'alinéa c) de la disposition 10.3 du Règlement du personnel ;

b) Renvoyer l'affaire devant le Comité paritaire de discipline pour avis si les faits semblent indiquer qu'une faute a été commise ; ou

c) Renvoyer le (la) fonctionnaire sans préavis s'il ressort des éléments de preuve qu'il (elle) a commis une faute dont la gravité justifie son renvoi sans préavis.

53. Il est procédé à toutes instances disciplinaires conformément aux dispositions du chapitre X du Règlement du personnel.

54. Tout manquement de la part du (de la) fonctionnaire de l'Autorité aux obligations résultant du paragraphe 2 de l'article 168 de la Convention donne lieu, à la demande de l'État partie lésé par un tel manquement ou de toute personne physique ou morale patronnée par tout État partie conformément à l'article 153, paragraphe 2, alinéa b) de la Convention, et lésée par un tel manquement, au renvoi par l'Autorité du (de la) fonctionnaire en cause devant un tribunal spécial composé de trois personnes qualifiées, nommées par le Secrétaire général de l'Organisation des

Nations Unies. La partie lésée a le droit de participer à l'instance. Si le tribunal le recommande, le Secrétaire général licencie le (la) fonctionnaire en cause.

Section 5

Dispositions finales

55. Les dispositions de la présente circulaire ne s'appliquent pas à la classification et au traitement des documents expressément visés par d'autres circulaires ou textes administratifs adoptés par le Secrétaire général, ou par des engagements juridiques souscrits par l'Autorité envers des tiers.

56. La présente circulaire prend effet à sa date de publication.

57. La circulaire du Secrétaire général [ISBA/ST/SGB/2011/03](#) est remplacée, étant entendu que l'Annexe II de la présente circulaire reste applicable à la Commission juridique et technique conformément à la décision du Conseil [ISBA/22/C/28](#).

Le Secrétaire général
(*Signé*) Michael W. Lodge

Annexe I

Dispositions pertinentes de la Convention et des règles, règlements et procédures de l'Autorité

Convention des Nations Unies sur le droit de la mer

Article 168

Caractère international du Secrétariat

1. Dans l'exercice de leurs fonctions, le Secrétaire général et le personnel ne sollicitent et n'acceptent d'instructions d'aucun gouvernement ni d'aucune autre source extérieure à l'Autorité. Ils s'abstiennent de tout acte incompatible avec leur qualité de fonctionnaires internationaux et ne sont responsables qu'envers l'Autorité. Chaque État partie s'engage à respecter le caractère exclusivement international des fonctions du Secrétaire général et du personnel et à ne pas chercher à les influencer dans l'exécution de leur tâche. Tout manquement à ses obligations de la part d'un fonctionnaire est soumis à un tribunal administratif désigné selon les règles, règlements et procédures de l'Autorité.

2. Le Secrétaire général et le personnel ne doivent posséder d'intérêts financiers dans aucune des activités touchant l'exploration et l'exploitation dans la Zone. Sous réserve de leurs obligations envers l'Autorité, ils ne doivent divulguer, même après la cessation de leurs fonctions, aucun secret industriel, aucune donnée qui est propriété industrielle et qui a été transférée à l'Autorité en application de l'article 14 de l'annexe III, ni aucun autre renseignement confidentiel dont ils ont connaissance à raison de leurs fonctions.

3. Les manquements de la part d'un fonctionnaire de l'Autorité aux obligations énoncées au paragraphe 2 donnent lieu, à la demande d'un État partie lésé par un tel manquement ou d'une personne physique ou morale patronnée par un État partie conformément à l'article 153, paragraphe 2, alinéa b), et lésée par un tel manquement, à des poursuites de l'Autorité contre le fonctionnaire en cause devant un tribunal désigné selon les règles, règlements et procédures de l'Autorité. La partie lésée a le droit de participer à la procédure. Si le tribunal le recommande, le Secrétaire général licencie le fonctionnaire en cause.

