



OIAC

Conférence des États parties

Première session
Point 39 de l'ordre du jour

C-I/DEC.13/Rev.1
2 février 2006
FRANÇAIS
Original : ANGLAIS

DÉCISION ¹

- **PRINCIPES DIRECTEURS SERVANT À ÉLABORER DES PROCÉDURES RELATIVES À LA DIFFUSION, PAR L'OIAC, D'INFORMATIONS CLASSÉES CONFIDENTIELLES, CONFORMÉMENT À L'ALINÉA C III) DU PARAGRAPHE 2 DE L'ANNEXE SUR LA CONFIDENTIALITÉ**
- **SYSTÈME DE CLASSIFICATION ÉTABLISSANT DES CRITÈRES DE DÉTERMINATION DU NIVEAU DE SENSIBILITÉ DES DONNÉES ET DES DOCUMENTS CONFIDENTIELS, COMPTE TENU DES TRAVAUX PERTINENTS ENTREPRIS POUR PRÉPARER LA CONVENTION, CONFORMÉMENT À L'ALINÉA D DU PARAGRAPHE 2 DE L'ANNEXE SUR LA CONFIDENTIALITÉ**
- **RECOMMANDATIONS DE PROCÉDURES À SUIVRE EN CAS DE MANQUEMENT OU D'ALLÉGATION DE MANQUEMENT À LA CONFIDENTIALITÉ, CONFORMÉMENT AU PARAGRAPHE 18 DE L'ANNEXE SUR LA CONFIDENTIALITÉ (ALINÉAS U, V ET W DU PARAGRAPHE 12 DE LA RÉOLUTION DE PARIS)**

La Conférence des États parties,

Rappelant que la Commission préparatoire a établi un projet de politique de l'OIAC en matière de confidentialité ("la politique de confidentialité") combinant à la fois les questions susmentionnées et les dispositions concernant la composition et le mode de fonctionnement de la Commission pour le règlement des litiges relatifs à la confidentialité ("la Commission de la confidentialité"), comme requis par le paragraphe 23 de l'Annexe sur la confidentialité de la Convention sur l'interdiction des armes chimiques ("l'Annexe sur la confidentialité"),

¹ La version révisée de la Politique de l'OIAC en matière de confidentialité, ci-annexée, contient deux séries de modifications : celles qui sont indiquées dans le document C-I/DEC.13/Corr.1 du 20 mars 2000 et suppriment toute mention du projet de politique de l'OIAC en matière de confidentialité présenté par la Commission préparatoire, et celles qui découlent de la décision C-10/DEC.9 du 10 novembre 2005 contenant des amendements de la Politique de l'OIAC en matière de confidentialité.



Rappelant également que la Commission préparatoire a adopté le projet de politique de l'OIAC en matière de confidentialité annexé au document PC-XI/B/WP.8 du 23 juin 1995 tel que modifié par le Groupe de travail B et a décidé d'appliquer les dispositions de ce projet, *mutatis mutandis*, aux activités de la Commission préparatoire (paragraphe 7.7 du document PC-XI/17 du 27 juillet 1995, Corr.1 du 14 août 1995, et Corr.2, en anglais seulement, du 12 septembre 1995),

Rappelant en outre que la Commission préparatoire a décidé de corriger l'erreur de rédaction commise à l'avant-dernière ligne du paragraphe 6.2 du chapitre VI de la version anglaise du projet de politique de confidentialité en remplaçant le mot "should" par "shall" (paragraphe 8.7 du document PC-XII/17 du 14 décembre 1995),

Sachant que la Commission préparatoire a recommandé, au paragraphe 45.4 de son rapport final (PC-XVI/37 du 15 avril 1997), que la Conférence des États parties ("la Conférence") adopte la politique susmentionnée de confidentialité, telle que modifiée,

Adopte la Politique de l'OIAC en matière de confidentialité susmentionnée, telle que modifiée, jointe en annexe.

Annexe : Politique de l'OIAC en matière de confidentialité

**ORGANISATION POUR L'INTERDICTION
DES ARMES CHIMIQUES**

POLITIQUE DE L'OIAC EN MATIÈRE DE CONFIDENTIALITÉ

La Haye

Mai 1997

Table des matières

Politique de l'OIAC en matière de confidentialité

Chapitre I :	Introduction.....	1
Chapitre II :	Politique générale	3
Chapitre III :	Information et confidentialité	5
Chapitre IV :	Responsabilités fondamentales en matière de confidentialité	9
Chapitre V :	Système de classification de l'information confidentielle de l'OIAC	14
Chapitre VI :	Principes généraux applicables au traitement et à la protection d'informations confidentielles.....	23
Chapitre VII :	Procédures applicables à la diffusion de l'information par l'OIAC	42
Chapitre VIII :	Administration	46
Chapitre IX :	Procédures en cas de manquement à la confidentialité.....	47
	IX.1 : Procédures d'enquête en cas de manquement à la confidentialité	47
	IX.2 : Règles régissant le fonctionnement de la Commission pour le règlement des litiges relatifs à la confidentialité ("la Commission de la confidentialité").....	55
	IX.3 : Rôle des États parties en ce qui concerne les procédures applicables en cas de manquement à la confidentialité	61
Chapitre X :	Rapport annuel sur l'application du régime régissant le traitement de l'information confidentielle par le Secrétariat.....	64
Chapitre XI :	Procédure d'amendement	66
Glossaire	67

Politique de l'OIAC en matière de confidentialité²

² La version originale de la Politique de l'OIAC en matière de confidentialité était ainsi préfacée :

"Le Groupe d'experts sur la confidentialité a mis au point le projet de politique de l'OIAC en matière de confidentialité (annexe au document PC-XI/B/WP.8), que la Commission préparatoire a adopté, avec des modifications, à sa onzième session (paragraphe 7.7 du document PC-XI/17 et paragraphe 7.2 du document PC-XI/B/12). Le projet de politique de l'OIAC en matière de médias et de relations publiques a été mis au point lors des consultations officielles tenues à cet effet (pièce jointe au document PC-X/A/WP.5); la Commission préparatoire l'a provisoirement adopté, avec des modifications, à sa dixième session (paragraphe 6.11 du document PC-X/23 et paragraphe 6.4 du document PC-X/A/3), sous réserve de l'adoption d'autres documents pertinents, dont le projet de politique de l'OIAC en matière de confidentialité.

La Commission préparatoire a aussi décidé que ces deux projets de texte s'appliqueraient *mutatis mutandis* à la Commission préparatoire (paragraphe 7.7 du document PC-XI/17 et paragraphe 6.12 du document PC-X/23).

Le Secrétaire exécutif,

Ian R. Kenyon"

C-I/DEC.13/Rev.1

Annexe

page iv

(page blanche)

CHAPITRE I

INTRODUCTION

1. La présente politique définit les bases de la politique que devra suivre l'Organisation en ce qui concerne la protection du caractère confidentiel des activités liées à l'application de la Convention, la classification de l'information en fonction de son degré de confidentialité et son traitement et les mesures à prendre en cas de manquement à la confidentialité.
2. L'élaboration d'une politique définissant le traitement à réserver à l'information confidentielle est essentielle à l'activité de l'Organisation en raison des mesures de vérification intrusives dont l'objectif est de donner la certitude que la Convention est appliquée, tout en respectant l'inquiétude légitime des États parties quant au risque de divulgation d'informations sensibles. Pour que la vérification soit crédible, il faut une certaine réceptivité de la part des États parties et les activités de vérification doivent être plus ou moins intrusives. La nécessité de divulguer certaines informations pour démontrer que le respect de la Convention va de pair avec l'assurance crédible, pour les États parties, que les mesures appropriées sont prises pour empêcher la divulgation d'informations sans rapport avec la Convention et que toute information confidentielle, une fois divulguée, sera protégée comme il convient.
3. Dans la définition qu'elle donne des droits et des obligations des États parties, la Convention s'efforce par conséquent d'établir un équilibre entre la divulgation nécessaire pour donner l'assurance que la Convention est respectée et les mesures à prendre pour prévenir la divulgation d'informations sans rapport avec la Convention dans le but de sauvegarder la sécurité nationale et les droits de propriété intellectuelle, compte tenu des obligations constitutionnelles des États. Ces deux objectifs ne sont pas nécessairement contradictoires; au contraire, il peut être mis en place un processus de vérification crédible et efficace qui protège activement et entièrement la confidentialité de l'information. Le texte de la Convention donne des assurances concrètes pour que toutes les informations confidentielles soient protégées comme il convient, et donne également l'assurance que les procédures de vérification suivies tendront à prévenir la divulgation d'informations sans rapport avec la vérification du respect de la Convention.

CHAPITRE II

POLITIQUE GÉNÉRALE

1. Le paragraphe 5 de l'Article VIII de la Convention constitue la base de l'obligation pour l'Organisation de respecter la confidentialité de l'information. Cette disposition est ainsi conçue :

"L'Organisation exécute les activités de vérification prévues par la présente Convention de sorte que leurs objectifs soient atteints de la manière la moins intrusive possible dans les délais et avec l'efficacité voulus. Elle ne demande que les informations et données qui lui sont nécessaires pour s'acquitter des responsabilités qui lui sont confiées par la Convention. Elle prend toutes les précautions qui s'imposent pour protéger la confidentialité des informations relatives à des activités et des installations civiles et militaires dont elle a connaissance dans le cadre de l'application de la Convention et, en particulier, elle se conforme aux dispositions de l'Annexe sur la confidentialité."