4. Les règles, règlements et procédures de l'Autorité prévoient les modalités d'application du présent article.

Annexe III

Article 14

Communication de données

1. Conformément aux règles, règlements et procédures de l'Autorité et selon les conditions et modalités du plan de travail, l'exploitant communique à l'Autorité, à des intervalles fixés par elle, toutes les données qui sont à la fois nécessaires et pertinentes en vue de l'exercice effectif par les principaux organes de l'Autorité de leurs pouvoirs et fonctions en ce qui concerne le secteur visé par le plan de travail.

2. Les données communiquées au sujet du secteur visé par le plan de travail et réputées être propriété industrielle ne peuvent être utilisées qu'aux fins énoncées au présent article. Les données qui sont nécessaires à l'élaboration par l'Autorité des règles, règlements et procédures relatifs à la protection du milieu marin et à la sécurité, autres que les données relatives à la conception de l'équipement, ne sont pas réputées être propriété industrielle.

3. L'Autorité s'abstient de communiquer à l'Entreprise ou à quiconque est étranger à l'Autorité les données qui lui sont fournies par des prospecteurs, des demandeurs

de contrat et des contractants et qui sont réputées être propriété industrielle, mais les données concernant le secteur réservé peuvent être communiquées à l'Entreprise. L'Entreprise s'abstient de communiquer à l'Autorité ou à quiconque est étranger à l'Autorité les données de ce type qui lui sont fournies de la même façon.

Règlement relatif à la prospection et à l'exploration des nodules polymétalliques dans la Zone¹

Article 36

Confidentialité des données et informations

1. Sont réputées confidentielles les données et informations présentées ou communiquées à l'Autorité, ou à toute personne participant à un programme ou activité de l'Autorité en application du [...] Règlement [relatif à la prospection et à l'exploration des nodules polymétalliques dans la Zone] ou d'un contrat émis en vertu du présent Règlement, que le contractant, en consultation avec le Secrétaire général, a désignées comme telles, à moins qu'il ne s'agisse de données et informations :

- a) Qui sont de notoriété publique ou facilement accessibles auprès d'autres sources ;
- b) Que leur propriétaire a antérieurement rendues accessibles sans obligation de confidentialité ; ou
- c) Dont l'Autorité est déjà en possession sans obligation de confidentialité.

2. Les données et informations qui sont nécessaires à l'élaboration par l'Autorité des règles, règlements et procédures relatifs à la protection et à la préservation du milieu marin et à la sécurité, autres que les données relatives à la conception de l'équipement réputées être propriété industrielle, ne sont pas considérées comme confidentielles.

3. Le Secrétaire général, le personnel du Secrétariat, autorisé par le Secrétaire général, et les membres de la Commission juridique et technique ne peuvent utiliser les données et informations confidentielles que dans la mesure nécessaire à l'exercice effectif de leurs attributions et fonctions. Le Secrétaire général n'en autorise l'accès aux membres du personnel du Secrétariat et de la Commission juridique et technique que dans le cadre de leurs fonctions et attributions et pour un usage précis.

4. Dix ans après la date à laquelle les données et informations confidentielles ont été communiquées à l'Autorité ou après la date d'expiration du contrat d'exploration, la date la plus tardive étant retenue, et tous les cinq ans par la suite, le Secrétaire général et le contractant passent en revue ces données et informations pour déterminer lesquelles doivent demeurer confidentielles. Demeurent confidentielles celles dont le contractant considère que leur divulgation serait susceptible de lui causer injustement un grave préjudice économique. Aucune donnée ou information n'est divulguée avant que le contractant n'ait raisonnablement eu la possibilité d'épuiser les recours judiciaires prévus à la section 5 de la partie XI de la Convention.

5. Si, à tout moment après l'expiration du contrat d'exploration, le contractant conclut un contrat d'exploitation relatif à un secteur de la zone d'exploration, les données et informations confidentielles se rapportant à ce secteur restent confidentielles, conformément au contrat d'exploitation.

6. Le contractant peut, à tout moment, lever la confidentialité des données et informations.

¹ ISBA/19/A/9 et ISBA/19/C/17, annexe.

*Article 37**Protection de la confidentialité*

1. Le Secrétaire général veille au respect de la confidentialité de toutes les données et informations et ne les divulgue pas à des personnes extérieures à l'Autorité, sauf autorisation écrite préalable du contractant. Pour garantir la confidentialité des données et informations, il met au point des procédures conformément aux dispositions de la Convention qui régissent l'utilisation d'informations confidentielles par le Secrétariat, les membres de la Commission juridique et technique et toute autre personne participant à une activité ou un programme de l'Autorité. Ces procédures consistent notamment :

a) À conserver en lieu sûr les données et informations confidentielles et à prévoir des mesures de sécurité pour prévenir tout accès non autorisé à ces données et informations ou leur saisie ;

b) À mettre au point un système de classement, d'enregistrement et d'inventaire de toutes les données et informations écrites reçues, y compris le type, l'origine et le cheminement de ces données et informations depuis leur réception jusqu'à leur dernière utilisation.

2. Les personnes autorisées qui ont accès à des données et informations confidentielles en vertu du présent Règlement ne les divulguent pas, sauf dans les cas prévus par la Convention et le présent Règlement. Le Secrétaire général demande à toute personne ayant accès à des données et informations confidentielles de faire une déclaration écrite en sa présence ou en présence de son représentant accrédité, aux termes de laquelle cette personne :

a) Reconnaît qu'elle est légalement tenue, en vertu de la Convention et du présent Règlement, de ne pas divulguer les données et informations confidentielles ;

b) S'engage à respecter les règles et procédures établies pour garantir la confidentialité de ces données et informations.

3. La Commission juridique et technique protège la confidentialité de toutes les données et informations qui lui sont communiquées conformément au présent Règlement ou à un contrat émis en vertu du présent Règlement. En application du paragraphe 8 de l'article 163 de la Convention, les membres de la Commission, même après la cessation de leurs fonctions, ne divulguent aucun secret industriel, aucune information réputée propriété industrielle communiquée à l'Autorité conformément à l'article 14 de l'annexe III à la Convention, ni aucune autre donnée ou information confidentielle dont ils ont eu connaissance dans l'accomplissement des fonctions qu'ils ont exercées pour le compte de l'Autorité.

4. Le Secrétaire général et le personnel de l'Autorité ne divulguent, même après la cessation de leurs fonctions, aucun secret industriel, aucune information réputée propriété industrielle et qui a été communiquée à l'Autorité en application de l'article 14 de l'annexe III à la Convention, ni aucun autre renseignement confidentiel dont ils ont eu connaissance dans l'accomplissement des fonctions qu'ils ont exercées pour le compte de l'Autorité.

5. Compte tenu de sa responsabilité et de l'obligation qui lui incombent de réparer les dommages causés en vertu de l'article 22 de l'annexe III à la Convention, l'Autorité peut prendre les mesures appropriées contre toute personne qui, ayant eu accès, de par ses fonctions à l'Autorité, à des données et informations confidentielles, a violé l'obligation de confidentialité énoncée dans la Convention et dans le présent Règlement.

Règlement relatif à la prospection et à l'exploration des sulfures polymétalliques dans la Zone²

Article 38

Confidentialité des données et informations

1. Sont réputées confidentielles les données et informations présentées ou communiquées à l'Autorité, ou à toute personne participant à un programme ou activité de l'Autorité en application du [...] Règlement [relatif à la prospection et à l'exploration des sulfures polymétalliques dans la Zone] ou d'un contrat émis en vertu du présent Règlement, que le contractant, en consultation avec le Secrétaire général, a désignées comme telles, à moins qu'il ne s'agisse de données et informations :

- a) Qui sont de notoriété publique ou facilement accessibles auprès d'autres sources ;
- b) Que leur propriétaire a antérieurement rendues accessibles sans obligation de confidentialité ; ou
- c) Dont l'Autorité est déjà en possession sans obligation de confidentialité.