2. Le paragraphe 6 de l'Article VII de la Convention stipule que chaque État partie :

"traite de façon confidentielle et particulière l'information et les données qu'il reçoit en confiance de l'Organisation concernant l'application de la présente Convention. Il traite cette information et ces données exclusivement dans le cadre des droits et obligations qui sont les siens aux termes de la Convention et en se conformant aux dispositions de l'Annexe sur la confidentialité."

3. Ces stipulations fondamentales sont développées dans plusieurs autres dispositions de la Convention, et spécialement dans l'Annexe sur la confidentialité, ainsi que dans les dispositions exposant en détail les procédures de vérification (par exemple le paragraphe 10 de l'Article VI, les paragraphes 56 et 62 de la deuxième partie et le paragraphe 48 de la dixième partie de l'Annexe sur la vérification). Sur cette base, les éléments fondamentaux de la politique de confidentialité de l'OIAC sont les suivants :

- a) l'Organisation ne demande et ne requiert que les informations nécessaires pour lui permettre de s'acquitter ponctuellement et efficacement de ses responsabilités en vertu de la Convention, et les règles concernant les informations auxquelles un État partie doit permettre à l'Organisation d'avoir accès doivent être spécifiées de manière aussi précise que possible;
- b) les activités de vérification sont conçues, planifiées et exécutées de manière à éviter toute divulgation inutile d'informations confidentielles et tendent à prévenir la divulgation d'informations confidentielles sans rapport avec l'observation de la Convention, dans la mesure où cela est compatible avec l'exécution efficace et ponctuelle des obligations stipulées par la Convention en matière de vérification;

- c) l'Organisation ne demande, ne consigne ni ne conserve d'informations confidentielles sans rapport avec la Convention au cours de la vérification ou d'autres activités, sans préjudice du droit de l'État partie inspecté de demander leur divulgation conformément à la Convention. Une fois divulguées, ces informations sont protégées, ne font l'objet d'aucune autre diffusion et sont détruites comme il convient;
- d) il sera établi des procédures systématiques en vue de limiter l'accès aux informations qui auront été rassemblées et classées confidentielles et la diffusion de ces informations, et le respect desdites procédures sera suivi et contrôlé;
- e) les informations obtenues dans le contexte de l'application de la Convention ne sont publiées ou divulguées de toute autre manière que sur autorisation expresse et conformément aux procédures de divulgation énoncées au chapitre VII de la présente politique;
- f) les procédures de sélection et de formation des fonctionnaires, ainsi que la politique et le règlement du personnel, tiendront compte de la nécessité de faire en sorte que tous les fonctionnaires du Secrétariat possèdent les plus hautes qualités d'efficacité, de compétence et d'intégrité.

CHAPITRE III

INFORMATION ET CONFIDENTIALITÉ

1. La présente section énonce les principes directeurs à appliquer pour comprendre ce que recouvrent dans la pratique des expressions comme "information", "information confidentielle" et "confidentialité". La Convention n'indique pas avec précision comment ces expressions doivent être appliquées, et il est clair qu'elles doivent être définies dans un contexte opérationnel conforme aux différentes responsabilités que la Convention confie à l'Organisation et aux États parties.
2. La façon dont l'Organisation pourra s'acquitter de ses responsabilités dépendra dans une large mesure des informations qu'elle aura obtenues au moyen de ses activités de vérification et de celles qui lui seront fournies par les États parties. Ainsi, l'information parviendra à l'Organisation ou aux fonctionnaires de l'Organisation dans le cadre d'un processus continu d'entrées et de sorties consistant à acquérir, à traiter et à produire les informations nécessaires.
3. Vu que la confidentialité fait partie intégrante de toutes les activités de l'Organisation, l'information peut, d'une façon générale, être considérée en termes opérationnels, c'est-à-dire ses caractéristiques, les moyens par lesquels elle sera acquise et conservée et les supports qui seront utilisés pour la traiter et la transmettre.

Contenu de l'"information"

4. L'expression "**information**" doit être entendue dans un sens très large. L'information est définie par sa capacité ou par la possibilité qu'elle offre de communiquer directement ou indirectement des données ou des connaissances, quelle que soit sa composition ou qu'elle soit tangible ou intangible.
5. Cette expression englobe également tous les moyens d'acquisition, de transmission ou de conservation de connaissances ou de données pouvant être appréhendées, acquises, dérivées ou conservées par tout individu ou par l'Organisation, y compris par son personnel ou son matériel, dans le cadre de l'application de la Convention.
6. L'expression "**données**" apparaît dans la Convention dans plusieurs contextes. D'une façon générale, l'expression "données" tend à désigner une information comportant une structure particulière ou se présentant sous une forme spécifique, comme les informations données dans une déclaration nationale. Toutefois, pour interpréter cette expression du point de vue de la confidentialité, aucune distinction de fond n'est faite entre "information" et "données". Aux fins de la présente politique, par conséquent, l'expression "information" sera réputée englober toutes références aux "données". Les "informations" ou les "données" pourront être des informations incorrectes, fausses ou inexactes.

7. À titre d'illustration de son champ d'application, on considère que l'expression "information" comprend, **mais sans s'y limiter**, les éléments suivants :
- les documents contenant des informations graphiques, schématiques, numériques, symboliques, représentatives, analogiques, photographiques ou écrites;
 - des produits obtenus par la photographie, l'image, l'inspection, l'observation, le traitement de données et le prélèvement et l'analyse d'échantillons;
 - les données stockées ou représentées par des moyens électroniques ou magnétiques ou par tout autre moyen physique;
 - les informations exprimées en termes relatifs ou absolus;
 - les échantillons et autres groupes de produits chimiques y compris les produits chimiques transportés par la terre, la poussière, les filtres et les échantillons, ainsi que le matériel, y compris le matériel de prélèvement et d'analyse d'échantillons et le matériel de sécurité. Les échantillons contiennent des informations et, après analyse, peuvent donner d'autres informations.

L'information peut être acquise ou transmise par tout moyen de communication ou tout sens humain. L'information peut être obtenue et transmise du fait de la simple présence d'une personne en un endroit déterminé ou par l'accès qui est accordé à cette personne. Ainsi, du matériel, des objets, des vêtements et d'autres effets personnels peuvent devenir des sources d'information.

Définitions opérationnelles de certaines formes d'information

8. Les définitions opérationnelles ci-après, qui n'englobent que certaines formes d'information, s'entendent dans le contexte des principes directeurs applicables au traitement et à la protection de l'information conformément à la présente politique. Il doit être entendu que les définitions ci-après sont suffisamment souples pour que les principes directeurs applicables au traitement de l'information puissent être appliqués de façon efficace et concrète :
- l'expression "**document**" peut s'appliquer à divers moyens physiques d'affichage d'informations ou de données;
 - l'expression "**documents informatiques**" englobe tout système informatique de stockage et de traitement, comme les disques, les bandes magnétiques et les disquettes. Cette expression englobe également les ordinateurs portables pouvant être utilisés pour enregistrer des informations pendant une inspection sur place;
 - l'expression "**documents audiovisuels**" englobe les enregistrements magnétiques et bandes vidéo, les pellicules photographiques développées et non développées, y compris les négatifs d'instantanés et leurs épreuves

positives. (Les épreuves positives d'instantanés peuvent également être considérées comme des documents);

- l'expression "**échantillon**" englobe tout moyen de prélèvement d'un échantillon ainsi que toutes autres informations acquises ou dérivées au moyen d'une analyse.

Dans l'application des principes directeurs généraux à tel ou tel type d'information relevant des définitions ci-dessus, il peut y avoir chevauchement (par exemple, la diapositive destinée à une projection peut être considérée comme un document ou comme un matériel audiovisuel, et une copie papier peut être considérée comme un document ou comme un matériel informatique).

Confidentialité de l'information conformément à la Convention

9. L'un des principes fondamentaux du régime de confidentialité, énoncé à l'alinéa *c* du paragraphe 2 de l'Annexe sur la confidentialité, veut qu'aucune information obtenue par l'Organisation dans le cadre de l'application de la Convention ne soit publiée ni divulguée, sauf disposition expresse contraire.
10. Les directives spécifiques énoncées à l'alinéa *a* du paragraphe 2 de l'Annexe sur la confidentialité stipulent que l'information est considérée comme confidentielle :
 - a) si elle est ainsi qualifiée par l'État partie d'où elle provient et auquel elle se rapporte;
 - b) si le Directeur général estime être fondé à craindre que sa diffusion non autorisée ne nuise à l'État partie qu'elle concerne ou aux mécanismes d'application de la Convention.
11. Pour déterminer si une information est confidentielle, le Directeur général ou la personne désignée par lui devra peser et évaluer soigneusement les facteurs suivants :
 - le risque que sa divulgation porte préjudice à un État partie, à une entité d'un État partie, y compris une entreprise commerciale, ou à un ressortissant d'un État partie, ou encore à la Convention ou à l'Organisation;
 - le risque que sa divulgation offre un avantage particulier ou sélectif à un particulier, à un État ou à toute autre entité, y compris à une entreprise commerciale;
 - la nécessité fondamentale d'une vérification efficace de l'application de la Convention;
 - les avantages provenant de la diffusion d'informations de caractère général touchant l'application de la Convention afin de promouvoir son acceptation et de renforcer sa crédibilité.