Les données et informations qui sont nécessaires à l'élaboration par l'Autorité des règles, règlements et procédures relatifs à la protection et à la préservation du milieu marin et à la sécurité, autres que les données relatives à la conception de l'équipement qui sont de propriété industrielle, ne sont pas considérées comme confidentielles.

2. Le Secrétaire général, le personnel du Secrétariat, autorisé par le Secrétaire général, et les membres de la Commission juridique et technique ne peuvent utiliser les données et informations confidentielles que dans la mesure nécessaire à l'exercice effectif de leurs attributions et fonctions. Le Secrétaire général n'en autorise l'accès aux membres du personnel du Secrétariat et de la Commission juridique et technique que dans le cadre de leurs fonctions et attributions et pour un usage précis.

3. Dix ans après la date à laquelle les données et informations confidentielles ont été communiquées à l'Autorité ou après la date d'expiration du contrat d'exploration si celle-ci est postérieure, et tous les cinq ans par la suite, le Secrétaire général et le contractant passent en revue ces données et informations pour déterminer lesquelles doivent demeurer confidentielles. Demeurent confidentielles celles dont le contractant considère que leur divulgation serait susceptible de lui causer injustement un grave préjudice économique. Aucune donnée ou information n'est divulguée avant que le contractant n'ait raisonnablement eu la possibilité d'épuiser les recours judiciaires prévus à la section 5 de la partie XI de la Convention.

4. Si, à tout moment après l'expiration du contrat d'exploration, le contractant conclut un contrat d'exploitation relatif à un secteur de la zone d'exploration, les données et informations confidentielles se rapportant à ce secteur restent confidentielles, conformément au contrat d'exploitation.

5. Le contractant peut, à tout moment, lever la confidentialité des données et informations.

Article 39

Protection de la confidentialité

1. Le Secrétaire général veille au respect du caractère confidentiel de toutes les données et informations et ne les divulgue pas à des personnes extérieures à l'Autorité, sauf autorisation écrite préalable du contractant. Pour garantir la confidentialité des données et informations, il met au point des procédures,

² ISBA/16/A/12/Rev.1, annexe.

conformément aux dispositions de la Convention, qui régissent l'utilisation d'informations confidentielles par le Secrétariat, les membres de la Commission juridique et technique et toute autre personne participant à une activité ou un programme de l'Autorité. Ces procédures consistent notamment :

a) À conserver en lieu sûr les données et informations confidentielles et à prévoir des mesures de sécurité pour prévenir tout accès non autorisé à ces données et informations ou leur saisie ;

b) À mettre au point un système de classement, d'enregistrement et d'inventaire de toutes les données et informations écrites reçues, y compris le type, l'origine et le cheminement de ces données et informations depuis leur réception jusqu'à leur dernière utilisation.

2. Les personnes autorisées à accéder à des données et informations confidentielles en vertu du présent Règlement ne les divulguent pas, sauf dans les cas prévus par la Convention et le présent Règlement. Le Secrétaire général demande à toute personne ayant accès à des données et informations confidentielles de faire une déclaration écrite en sa présence ou en présence de son représentant accrédité, aux termes de laquelle cette personne :

a) Reconnaît qu'elle est légalement tenue, en vertu de la Convention et du présent Règlement, de ne pas divulguer les données et informations confidentielles ;

b) S'engage à respecter les règles et procédures établies pour garantir le caractère confidentiel de ces données et informations.

3. La Commission juridique et technique protège la confidentialité de toutes les données et informations qui lui sont communiquées conformément au présent Règlement ou à un contrat émis en vertu du présent Règlement. En application de l'article 163, paragraphe 8, de la Convention, les membres de la Commission ne doivent divulguer, même après la cessation de leurs fonctions, aucun secret industriel, aucune donnée qui est propriété industrielle et qui a été communiquée à l'Autorité en application de l'article 14 de l'annexe III de la Convention, ni aucun autre renseignement confidentiel dont ils ont connaissance à raison de leurs fonctions au service de l'Autorité.