12. Pour déterminer si les informations qu'il fournit à l'Organisation contiennent des informations confidentielles, l'État partie peut également prendre en considération les facteurs susmentionnés. Le fait de qualifier une information de confidentielle n'affecte aucunement l'obligation qu'a l'État partie de démontrer qu'il respecte la Convention et ne doit pas être invoqué par lui pour dissimuler une inobservation de la Convention. De plus, un État partie ne saurait empêcher la diffusion d'informations qui, conformément à la Convention, doivent être soumises aux États parties selon des modalités spécifiées, que ce soit sur leur demande ou systématiquement.
13. Une fois qu'il a été déterminé qu'une information contient des éléments confidentiels, il faut en déterminer la sensibilité et en limiter l'accès. Généralement, on a recours pour cela à un système de classification, comme défini au chapitre V de la présente politique.

Relation entre l'information et la Convention

14. La relation qui existe entre l'information et les buts de la Convention peut avoir des incidences sur la façon dont les mesures de confidentialité seront appliquées à cette information. Trois catégories importantes peuvent être distinguées dans le contexte de l'application de la Convention :
 - les informations pertinentes dont l'Organisation a besoin pour s'acquitter des responsabilités qui lui incombent en vertu de la Convention ou qui sont fournies par les États parties en application des obligations que leur fait la Convention;
 - les informations sans rapport avec les buts de la Convention auxquelles l'État partie inspecté donne accès pour démontrer son respect de la Convention, ou qu'il divulgue incidemment dans le cadre des activités de vérification;
 - les informations, y compris des informations sensibles, sans rapport avec les buts de la Convention et auxquelles un État partie inspecté refuse l'accès, conformément à ses droits et obligations en vertu de la Convention.
15. Les procédures et activités de vérification doivent tenir compte de ces distinctions. Toutefois, la décision quant à la relation entre l'information et les buts de la Convention pourrait être prise au niveau opérationnel, une telle qualification de l'information dépendant dans une large mesure des divers contextes et circonstances. Les obligations de protection de la confidentialité seront définies par rapport aux informations visées dans chacune de ces catégories.

CHAPITRE IV

RESPONSABILITÉS FONDAMENTALES EN MATIÈRE DE CONFIDENTIALITÉ

1. Responsabilités d'ensemble de l'Organisation

1.1 L'OIAC recevra un volume considérable d'informations confidentielles des États parties et pourra prendre connaissance ou acquérir d'autres informations confidentielles, souvent plus sensibles, lors de ses activités de vérification. Les processus internes de l'OIAC vont eux-mêmes générer d'autres informations confidentielles. L'Organisation, y compris ses éléments constituants, devra par conséquent respecter un certain nombre d'obligations pour protéger la confidentialité de l'information, et en particulier :

- a) ne pas publier ni diffuser de toute autre manière les informations obtenues dans le cadre de l'application de la Convention, si ce n'est conformément aux procédures de diffusion de l'information définies dans le chapitre VII de la présente politique.
- b) concevoir, planifier et mener les activités de vérification de la manière la moins intrusive possible afin d'éviter la divulgation d'informations non pertinentes et de minimiser la divulgation d'informations confidentielles, lorsque cela est compatible avec des activités de vérification efficaces et opportunes;
- c) ne solliciter et ne demander que la divulgation des informations nécessaires aux fins de la Convention, et spécifier la teneur des informations demandées avec autant de précision que possible;
- d) réduire au minimum l'accès aux informations confidentielles sans rapport avec la Convention qui pourraient être divulguées incidemment dans le cadre des activités de vérification, les protéger et empêcher qu'elles soient diffusées plus largement, tout en veillant à ce que les activités de vérification soient efficaces et opportunes;
- e) établir, appliquer et suivre l'application de procédures systématiques en vue de limiter la diffusion d'informations classées confidentielles et l'accès à ces informations.

1.2 Responsabilités du Directeur général

- 1.2.1 C'est le Directeur général qui est expressément et principalement responsable de la protection de l'information confidentielle. Le Directeur général doit établir le régime régissant le traitement de l'information confidentielle par le Secrétariat conformément aux principes directeurs énoncés dans la Convention, y compris son Annexe sur la confidentialité, et dans la présente politique.
- 1.2.2 Le Directeur général doit veiller au respect du régime de confidentialité au sein du Secrétariat et faire rapport chaque année sur l'application de ce régime.
- 1.2.3 Le Directeur général a un rôle central à jouer en cas de manquements avérés ou allégués à la confidentialité. Il doit notamment établir les procédures à suivre et ouvrir des enquêtes, conformément aux procédures applicables en cas de manquement à la confidentialité³, et imposer des sanctions et des mesures disciplinaires conformément au Statut et au Règlement du personnel. Les procédures à suivre devront être conformes aux décisions éventuellement adoptées par la Conférence à ce sujet.
- 1.2.4 Le Directeur général peut prendre l'initiative de demander à tout État partie d'apporter "des précisions concernant le traitement de l'information que lui a communiquée l'Organisation" (paragraphe 4 de l'Annexe sur la confidentialité) et consulter les États parties sur la forme et les délais de ces demandes, conformément aux principes directeurs éventuellement fixés par la Conférence. Le Directeur général pourrait, par exemple, demander à tous les États parties de faire périodiquement rapport sur le traitement des informations confidentielles que leur aurait communiquées l'OIAC.

1.3 Responsabilités du Secrétariat

- 1.3.1 Les responsabilités fondamentales du Secrétariat en matière de confidentialité découlent, pour l'essentiel, de celles qui incombent à l'Organisation et au Directeur général. Toutefois, dans le cadre de l'application pratique de la Convention, la définition, l'exécution et le contrôle des responsabilités qui incombent aux fonctionnaires du Secrétariat de préserver la confidentialité de l'information revêtent une importance capitale. Des obligations particulières s'appliquent aux fonctionnaires du Secrétariat du fait de leur participation aux activités de vérification et du fait qu'ils ont donc accès à des informations confidentielles tant civiles que militaires, et notamment aux informations divulguées par les États parties conformément aux obligations que leur impose la Convention ainsi qu'à des informations sensibles qui pourront être divulguées mais qui sont sans rapport avec les buts de la Convention.

³ Énoncées au chapitre IX ci-après.

1.3.2 Outre les obligations générales esquissées ci-dessus, le Secrétariat a les responsabilités spécifiques ci-après :

- a) évaluer, par l'entremise du service approprié, toutes les données et tous les documents qu'il obtient pour déterminer s'ils contiennent des informations confidentielles;
- b) inclure dans les définitions d'emploi une spécification de l'accès à l'information confidentielle que devra avoir le titulaire de chaque poste;
- c) obtenir des engagements de secret de chaque fonctionnaire ainsi que des organes autorisés extérieurs à l'Organisation, selon que de besoin;
- d) mettre en place un programme permanent de formation et de sensibilisation de tous les fonctionnaires aux questions liées à la confidentialité, et suivre la performance de chaque fonctionnaire en matière de protection de l'information confidentielle, en tant qu'élément explicite du processus d'appréciation du comportement professionnel;
- e) aviser tout État partie, lorsqu'il est envisagé d'accorder à un fonctionnaire l'accès à des informations confidentielles en rapport avec les activités menées sur son territoire ou en tout autre lieu placé sous la juridiction ou sous le contrôle dudit État, au moins 30 jours avant que l'accès à l'information soit accordé au fonctionnaire;
- f) traiter et conserver l'information confidentielle de manière à empêcher l'association directe à l'installation concernée, dans la mesure où cela peut être compatible avec une vérification efficace.

1.3.3 Les responsabilités de chaque fonctionnaire sont définies plus en détail dans l'engagement de secret qui doit être signé par l'intéressé.

1.4 Responsabilités de l'équipe d'inspection

1.4.1 Les responsabilités particulières qui incombent aux membres d'une équipe d'inspection découlent du fait que :

- a) les inspecteurs se trouvant sur place peuvent avoir accès à des informations confidentielles;
- b) l'équipe d'inspection doit négocier avec l'État partie inspecté certaines questions touchant la confidentialité, qui exigent un accord⁴;
- c) l'équipe d'inspection est guidée par son mandat, élabore un plan d'inspection et doit décider des mesures spécifiques à mettre en œuvre pendant l'inspection.

⁴ Par exemple conformément au paragraphe 46 de la dixième partie de l'Annexe sur la vérification et au paragraphe 14 de l'Annexe sur la confidentialité.

1.4.2 Les équipes d'inspection devront par conséquent :

- a) effectuer les inspections de la façon la moins intrusive possible, compatible avec l'accomplissement de sa mission de manière efficace et dans les délais;
- b) planifier l'inspection et prendre en considération les propositions que peut faire l'État partie inspecté, à quelque stade que ce soit de l'inspection, pour protéger du matériel ou des informations sensibles sans rapport avec les armes chimiques;
- c) respecter pleinement les procédures visant à protéger les installations sensibles et à empêcher la divulgation non autorisée de données confidentielles;
- d) ne solliciter que les informations et les données nécessaires à l'exécution du mandat d'inspection;
- e) établir un rapport d'inspection qui ne contient que des faits pertinents à l'application de la Convention;
- f) protéger les informations confidentielles sans rapport avec la Convention dont elles peuvent avoir connaissance pendant les inspections sur place et empêcher que ces informations soient plus largement diffusées;
- g) respecter le droit d'un État partie inspecté de refuser l'accès à des informations sensibles, conformément aux droits et obligations dudit État.

2.1 Responsabilités des États parties

2.1.1 Les États parties doivent traiter les informations reçues de l'Organisation en fonction du niveau de sensibilité indiqué dans leur catégorie de classification. La façon dont les États parties s'acquitteront de cette obligation variera naturellement d'un cas à un autre mais, en règle générale, ces informations devront recevoir au moins le même niveau de protection que celui accordé aux informations ayant une classification nationale comparable ou un caractère de confidentialité comparable au regard des législations nationales. Les États doivent mettre en place ou adapter des moyens appropriés pour traiter et protéger les informations confidentielles de l'OIAC dans le respect des principes énoncés au chapitre VI de la présente politique.

2.1.2 Chaque État partie doit, sur demande, apporter des précisions concernant le traitement de l'information que lui a communiquée l'Organisation. Cette procédure vise à renforcer parmi tous les États parties l'assurance que la confidentialité de l'information est efficacement préservée. Lorsqu'ils répondront à de telles demandes, les États parties devront tout au moins

confirmer que les normes appliquées au traitement de l'information sont conformes aux dispositions du paragraphe 2.1.1. ci-dessus.

2.1.3 Pour préserver le caractère confidentiel de l'information, les États parties doivent garder à l'esprit leur obligation essentielle de démontrer qu'ils observent la Convention, conformément aux dispositions de celle-ci relatives à la vérification.

2.1.4 Les États parties doivent coopérer avec le Directeur général, lui fournir tout l'appui possible lors des enquêtes ouvertes sur les manquements avérés ou allégués à la confidentialité et l'aider à prendre les mesures appropriées conformément aux procédures détaillées applicables en pareil cas si l'enquête fait apparaître qu'il y a eu manquement. Cette obligation pourra inclure la fourniture de précisions sur le traitement accordé à l'information que leur aura communiquée l'Organisation et, le cas échéant, la participation de l'État partie, en tant que partie à un différend, à la procédure de la Commission de la confidentialité au cas où cet organe serait saisi du manquement en question.

2.2 Responsabilités des observateurs

2.2.1 Lorsque l'État partie inspecté accepte, pendant une inspection par mise en demeure, de donner accès à ses installations à un observateur conformément au paragraphe 55 de la dixième partie de l'Annexe sur la vérification, l'observateur risque d'avoir accès à certaines informations confidentielles et il lui incombe par conséquent certaines responsabilités particulières pour ce qui est du traitement et de la protection desdites informations. Ainsi, la façon dont l'observateur traite et protège les informations confidentielles doit être pleinement conforme à toutes les dispositions pertinentes de la Convention, y compris son Annexe sur la confidentialité, ainsi qu'à la présente politique, et en particulier aux dispositions détaillées du chapitre VI relatives au traitement de l'information. Vu qu'il est précisé à l'alinéa *a* du paragraphe 12 de l'Article IX de la Convention que l'observateur est un "représentant" de l'État partie requérant, ces informations sont également sujettes aux dispositions du paragraphe 6 de l'Article VII en ce qui concerne tant l'État partie requérant que l'observateur en sa qualité de représentant dudit État, et elles doivent par conséquent être considérées comme confidentielles et bénéficier d'un traitement spécial.

2.2.2 C'est donc l'État partie requérant qui aura l'entière responsabilité de veiller, et il prendra toutes les mesures nécessaires pour cela, à ce que l'observateur se conforme et soit individuellement soumis à toutes les dispositions pertinentes de la présente politique; l'État partie requérant a également l'entière responsabilité de veiller à ce que soient en place des recours et sanctions juridiques effectifs en cas de manquement à la confidentialité de la part de l'observateur comparables aux mesures prévues en cas de manquement à la confidentialité de la part d'un agent dudit État. Dès lors que des informations confidentielles sont divulguées à l'observateur ou que celui-ci en a connaissance, et indépendamment et sans préjudice de la responsabilité individuelle de l'observateur lui-même, l'État partie requérant devient lui aussi

responsable du traitement et de la protection de ces informations conformément à la Convention et à la présente politique. L'observateur, pour sa part, est lié par toutes les dispositions de la présente politique concernant la protection de l'information confidentielle et doit les respecter, et il ne doit poser aucun acte non autorisé à cet égard.

CHAPITRE V

SYSTÈME DE CLASSIFICATION DE L'INFORMATION CONFIDENTIELLE DE L'OIAC

1. Catégories d'informations confidentielles

1.1 Toutes les informations acquises ou générées par l'Organisation et par ses éléments constitutants et qui sont réputées confidentielles doivent être classées dans des catégories établies correspondant à leur niveau de sensibilité. Le système de classification, tel qu'appliqué, ne porte aucunement atteinte à la nécessité d'une vérification efficace du respect de la Convention et devrait permettre, selon que de besoin, la publication d'informations de caractère général, dont les éléments sensibles auront été expurgés, concernant la mise en œuvre de la Convention dans le but de promouvoir son acceptation et de renforcer sa crédibilité.

1.2 Les facteurs essentiels à prendre en considération pour déterminer le niveau de sensibilité d'une information sont les suivants :

- a) le préjudice potentiel que sa divulgation pourrait causer à un État partie, à une entité d'un État partie, y compris une entreprise commerciale, ou à un ressortissant d'un État partie, ou encore à la Convention ou à l'Organisation;
- b) l'avantage particulier ou sélectif que sa divulgation pourrait présenter pour un particulier, un État ou toute autre entité, y compris une entreprise commerciale.

Ces facteurs correspondent à ceux qui sont utilisés pour déterminer le caractère confidentiel de l'information.

1.3 Sur la base de ces principes directeurs et des critères spécifiques de classification énoncés ci-après, l'information confidentielle sera classée selon les catégories ci-après, par ordre croissant de sensibilité :

- **OIAC RESTREINT**
- **OIAC PROTÉGÉ**
- **OIAC HAUTEMENT PROTÉGÉ**

Le préfixe "**OIAC**", dans la désignation de ces catégories, a simplement pour but de faciliter le traitement d'informations classées en indiquant clairement que les catégories en question sont celles appliquées par l'Organisation, afin d'éviter tout conflit ou risque de confusion avec les différents systèmes de classification nationaux. L'emploi de ce préfixe n'a rien à voir avec l'étendue de la diffusion de l'information.

- 1.4 Il convient de distinguer la catégorie de classification (fondée sur la sensibilité de l'information) de l'étendue de la diffusion de l'information (qui dépend, par exemple, du sujet dont il s'agit, du principe du besoin de connaître et de l'utilisation spécifique à laquelle l'information est destinée). Le niveau de classification n'empêche pas la diffusion d'informations dans les conditions spécifiquement prévues par la Convention, notamment à l'alinéa *b* du paragraphe 2 de l'Annexe sur la confidentialité.
- 1.5 Les informations ne relevant d'aucune des catégories susmentionnées sont réputées non classifiées et pourront être identifiées en conséquence. Les informations non classifiées font l'objet des mesures appropriées de protection de la part de l'Organisation et des États parties pour éviter qu'elles ne soient publiées, à moins que leur publication ne soit spécifiquement autorisée conformément aux procédures spécialement établies à cet effet.
- 1.6 Le niveau de protection accordé à l'information confidentielle dépend de son niveau de sensibilité, tel qu'indiqué par sa catégorie de classification. Chaque État partie et l'Organisation protègent les informations classifiées de l'OIAC émanant tant de l'Organisation elle-même que des États parties conformément à leur niveau de sensibilité, tel qu'indiqué par leur catégorie de classification.

Catégorie de classification : OIAC RESTREINT

CRITÈRE :

- 1.7 Cette catégorie comprend les informations dont la divulgation non autorisée porterait préjudice à l'efficacité ou à la crédibilité de la Convention, ou nuirait aux intérêts d'un État partie ou d'une entreprise commerciale, d'un organe gouvernemental ou d'un ressortissant d'un État partie.

EXEMPLES :

- 1.8 Sauf disposition contraire en raison de la plus grande ou de la moindre sensibilité des données en question, les types d'informations ci-après peuvent être classifiés **OIAC RESTREINT** lorsque les informations sont acquises ou générées par l'Organisation de quelque manière que ce soit :
- a) rapports et déclarations initiaux et annuels communiqués par les États parties en application des Articles III, IV, V et VI de la Convention et conformément à l'Annexe sur la vérification lorsque les États parties dont ils émanent leur accordent ce degré de sensibilité;
 - b) les rapports généraux sur les résultats et l'efficacité des activités de vérification;
 - c) les informations devant être communiquées à tous les États parties conformément à d'autres dispositions de la Convention.

- 1.9 Les autres informations pouvant être classifiées **OIAC RESTREINT** et soumises au régime correspondant peuvent comprendre : la correspondance confidentielle usuelle échangée entre les États parties et le Secrétariat, et les documents de travail internes de l'Organisation qui ne sont pas particulièrement sensibles. Ces informations peuvent comprendre aussi les renseignements sur les processus internes et le processus décisionnel du Secrétariat ainsi que d'autres informations intéressant la gestion ou l'administration dont la divulgation risquerait de porter atteinte à l'efficacité de la mise en œuvre de la Convention par l'Organisation.

DIFFUSION :

- 1.10 Les informations classées dans la catégorie **OIAC RESTREINT** qui doivent être systématiquement communiquées aux États parties conformément à l'alinéa *b* du paragraphe 2 de l'Annexe sur la confidentialité sont diffusées en conséquence.