4. Le Secrétaire général et le personnel de l'Autorité ne doivent divulguer, même après la cessation de leurs fonctions, aucun secret industriel, aucune information qui est propriété industrielle et qui a été communiquée à l'Autorité en application de l'article 14 de l'annexe III à la Convention, ni aucun autre renseignement confidentiel dont ils ont connaissance à raison de leurs fonctions au service de l'Autorité.

5. Compte tenu de sa responsabilité visée à l'article 22 de l'annexe III de la Convention, l'Autorité peut prendre des mesures appropriées contre toute personne qui, à raison de fonctions au service de l'Autorité, a accès à des données et informations confidentielles et n'a pas observé les obligations de confidentialité énoncées dans la Convention et dans le présent Règlement.

Règlement relatif à la prospection et à l'exploration des encroûtements cobaltifères de ferromanganèse dans la Zone³

Article 38

Confidentialité des données et informations

1. Sont réputées confidentielles les données et informations présentées ou communiquées à l'Autorité, ou à toute personne participant à un programme ou une

³ ISBA/18/A/11, annexe.

activité de l'Autorité en application du [...] Règlement [relatif à la prospection et à l'exploration des encroûtements cobaltifères de ferromanganèse dans la Zone] ou d'un contrat émis en vertu du présent Règlement, que le contractant, en consultation avec le Secrétaire général, a désignées comme telles, à moins qu'il ne s'agisse de données et informations :

- a) Qui sont de notoriété publique ou facilement accessibles auprès d'autres sources ;
- b) Que leur propriétaire a antérieurement rendues accessibles sans obligation de confidentialité ; ou
- c) Dont l'Autorité est déjà en possession sans obligation de confidentialité.

2. Les données et informations qui sont nécessaires à l'élaboration par l'Autorité des règles, règlements et procédures relatifs à la protection et à la préservation du milieu marin et à la sécurité, autres que les données relatives à la conception de l'équipement qui sont de propriété industrielle, ne sont pas considérées comme confidentielles.

3. Le Secrétaire général, le personnel du Secrétariat, avec l'autorisation du Secrétaire général, et les membres de la Commission juridique et technique peuvent utiliser les données et informations confidentielles uniquement dans la mesure nécessaire à l'exercice effectif de leurs attributions et fonctions. Le Secrétaire général n'en autorise l'accès aux membres du personnel du Secrétariat et de la Commission juridique et technique que dans le cadre de leurs fonctions et attributions et pour un usage précis.

4. Dix ans après la date à laquelle les données et informations confidentielles ont été communiquées à l'Autorité ou la date d'expiration du contrat d'exploration si celle-ci est postérieure, et tous les cinq ans par la suite, le Secrétaire général et le contractant passent en revue ces données et informations pour déterminer si elles doivent demeurer confidentielles. Demeurent confidentielles celles dont le contractant considère que la divulgation serait susceptible de lui causer injustement un grave préjudice économique. Aucune donnée ou information n'est divulguée avant que le contractant n'ait raisonnablement eu la possibilité d'épuiser les recours judiciaires dont il dispose conformément à la section 5 de la partie XI de la Convention.

5. Si, à tout moment après l'expiration du contrat d'exploration, le contractant conclut un contrat d'exploitation relatif à un secteur de la zone d'exploration, les données et informations confidentielles se rapportant à ce secteur restent confidentielles, conformément au contrat d'exploitation.