Catégorie de classification : OIAC PROTÉGÉ

CRITÈRE :

- 1.11 Cette catégorie comprend les informations dont la divulgation non autorisée risque de porter gravement atteinte à l'efficacité ou à la crédibilité de la Convention ou de causer un préjudice aux intérêts d'un État partie ou d'une entreprise commerciale, d'un organe gouvernemental ou d'un ressortissant d'un État partie.

EXEMPLES :

- 1.12 Sauf disposition contraire en raison de la plus grande ou de la moindre sensibilité des données en question, les types d'informations ci-après peuvent être classifiés **OIAC PROTÉGÉ** lorsque les informations sont acquises ou générées par l'Organisation de quelque manière que ce soit :
- a) rapports et déclarations initiaux et annuels communiqués par les États parties en application des Articles III, IV, V et VI de la Convention et conformément à l'Annexe sur la vérification lorsque les États parties dont ils émanent leur accordent ce degré de sensibilité ;
 - b) les informations technologiques non publiées intéressant des procédés et des installations de fabrication, ainsi que les informations techniques concernant des produits industriels;
 - c) les informations moins sensibles ou plus générales intéressant des transactions commerciales et les éléments intervenant dans les coûts des procédés industriels et de la fabrication;

- d) les rapports initiaux détaillés concernant une inspection, y compris les informations touchant les anomalies décelées ou les incidents survenus dans des installations, ainsi que les rapports d'inspection;
- e) les données et informations touchant la planification des inspections par le Secrétariat ainsi que les objectifs de l'inspection d'une installation déterminée;
- f) les accords d'installation, avec toutes leurs annexes;
- g) les informations touchant la confirmation et l'évaluation des informations contenues dans les déclarations, accords d'installation et rapports d'inspection.

Lorsque ces informations ne sont pas jugées pertinentes aux fins de la vérification du respect de la Convention, elles reçoivent normalement, au départ, la classification **OIAC HAUTEMENT PROTÉGÉ**, avant même que leur classification officielle ne soit déterminée, comme spécifié au paragraphe 1.17 du présent chapitre.

DIFFUSION :

- 1.13 Les informations classées dans la catégorie **OIAC PROTÉGÉ** qui doivent être systématiquement communiquées aux États parties conformément à l'alinéa *b* du paragraphe 2 de l'Annexe sur la confidentialité sont diffusées en conséquence.

Catégorie de classification : OIAC HAUTEMENT PROTÉGÉ

CRITÈRE :

- 1.14 Cette catégorie comprend les informations confidentielles sensibles dont la divulgation non autorisée nuirait gravement à l'efficacité ou à la crédibilité de la Convention ou aux buts et à l'objet de celle-ci, ou causerait gravement préjudice, du point de vue de la sécurité nationale ou du secret commercial, aux intérêts d'un État partie ou d'une entreprise commerciale, d'un organe gouvernemental ou d'un ressortissant d'un État partie.

EXEMPLES :

- 1.15 Sauf disposition contraire en raison de la plus grande ou de la moindre sensibilité des données en question, les types d'informations ci-après peuvent être classifiés **OIAC HAUTEMENT PROTÉGÉ** lorsque les informations sont acquises ou générées par l'Organisation de quelque manière que ce soit :
- a) rapports et déclarations initiaux et annuels communiqués par les États parties en application des Articles III, IV, V et VI de la Convention et conformément à l'Annexe sur la vérification lorsque les États parties dont ils émanent leur accordent ce degré de sensibilité;

- b) les échantillons prélevés sur les sites inspectés et les échantillons retournés par les laboratoires désignés, ainsi que les résultats de l'analyse des échantillons;
- c) les informations confidentielles particulièrement sensibles spécialement communiquées par un État partie;
- d) les informations confidentielles auxquelles l'accès n'est nécessaire ou volontairement ou incidemment fourni que lors de la conduite effective d'une inspection sur place, comme :
 - les diagrammes d'opération;
 - les photographies, plans et schémas du site;
 - les données spécifiques intéressant des procédés technologiques et leurs paramètres;
 - les données relatives à l'analyse d'échantillons prélevés et analysés sur place;
 - les informations commerciales sensibles, comme une liste détaillée de clients et les quantités de produits qui leur ont été vendues;
 - toutes autres informations détaillées et hautement spécifiques de caractère technique ou commercial ou intéressant la sécurité nationale.

Lorsque ces informations ne sont pas jugées pertinentes aux fins de la vérification du respect de la Convention, elles reçoivent normalement, au départ, la classification **OIAC HAUTEMENT PROTÉGÉ**, avant même que leur classification officielle ne soit déterminée, comme spécifié au paragraphe 1.17 ci-dessous.

- 1.16 Dans le cas de la plupart des inspections, les informations extrêmement sensibles visées à l'alinéa *d* du paragraphe qui précède, qu'elles soient ou non l'objet d'une classification confidentielle à l'échelle nationale, peuvent être conservées dans l'installation inspectée et n'être communiquées que pour utilisation sur place pendant l'inspection. Lorsque de telles informations ne sont pas sorties du site et que l'accès à ces informations est limité, il n'y a par conséquent pas lieu d'appliquer le processus de classification de l'OIAC au niveau du Secrétariat. Même en pareil cas, l'équipe d'inspection, pendant ses activités, accorde à ces informations une protection au moins égale à celle dont bénéficient les informations classifiées **OIAC HAUTEMENT PROTÉGÉ**. La catégorie dans laquelle ces informations sont classées doit, dans toute la mesure du possible, être spécifiée dans les accords d'installation.

- 1.17 Les informations confidentielles sensibles sans rapport avec la vérification du respect de la Convention qui sont révélées ou rassemblées incidemment par un membre de l'équipe d'inspection ne doivent être enregistrées sous aucune forme que ce soit et leur diffusion ne doit pas sortir du cadre de l'inspection. Lorsque l'accès à de telles informations sensibles est accordé dans le cadre des activités d'inspection, tout membre de l'équipe d'inspection doit leur accorder un niveau de protection au moins égal à celui dont bénéficient les informations classifiées **OIAC HAUTEMENT PROTÉGÉ**, tant et pour autant que l'État partie inspecté ne spécifie pas un traitement ou un niveau de sensibilité particuliers. En pareil cas, l'État partie inspecté peut, dans le cadre du processus d'inspection ou dans un accord d'installation, indiquer (comme prévu au paragraphe 2.5 du présent chapitre) la catégorie dans laquelle ces informations devront initialement être classées. Si de telles informations sensibles sont apportées au Secrétariat par inadvertance ou d'un commun accord avec l'État partie inspecté, elles sont classées dans la catégorie **OIAC HAUTEMENT PROTÉGÉ** et bénéficient de la protection correspondante, à moins que l'État partie inspecté n'en dispose autrement.

DIFFUSION :

- 1.18 Les informations classées dans la catégorie **OIAC HAUTEMENT PROTÉGÉ** qui doivent être systématiquement communiquées aux États parties conformément à l'alinéa *b* du paragraphe 2 de l'Annexe sur la confidentialité sont diffusées en conséquence.

2. Autorité responsable de la classification

- 2.1 Dans le cas des informations dont il a été déterminé qu'elles doivent être classées et qui sont transmises au Secrétariat ou générées par celui-ci, un régime de classification doit obligatoirement être appliqué sur la base des catégories et des principes directeurs susmentionnés sous l'autorité directe du Directeur général. Ce régime comprendra des procédures internes visant à assurer la cohérence du système de classification des documents émanant du Secrétariat et concernant les consultations touchant cette classification et, si besoin est, son autorisation.
- 2.2 La classification desdites informations doit être établie par les autorités suivantes :
- a) dans le cas d'informations confidentielles communiquées par un État partie, ce dernier a compétence pour désigner la catégorie dans laquelle elles devront être initialement classées;
 - si un État communique des informations qui semblent confidentielles sans indiquer leur niveau de sensibilité, le Directeur général ou son représentant devra appliquer une catégorie de classification provisoire et traiter ces informations en conséquence, et il devra consulter sans tarder l'État partie

dont émanent lesdites informations pour confirmer, modifier ou supprimer cette classification provisoire;

- b) dans le cas d'informations confidentielles émanant du Secrétariat, leur auteur devra assigner une classification provisoire, la classification définitive relevant du Directeur général ou de son représentant.
- 2.3 Tout document émanant de l'Organisation qui contient des informations confidentielles doit être classifié à titre provisoire par son auteur. Pour déterminer la catégorie de classification d'un nouveau document émanant de l'Organisation, son auteur tient dûment compte du niveau de sensibilité déjà établi pour les documents ou informations détenus par l'Organisation qui sont en rapport avec ce nouveau document.
- 2.4 Les États parties, aux fins de la détermination de la catégorie de classification des informations confidentielles, tiennent compte de leur niveau de sensibilité et des critères correspondants établis pour chaque catégorie aux paragraphes 1.7, 1.11 et 1.14 ci-dessus. Les indications données ci-dessus à titre d'exemple au sujet des types d'informations pouvant être classées dans chaque catégorie ne portent aucunement atteinte au droit d'un État partie de déterminer la catégorie de classification des informations confidentielles qu'il fournit.