6. Le contractant peut, à tout moment, lever la confidentialité des données et informations.

Article 39

Protection de la confidentialité

1. Le Secrétaire général veille au respect du caractère confidentiel de toutes les données et informations et ne les divulgue pas à des personnes extérieures à l'Autorité, sauf autorisation écrite préalable du contractant. Pour garantir la confidentialité des données et informations, il met au point des procédures, conformément aux dispositions de la Convention, qui régissent l'utilisation des informations confidentielles par le Secrétariat, les membres de la Commission juridique et technique et toute autre personne participant à une activité ou un programme de l'Autorité. Ces procédures consistent notamment :

a) À conserver en lieu sûr les données et informations confidentielles et à prévoir des mesures de sécurité pour prévenir tout accès non autorisé à ces données et informations ou leur saisie ;

b) À mettre au point un système de classement, d'enregistrement et d'inventaire de toutes les données et informations écrites reçues, y compris le type, l'origine et le cheminement de ces données et informations depuis leur réception jusqu'à leur dernière utilisation.

2. Les personnes autorisées à accéder à des données et informations confidentielles en vertu du présent Règlement ne les divulguent pas, sauf dans les cas prévus par la Convention et le présent Règlement. Le Secrétaire général demande à toute personne ayant accès à des données et informations confidentielles de faire une déclaration écrite en sa présence ou en présence de son représentant accrédité, aux termes de laquelle cette personne :

a) Reconnaît qu'elle est juridiquement tenue, en vertu de la Convention et du présent Règlement, de ne pas divulguer les données et informations confidentielles ;

b) S'engage à respecter les règles et procédures établies pour garantir le caractère confidentiel de ces données et informations.

3. La Commission juridique et technique protège la confidentialité de toutes les données et informations qui lui sont communiquées conformément au présent Règlement ou à un contrat émis en vertu du présent Règlement. En application de l'article 163, paragraphe 8, de la Convention, les membres de la Commission ne doivent divulguer, même après la cessation de leurs fonctions, aucun secret industriel, aucune donnée qui est propriété industrielle et qui a été communiquée à l'Autorité en application de l'article 14 de l'annexe III de la Convention, ni aucun autre renseignement confidentiel dont ils ont connaissance à raison de leurs fonctions au service de l'Autorité.

4. Le Secrétaire général et le personnel de l'Autorité ne doivent divulguer, même après la cessation de leurs fonctions, aucun secret industriel, aucune donnée qui est propriété industrielle et qui a été communiquée à l'Autorité en application de l'article 14 de l'annexe III de la Convention, ni aucun autre renseignement confidentiel dont ils ont connaissance à raison de leurs fonctions au service de l'Autorité.

5. Compte tenu de sa responsabilité visée à l'article 22 de l'annexe III de la Convention, l'Autorité peut prendre des mesures appropriées contre toute personne qui, à raison de fonctions au service de l'Autorité, a accès à des données et informations confidentielles et n'a pas observé les obligations de confidentialité énoncées dans la Convention et dans le présent Règlement.

Annexe II

Procédures complémentaires relatives à l'utilisation des données et des informations présentées ou communiquées à l'Autorité en application de l'annexe III de la Convention et des règles, règlements et procédures de l'Autorité

Objet et portée

1. Les dispositions de la présente annexe s'appliquent en sus des directives générales résultant de la présente circulaire.

2. Les dispositions de la présente annexe s'appliquent spécialement aux données et informations présentées ou communiquées à l'Autorité, ou à toute personne participant à un programme ou une activité de l'Autorité en application des règles, règlements et procédures de l'Autorité (ci-après, les Règlements) ou d'un contrat émis en vertu des Règlements. Conformément aux Règlements, les dispositions de l'annexe portent sur :

a) La conservation en lieu sûr des données et informations confidentielles et la définition de mesures de sécurité visant à prévenir tout accès non autorisé à ces données et informations ou leur saisie ;

b) La mise au point d'un système de classement, d'enregistrement et d'inventaire de toutes les données et informations écrites reçues, y compris le type, l'origine et le cheminement de ces données et informations depuis leur réception jusqu'à leur dernière utilisation.