Autorité responsable de la classification pendant les inspections

- 2.5 Au cours d'une inspection ou lors de la formulation d'un accord d'installation, l'État partie inspecté peut désigner la catégorie initiale de classification des informations confidentielles, compte tenu de leur niveau de sensibilité et des critères de classification correspondants. Cette classification initiale est applicable avec effet immédiat pendant la conduite d'une inspection ainsi que pour la communication d'informations confidentielles au Secrétariat une fois l'inspection achevée. Lorsque l'État partie inspecté divulgue à un membre de l'équipe d'inspection des informations confidentielles sensibles sans avoir désigné à cette fin de catégorie officielle pour leur classification, ou lorsque de telles informations sont révélées à un membre de l'équipe d'inspection, ce dernier doit les traiter comme si elles étaient classifiées **OIAC HAUTEMENT PROTÉGÉ**, à moins que l'État partie inspecté n'en dispose autrement.

3. Durée de la classification

- 3.1. En règle générale, la classification déterminée pour une information spécifique demeure applicable tant qu'elle n'a pas été expressément modifiée ou supprimée, conformément aux directives pertinentes. Lorsqu'il communique des informations confidentielles, un État partie peut indiquer la durée pendant laquelle la classification doit leur être appliquée. Faute d'indication, cette durée est réputée illimitée.

- 3.2 Pour assurer une protection viable et efficace des informations confidentielles, promouvoir l'efficacité de la vérification du respect de la Convention et encourager une meilleure compréhension de l'ensemble du système de vérification et réduire le volume des archives dans lesquelles sont conservés des documents précédemment considérés comme sensibles, les États parties, le Directeur général et les personnes qui ont établi ces documents au sein de l'Organisation devront peut-être, entre autres, revoir périodiquement le caractère confidentiel desdites informations et le maintien de l'application de catégorie de classification, en vue soit de rayer ces informations de la liste des documents confidentiels, soit de les classer dans une catégorie de sensibilité moindre, soit encore de les diffuser.
- 3.3 La classification de l'information et sa durée peuvent être revues, en particulier dans le contexte d'un programme de destruction des archives de l'Organisation. Le Directeur général peut de temps en temps, pour mener à bien un tel programme, solliciter l'autorisation écrite des États parties dont ils émanent pour que les documents ne soient plus classés confidentiels conformément à des procédures convenues. Dans le cas des informations confidentielles émanant du Secrétariat, le Directeur général pourra périodiquement revoir leur catégorie de classification pour l'archivage. Si les informations en question visent un État partie, ce dernier doit donner son assentiment écrit avant qu'il puisse être mis fin à la classification. Une procédure interne de révision sera établie à cette fin.

4. Changement de catégorie de classification

Reclassification d'informations confidentielles

- 4.1 L'autorité habilitée à changer la catégorie dans laquelle a été classée une information confidentielle est la même que celle spécifiée aux alinéas *a* et *b* du paragraphe 2.2 du présent chapitre aux fins de la détermination de la catégorie dans laquelle cette information doit initialement être classée. En particulier, une information communiquée par un État partie ne peut pas être reclassée sans le consentement écrit de ce dernier. Cette règle s'applique également aux informations contenues dans des documents ayant émané de l'Organisation.
- 4.2 Les États parties dont émane une information classée de l'OIAC ou ayant reçu une information classée de l'Organisation, ainsi que les hauts fonctionnaires du Secrétariat (chefs de service et au-dessus) qui utilisent une telle information peuvent demander que la catégorie dans laquelle elle est classée soit changée. Cette demande doit être justifiée par une nécessité opérationnelle claire et il doit y être donné suite conformément aux dispositions ci-après.
- 4.3 Lorsque l'État partie dont a émané une information classée de l'OIAC demande un changement de classification, il est donné suite à cette demande. Avant de confirmer le changement, le Directeur général peut consulter l'État partie intéressé à propos des conséquences du changement proposé.

- 4.4 Lorsqu'il est demandé, conformément au paragraphe 4.2 ci-dessus, un changement de la catégorie dans laquelle est classée une information confidentielle émanant du Secrétariat, le Directeur général ou son représentant doit, pour décider de la suite à donner à cette demande, s'en tenir aux critères établis pour l'application des catégories de classification en se référant à la nécessité opérationnelle indiquée.
- 4.5 La reclassification d'informations émanant du Secrétariat peut être demandée lorsque l'information est modifiée, complétée ou révisée à un point tel que son niveau de sensibilité change nettement. Par exemple, un projet de rapport sur le respect de la Convention peut être plus sensible que sa version finale, ou bien des données sensibles peuvent être omises dans la version révisée d'un rapport d'inspection destiné à recevoir une plus large diffusion. Les principes énoncés ci-dessus sont, à moins que la Convention n'en dispose autrement, appliqués à l'opération de reclassification.

Déclassification d'informations confidentielles

- 4.6 Les dispositions spécifiées ci-dessus pour la reclassification d'informations confidentielles s'appliquent également à leur déclassification. En particulier, une information communiquée par un État partie ne peut pas être déclassifiée sans le consentement écrit de ce dernier. En outre, il conviendra de suivre les principes directeurs ci-après pour décider de la déclassification d'informations confidentielles :
- a) s'il est proposé une déclassification pour une information confidentielle émanant du Secrétariat et mentionnant un État partie d'une manière ayant influé sur sa classification initiale, le Directeur général doit obtenir le consentement écrit exprès de l'État partie intéressé à la déclassification proposée;
 - b) dans le cas d'une information confidentielle émanant du Secrétariat, le Directeur général ou son représentant doit tenir compte au moins des mêmes aspects que ceux qu'il a pris en considération lorsqu'il a classé ladite information confidentielle.
- 4.7 La déclassification d'une information confidentielle ne signifie pas que celle-ci peut *ipso facto* être divulguée au public. La divulgation en dehors de l'Organisation d'une information quelconque, y compris d'une information précédemment confidentielle qui n'est plus classée comme telle, exige un processus distinct de consultation et d'approbation conformément au chapitre VII de la présente politique. Cette règle s'applique également aux informations que l'Organisation a communiquées aux États parties dans une des catégories de classification de l'OIAC.

CHAPITRE VI

PRINCIPES GÉNÉRAUX APPLICABLES AU TRAITEMENT ET À LA PROTECTION D'INFORMATIONS CONFIDENTIELLES

1. Introduction

- 1.1 Le présent chapitre énonce les principes généraux qui régissent d'une part l'accès que l'Organisation donne à l'information ainsi que la diffusion habituelle de l'information considérée comme confidentielle et d'autre part les procédures connexes de traitement et de protection de l'information confidentielle. Ces principes s'appliquent à la transmission d'informations confidentielles au sein de l'Organisation, y compris ses éléments constituants, ainsi qu'à la communication de telles informations à des représentants autorisés d'États parties. Les principes directeurs applicables à la diffusion publique ou à d'autres formes de diffusion de l'information en dehors de l'Organisation et des États parties sont exposés au chapitre VII.
- 1.2 Ces principes doivent être appliqués lors de la formulation détaillée de toutes les procédures concernant le traitement de l'information confidentielle, y compris le Manuel d'inspection de l'OIAC, le Manuel de déclaration et le Manuel des procédures de confidentialité. D'autres procédures concrètes devront être élaborées sur la base de ces principes dans le cadre des directives administratives publiées par le Directeur général. Les principes énoncés au présent chapitre s'appliquent à toutes les opérations de l'Organisation, au Secrétariat et dans les autres organes de l'Organisation, ainsi que dans les rapports entre eux et les États parties. Les États parties qui reçoivent de l'Organisation des informations confidentielles sont tenus de les protéger conformément aux obligations qu'ils ont assumées aux termes du paragraphe 6 de l'Article VII de la Convention ainsi que du paragraphe 4 de l'Annexe sur la confidentialité. Il conviendra par conséquent que les États parties établissent ou adaptent des procédures appropriées concernant le traitement et la protection de l'information confidentielle communiquée par l'OIAC, selon des modalités conformes aux présents principes.
- 1.3 L'Annexe sur la confidentialité consacre deux principes qui concernent l'accès à l'information confidentielle et sa diffusion au sein de l'Organisation :
- l'accès à l'information confidentielle doit être réglementé conformément à sa classification;
 - la diffusion de l'information confidentielle au sein de l'Organisation doit obéir strictement au principe du "besoin de connaître" (alinéa *h* du paragraphe 2 de l'Annexe sur la confidentialité).

- 1.4 Il découle de ces principes fondamentaux, premièrement, que le niveau de sensibilité de l'information confidentielle déterminera les procédures suivant lesquelles elle est communiquée à ses destinataires ainsi que les moyens employés pour la protéger, et, deuxièmement, que les destinataires autorisés de l'information confidentielle seront déterminés selon le besoin qu'ils ont de connaître cette information eu égard aux buts de la Convention. Un aspect important de la réglementation de la diffusion de l'information confidentielle est l'étendue de l'accès à l'information qui sera accordé aux États parties : dans ce contexte, la présomption fondamentale et inconditionnelle du besoin de connaître est établie par la règle selon laquelle les États parties doivent recevoir régulièrement communication des données dont ils ont besoin pour s'assurer du respect permanent de la Convention par les autres États parties (alinéa *b* du paragraphe 2 de l'Annexe sur la confidentialité). L'accès aux informations confidentielles pertinentes, telles qu'elles sont définies par la présente disposition, doit par conséquent être assuré aux États parties afin de réaliser l'objectif fondamental de transparence et d'une confiance mutuelle renforcée entre les États parties.
- 1.5 L'étendue de l'accès qui sera effectivement accordé à telle ou telle information confidentielle devra être déterminée spécifiquement, plutôt que présumée implicitement, et des mesures concrètes spécifiques devront être adoptées pour empêcher tout autre accès illégitime et non autorisé à cette information. La rigueur avec laquelle l'étendue de l'accès autorisé sera déterminée, de même que le niveau et l'intensité des mesures de protection qui seront prises pour empêcher tout accès non autorisé, devront être réglementés conformément à la classification de l'information. Toutefois, le niveau de classification ne détermine pas, en soi, l'étendue de l'accès qui doit être accordé à l'information confidentielle, mais simplement la façon dont celle-ci doit être traitée et protégée contre toute divulgation non autorisée.