3. Les données et informations visées à cette annexe sont réputées confidentielles à moins qu'il ne s'agisse de données et informations :

a) Qui sont de notoriété publique ou facilement accessibles auprès d'autres sources ;

b) Que leur propriétaire a antérieurement rendues accessibles sans obligation de confidentialité ; ou

c) Dont l'Autorité est déjà en possession sans obligation de confidentialité.

4. Le Secrétaire général doit veiller au traitement sécurisé de toutes données et informations visées au paragraphe 2. Il doit en particulier prendre les mesures techniques et organisationnelles nécessaires, comme décrit dans la présente disposition, afin de protéger ces données et informations contre toute destruction accidentelle ou illicite, perte accidentelle, altération, diffusion ou tout accès non autorisés, ainsi que contre toute autre forme de traitement non indiqué. Vu la complexité et le coût de leur mise en œuvre, ces mesures doivent pourvoir à un niveau de sécurité adéquat au regard des risques présentés par le traitement des données et informations à protéger, et doivent porter sur les aspects suivants :

a) Contrôle de l'accès au système : le système doit pouvoir résister à toute tentative d'intrusion de la part de personnes non autorisées ;

b) Contrôle de l'authenticité et de l'accès aux données : le système est conçu pour faire en sorte de limiter l'accès des parties autorisées à un seul ensemble prédéfini de données ;

c) Sécurité des transmissions : le système est conçu pour garantir la transmission de toutes les données et informations en toute sécurité ;

d) Sécurité des données : le système est conçu pour faire en sorte que toutes les données et informations entrantes soient stockées en toute sécurité aussi longtemps que nécessaire et qu'elles ne puissent pas être falsifiées ;

e) Procédures de sécurité : les procédures de sécurité tiennent compte des problèmes d'accès au système (matériel et logiciel), d'administration et de maintenance du système, de sauvegarde et d'utilisation générale du système.

Procédures générales de sécurité

5. Toutes données et informations visées dans la présente annexe, qu'elles soient sous format papier ou électronique, doivent être gardées en lieu sûr sous l'autorité du Secrétaire général ou de son (sa) représentant(e) à ce habilité(e). Le Secrétaire général doit veiller à ce que seuls les utilisateur(trice)s qu'il a autorisé(e)s ou désigné(e)s puissent y avoir accès dès lors qu'elles sont indispensables à l'exécution de telle ou telle tâche précise. Il n'est pas permis d'établir de copie de ces données et informations, sauf autorisation du Secrétaire général à des fins spécifiques, notamment pour examen par les membres de la Commission juridique et technique et pour utilisation par toute personne identifiée comme participant à un programme ou une activité de l'Autorité en application de la Convention ou des Règlements. Le Secrétaire général doit s'assurer que toutes copies soient numérotées, distribuées après enregistrement dans le système, puis récupérées et détruites rapidement après usage.

Contrôle de l'accès au système

6. Les critères de sécurité des moyens informatiques et télématiques utilisés par le Secrétariat pour stocker, analyser et archiver les données et informations visées dans la présente annexe doivent tendre vers ceux de tout système sécurisé de niveau C2, comme décrit à la section 2.2 du Trusted Computer System Evaluation Criteria (TCSEC) du Département de la défense des États-Unis (DOD 5200.28-STD, décembre 1985). Voici quelques-unes des caractéristiques d'un système sécurité de niveau C2 :

a) Système rigoureux de mot de passe et d'authentification. À chaque utilisateur(trice) est attribué un identifiant unique associé à un mot de passe. À chaque fois qu'il (elle) veut se connecter au système, l'utilisateur(trice) doit donner le mot de passe correct. Une fois connecté, il (elle) a accès aux seules fonctions et données pour lesquelles ses droits d'accès sont configurés. Ont seuls accès à toutes les données les utilisateur(trice)s privilégié(e)s ;

b) Contrôle de l'accès physique au système informatique, y compris identification biométrique obligatoire, système de vidéosurveillance et système d'accès par carte à double bande magnétique ;

c) Vérification. Un enregistrement sélectif des événements permet d'analyser et de détecter toutes atteintes à la sécurité ;

d) Contrôle de l'accès par tranches de temps. La durée de connexion au système peut être limitée à certaines heures de la journée ou certains jours de la semaine ;

e) Contrôle d'accès aux terminaux. Les utilisateur(trice)s autorisé(e)s à accéder aux terminaux sont spécifié(e)s pour chaque poste de travail.