2. Accès, diffusion et protection

- 2.1 L'étendue de l'accès à l'information confidentielle s'entend de l'ensemble des destinataires possibles autorisés à prendre connaissance de cette information ou à la conserver; la diffusion est le processus qui consiste à transmettre activement cette information à ses destinataires autorisés. En conséquence, la notion d'"accès" à l'information désigne la mesure dans laquelle une personne est autorisée à prendre connaissance de cette information ou à la conserver. La diffusion de l'information confidentielle est rendue possible par l'application de mesures de protection, en fonction du niveau de sensibilité de l'information, de sorte que celle-ci est diffusée dans la mesure requise aux fins de la bonne application de la Convention, sans divulgation inutile ou non autorisée. En conséquence, la diffusion de l'information confidentielle à tous les destinataires autorisés au sein de l'Organisation doit, quel que soit son niveau de classification, être soumise aux mesures de protection appropriées. À cet égard, il convient de noter qu'aux termes du paragraphe 6 de l'Article VII de la Convention, les États parties ont l'obligation d'appliquer un traitement spécial à l'information confidentielle reçue conformément à la Convention.

- 2.2 Des procédures et mesures détaillées de protection devront donc être élaborées pour donner l'accès à l'information confidentielle à un fonctionnaire du Secrétariat ou à un État partie en vertu du besoin fonctionnel de connaître ou d'une disposition spécifique de la Convention, tout en empêchant tout autre accès à ladite information, avec la rigueur et le sérieux qui s'attache à la sensibilité de l'information indiquée par sa classification. La communication d'informations confidentielles à la Conférence et au Conseil exécutif devra obéir aux principes généraux applicables à la diffusion de cette information.

Le principe du "besoin de connaître"

- 2.3 C'est le principe du "besoin de connaître" qui permet de déterminer l'étendue de l'accès à l'information ainsi que les destinataires auxquels elle sera diffusée. Il n'existe, à l'Organisation, aucun droit absolu de recevoir des informations confidentielles : aucun fonctionnaire du Secrétariat, ni aucun membre d'un organe de l'Organisation, n'a droit, en vertu de sa qualité ou de son rang seulement, d'avoir accès à toutes les informations confidentielles de l'OIAC.
- 2.4 L'accès à l'information confidentielle est normalement accordé à la fois au cas par cas et en vertu du besoin fonctionnel de connaître. Aux termes de l'alinéa *b* du paragraphe 2 de l'Annexe sur la confidentialité, toutefois, les États parties ont un droit inconditionnel d'accès à certaines informations, et ce paragraphe et les dispositions connexes doivent être considérés comme établissant un besoin incontestable de connaître pour chaque État partie, de sorte que chacun puisse être assuré que les autres États parties continuent de respecter la Convention.
- 2.5 Au sein du Secrétariat, les attributions ou les tâches spécifiques de chaque fonctionnaire sont, dans la mesure où cela est possible dans la pratique, le principal élément déterminant du besoin de connaître de l'intéressé et, par conséquent, de l'étendue de l'accès qu'il est autorisé à avoir à l'information confidentielle.
- 2.6 C'est le Directeur général qui est responsable au premier chef de la protection de l'information confidentielle (paragraphe 2 de l'Annexe sur la confidentialité). De ce fait, sous réserve des dispositions de la Convention, c'est le Directeur général qui détermine en dernière analyse le besoin de connaître telle ou telle information confidentielle.

Administration des procédures de diffusion et de traitement

- 2.7 Le Bureau de la confidentialité et de la sûreté est chargé par le Directeur général d'assurer la supervision d'ensemble de l'administration des dispositions relatives à la confidentialité. Le Directeur général pourra décider de déléguer certaines questions relatives à la confidentialité au Chef du Bureau de la confidentialité et de la sûreté. C'est au Directeur général que revient l'ultime responsabilité en matière de confidentialité.

- 2.8 Une fois déterminée l'étendue de l'accès autorisé à l'information confidentielle, conformément au principe du besoin de connaître, cet accès est accordé conformément à des procédures de traitement détaillées établies pour l'Organisation, en veillant à ce que les modalités d'accès à l'information et le niveau de protection accordé à celle-ci correspondent à sa classification. Un fonctionnaire du Secrétariat ne peut avoir accès à un support contenant une information confidentielle qu'en vertu du principe du besoin de connaître et chaque fois qu'il a accès à cette information, le fait est consigné dans un document qui est conservé. S'il accède à l'information confidentielle par le biais d'un système de traitement électronique des données, il est établi une procédure d'entrée et de sortie que doivent suivre tous les fonctionnaires autorisés pour éviter que quiconque puisse accéder à l'information en utilisant le nom d'un autre fonctionnaire. Le Bureau de la confidentialité et de la sûreté supervise l'application au quotidien de ces procédures de traitement de l'information.

Détermination de l'étendue de l'accès à l'information confidentielle et diffusion de cette information auprès des États parties

- 2.9 Dans différentes circonstances, le Secrétariat doit déterminer l'étendue de l'accès autorisé et par conséquent la portée de l'information confidentielle à communiquer aux États parties. Dans tous les cas, le principe déterminant est celui posé à l'alinéa *b* du paragraphe 2 de l'Annexe sur la confidentialité, et des procédures devront être élaborées pour veiller à ce que les règles prévues dans cette disposition soient respectées. De ce fait, les données dont les États parties ont besoin pour être assurés que les autres États parties continuent de respecter la Convention doivent leur être communiquées systématiquement. En particulier, il faudra suivre les procédures établies en matière de gestion et d'autorisation de l'information pour garantir que les informations qui doivent être communiquées à tous les États parties conformément à l'alinéa *b* du paragraphe 2 de l'Annexe sur la confidentialité leur soient dûment transmises sans qu'il soit nécessaire de mener d'autres consultations ou d'obtenir une approbation spécifique au sein du Secrétariat.
- 2.10 Dans le cas de certaines informations confidentielles qui doivent être communiquées à un État partie dans un but spécifique, non pas aux fins de l'application d'une disposition spécifique de la Convention mais plutôt parce que l'État partie intéressé a un besoin de connaître (par exemple dans le cas des éclaircissements prévus aux paragraphes 3 à 7 de l'Article IX ou pour le règlement d'un litige conformément à l'Article XIV), la règle générale veut que le Directeur général ou un seul haut fonctionnaire qu'il aura spécifiquement désigné à cette fin soit consulté et autorise expressément l'accès proposé, après s'être assuré que le destinataire de l'information a besoin de connaître, et après avoir obtenu l'accord, le cas échéant, de l'État partie visé par l'information en question ou l'ayant initialement fournie. Le Directeur général doit être tenu informé à tout moment des autorisations ainsi accordées.

- 2.11 Les modalités selon lesquelles l'information confidentielle est communiquée par l'Organisation à un État partie doivent se fonder sur la nécessité d'assurer une protection continue de l'information, à un niveau correspondant à sa sensibilité. L'État partie destinataire de l'information doit, à son tour, appliquer le traitement spécial approprié à son niveau de sensibilité et il doit, sur demande, indiquer en détail à l'Organisation les procédures qu'il applique à l'information que lui communique l'Organisation.

Accès à l'information d'autres destinataires autorisés associés à l'Organisation

- 2.12 Il peut s'avérer nécessaire de diffuser des informations confidentielles de l'OIAC à certaines entités ou personnes autorisées extérieures au Secrétariat, mais essentielles à l'accomplissement par l'Organisation de certaines tâches spécifiques qui lui sont confiées par la Convention. Le Directeur général devra mettre en place un régime rigoureux d'accès à ces informations et, conformément au paragraphe 2 de l'Annexe sur la confidentialité, demeurera principalement responsable de l'accès autorisé à ces informations conformément à ce régime. Tout accès proposé à l'information devra être spécifiquement autorisé par le Directeur général ou par l'unique haut fonctionnaire qu'il aura expressément autorisé à cette fin sous sa responsabilité directe conformément au régime établi, et seulement après qu'il aura été clairement établi que le destinataire de l'information a un besoin fonctionnel de connaître. Le Directeur général sera à tout moment tenu informé des autorisations ainsi accordées.

- Lorsque des entités ou personnes autorisées ont accès à des informations confidentielles concernant le territoire d'un État partie ou tout autre lieu placé sous sa juridiction ou son contrôle, le Secrétariat en informe l'État partie intéressé. L'accès à cette information n'est accordé qu'après que les intéressés ont pris un engagement spécifique de secret qui lie tous les destinataires autorisés de l'information. L'on peut, à titre de mesure préliminaire, évaluer le niveau de protection que le destinataire proposé applique à l'information confidentielle.
- Le principe ci-dessus s'applique à l'expédition d'échantillons aux laboratoires désignés conformément au régime établi en vertu du paragraphe 56 de la deuxième partie de l'Annexe sur la vérification. Il peut s'agir aussi de l'accès à des informations confidentielles de l'OIAC que doit avoir un expert autorisé (comme ceux qui peuvent être nommés conformément à l'alinéa e du paragraphe 4 de l'Article IX ou au paragraphe 8 de la onzième partie de l'Annexe sur la vérification) afin de s'acquitter de fonctions officielles.
- L'accès à l'information confidentielle éventuellement accordé à des entités et personnes autorisées extérieures au Secrétariat est rigoureusement limité au minimum nécessaire pour leur permettre de s'acquitter de fonctions inhérentes à l'application de la Convention.