Contrôle d'authenticité et d'accès aux données

7. Les protocoles d'échange de données utilisés pour la transmission électronique des données et informations visées par la présente annexe entre les contractants ou futurs contractants et le Secrétariat doivent être dûment testés par ce dernier.

Sécurité des transmissions

8. Selon que de besoin et s'il y a lieu, il est institué des protocoles de chiffrement soumis aux tests de rigueur par le Secrétariat pour garantir la confidentialité et l'authenticité des transmissions.

Sécurité des données

9. L'accès aux données et aux informations est restreint grâce à un mécanisme souple d'identification et de mot de passe. Les utilisateur(trice)s ne peuvent accéder qu'aux seules données dont ils (elles) ont besoin pour accomplir leurs tâches.

Procédures de sécurité

10. Le Secrétaire général nomme le directeur de l'informatique administrateur du système de sécurité. L'administrateur du système de sécurité vérifie les fichiers journaux générés par le logiciel, assure le bon entretien du système de sécurité, limite l'accès au système selon qu'il convient et assure la liaison avec chaque contractant afin de résoudre tous problèmes de sécurité.

Traitement et utilisation des données et informations

11. Toutes les données et informations présentées par les contractants ou futurs contrats (y compris les demandes d'approbation de plans de travail relatifs à l'exploration) doivent être transférées au Bureau du Secrétaire général, où elles sont enregistrées par des fonctionnaires à ce spécialement habilités par le Secrétaire général, qui déterminent la suite à leur donner. Les procédures d'enregistrement et d'utilisation des données consistent en :

a) La tenue d'un système d'enregistrement et d'inventaire de toutes les données et informations reçues par télécopie, courrier électronique, poste aérienne ou coursier, y compris le type, l'origine et le cheminement de ces données et informations depuis leur réception jusqu'à leur dernière utilisation ;

b) La conservation en lieu sûr des données et informations confidentielles dans la chambre forte de l'Autorité afin de prévenir tout accès non autorisé à ces données et informations ou leur saisie ;

c) La saisie des données électroniques dans un système informatique sécurisé tel que défini dans la présente annexe.

12. Tout(e) fonctionnaire autorisé(e) à accéder aux données et informations confidentielles doit souscrire une déclaration écrite rédigée en la forme suivante et dont il est versé copie dans son dossier personnel.

« Déclaration de confidentialité »

Je soussigné(e) déclare par la présente comprendre qu'à raison de mes fonctions au service de l'Autorité internationale des fonds marins, je serai amené(e) à accéder à des données et informations confidentielles sous forme de demandes, contrats, cartes, rapports, manuels, croquis, diagrammes, correspondance, télécopies, courriers électroniques, documents et programmes informatiques.

Je reconnais être légalement tenu(e), en vertu de la Convention des Nations Unies sur le droit de la mer et des règles, règlements et procédures de l'Autorité, de ne pas divulguer de données et informations confidentielles.

Je m'engage à respecter les règles, règlements et procédures établis pour garantir le caractère confidentiel de ces données et informations.

Je ne dois divulguer, même après la cessation de mes fonctions, aucun secret industriel, aucune information qui est propriété industrielle et qui a été communiquée à l'Autorité en application de l'article 14 de l'annexe III à la Convention, ni aucun autre renseignement confidentiel dont j'ai connaissance à raison de mes fonctions au service de l'Autorité.

Signature :

Nom :

Département :

Date :

Nom du responsable hiérarchique :

Signature :

Rang :

Date :... »