- 2.13 Toute personne à laquelle est accordé l'accès à des informations confidentielles de l'OIAC conformément à la présente disposition a la responsabilité de s'assurer que toute personne extérieure au Secrétariat à laquelle elle pourrait ultérieurement divulguer ces informations a un besoin de connaître, de par ses fonctions, et qu'elle a reçu du Directeur général ou de la personne désignée par celui-ci (comme prévu au paragraphe 2.12 ci-dessus) une autorisation écrite lui accordant l'accès nécessaire à l'information.

Détermination de l'étendue de l'accès à l'information confidentielle au sein du Secrétariat

- 2.14 L'accès aux informations confidentielles de l'OIAC, au sein du Secrétariat, n'est accordé qu'aux personnes qui doivent en avoir connaissance pour pouvoir s'acquitter des attributions professionnelles qui leur sont confiées. Pour déterminer le besoin de connaître au Secrétariat, il conviendra d'analyser de près la définition officielle du poste occupé par le fonctionnaire et l'étendue spécifiée de l'accès qu'il doit avoir à l'information confidentielle. Une référence expresse aux attributions professionnelles spécifiques de l'intéressé est indispensable avant de pouvoir autoriser l'accès à des informations classées **OIAC PROTÉGÉ** et **OIAC HAUTEMENT PROTÉGÉ**. L'étendue de l'accès autorisé aux informations confidentielles classées **OIAC HAUTEMENT PROTÉGÉ** sera indiquée par écrit, au cas par cas.
- 2.15 Il est tenu un registre des fonctionnaires qui, en raison de leurs attributions professionnelles, doivent avoir régulièrement accès à des informations confidentielles touchant chaque État partie. Lorsque le Secrétariat envisage d'accorder à un fonctionnaire l'accès à des informations confidentielles en rapport avec le territoire d'un État partie ou tout autre lieu placé sous sa juridiction et son contrôle, le Secrétariat en informe l'État partie intéressé. Ce dernier en est informé au moins 30 jours avant que l'accès à l'information soit accordé à l'intéressé. Les États parties intéressés doivent être informés, avec préavis d'au moins 30 jours, de la nomination de tout nouveau fonctionnaire ou des changements apportés à la structure des effectifs ou aux attributions des fonctionnaires qui pourraient se traduire par la divulgation d'informations confidentielles les concernant.
- 2.16 Seuls certains hauts fonctionnaires sont autorisés à accorder l'accès à l'information confidentielle aux fonctionnaires placés sous leur direction. Le Directeur général définira dans une directive administrative les critères à appliquer, strictement en fonction du besoin de connaître. Dans chaque cas particulier, l'accès à l'information confidentielle n'est accordé que lorsqu'il a été déterminé que ladite information concerne un sujet ayant un rapport direct avec les attributions spécifiées du destinataire de l'information et l'accès accordé reste toujours sujet à révision par le Directeur général. En cas d'incertitude quant au besoin fonctionnel ou spécifique de connaître l'information qu'a le destinataire proposé, il convient de consulter le supérieur hiérarchique de l'intéressé.

3. Principes applicables au traitement et à la diffusion de l'information

Diffusion de l'information confidentielle

- 3.1 Une distinction doit être établie entre la diffusion de l'information confidentielle et le processus de divulgation de l'information par l'Organisation. D'une façon générale, la diffusion de l'information confidentielle s'entend de la divulgation autorisée de cette information au sein de l'Organisation, y compris tous ses organes, ainsi qu'aux gouvernements des États parties, y compris les organisations gouvernementales et les entités ou personnes autorisées relevant des États parties et s'occupant de l'application de la Convention, lorsque cette divulgation est essentielle à l'accomplissement de fonctions professionnelles spécifiques ou est conforme aux dispositions de la Convention relatives à la communication d'informations aux États parties. Le processus de "divulgation" de l'information par l'Organisation⁵ et son champ d'application spécifique sont définis au chapitre VII de la présente politique.

Acquisition, collecte et génération d'informations confidentielles

- 3.2 Des procédures spécifiques de traitement et de protection doivent être appliquées continuellement dès l'acquisition, la collecte ou la génération d'informations confidentielles par l'Organisation ainsi qu'à toutes les activités ultérieures pendant la diffusion de celle-ci. L'Organisation acquiert, collecte et génère des informations⁶ de plusieurs façons :
- a) des informations sont fournies à l'Organisation par des États parties :
 - conformément aux obligations qui incombent aux États parties en matière de déclarations et de rapports;
 - dans le cadre d'une procédure formelle prévue par la Convention, comme celles visées à l'Article IX;
 - lorsqu'ils transmettent d'autres informations en rapport avec l'application de la Convention;
 - b) d'autres informations en rapport avec l'application de la Convention dans un État partie peuvent être communiquées au Secrétariat par cet État partie;
 - c) des informations peuvent être communiquées au Secrétariat ou à tout autre organe de l'Organisation par un représentant d'un État partie dans le cadre d'une procédure expressément prévue par la Convention, comme celles visées à l'Article IX;

⁵ Par "divulgation" de l'information, l'on entend la divulgation autorisée d'informations en dehors de l'Organisation elle-même (y compris tous ses éléments constitutants) et des gouvernements des États parties (c'est-à-dire, plus précisément, en dehors des organisations gouvernementales et des entités ou personnes autorisées, dans chaque État partie, dans le contexte de l'application de la Convention (paragraphe 1.1 du chapitre VII de la présente politique)).

⁶ Comme défini au chapitre III de la présente politique.

- d) des informations sont acquises ou collectées par une équipe d'inspection dans le cadre de ses activités d'inspection sur place;
 - e) les fonctionnaires du Secrétariat génèrent des informations par la synthèse ou autre traitement d'autres renseignements, par exemple lors de l'analyse d'échantillons ou lors de la compilation de rapports d'inspection. Les informations générées par l'Organisation peuvent utiliser ou répéter des informations initialement fournies par les États parties, ou n'être constituées que de renseignements internes au Secrétariat. La synthèse d'informations ou encore des analyses peuvent aboutir à des informations confidentielles plus sensibles que les sources initiales.
- 3.3 Lorsque l'Organisation reçoit des informations de l'une quelconque de ces sources, elle a des obligations spécifiques quant au traitement et à la protection appropriés de ces informations. En particulier, le destinataire initial ou la source de l'information est tenu de veiller à ce que le caractère confidentiel soit clairement déterminé et la classification correcte appliquée, en consultation, si besoin est, avec le Bureau de la confidentialité et de la sûreté. Les informations confidentielles dont des fonctionnaires du Secrétariat font une compilation ou une synthèse et qui sont tirées d'informations confidentielles provenant d'États parties doivent, en règle générale, être classées au minimum dans la catégorie désignée par l'État partie, à moins que le niveau de sensibilité de l'information n'ait été réduit avec l'accord de l'État partie qui en est la source, ou qu'il décide que son niveau de sensibilité est plus élevé. Toute dérogation à cette règle doit être autorisée par le Directeur général ou par le fonctionnaire qu'il aura habilité à ce faire. Le Directeur général a habilité le Chef du Bureau de la confidentialité et de la sûreté à le faire.
- 3.4 Les informations générées au sein du Secrétariat (comme les rapports d'analyses ou autres rapports, documents directifs, profils, lettres, memoranda) et considérées comme confidentielles doivent être initialement et visiblement classifiées par leur auteur selon leur sensibilité, à un niveau au moins aussi élevé que la classification de la source la plus sensible ayant servi à la synthèse. Lorsque la synthèse a pour effet d'accroître le niveau de sensibilité, il faut appliquer une classification plus élevée que celle de la source initiale.
- 3.5 Les informations qu'un État partie communique à l'Organisation, y compris celles qui sont classées confidentielles, doivent être fournies par un représentant officiel dudit État. Le Secrétariat établira et appliquera une procédure appropriée pour enregistrer la réception et la source officielle de ces informations.
- 3.6 La classification de l'information qu'un État partie a communiquée au Secrétariat aura, dans la plupart des cas, déjà été spécifiée par l'État partie intéressé étant donné que la classification relève au premier chef de celui-ci. Ce faisant, l'État partie devrait tenir compte du niveau de sensibilité et des critères correspondants établis pour chaque catégorie de classification au chapitre V de la présente politique. Si un État partie communique au

Secrétariat des informations qui semblent confidentielles, mais sans indiquer de niveau de sensibilité, il est appliqué une classification provisoire comme prévu au paragraphe 2.2 du chapitre V.

- 3.7 L'obligation générale de protéger et de traiter comme il convient l'information dès sa divulgation à l'Organisation est particulièrement importante lorsque des renseignements sont rassemblés pendant des inspections sur place, par exemple lors de la collecte d'observations spécifiques au site ou lors du prélèvement d'échantillons. Les principes particuliers qui s'appliquent au traitement et à la protection de l'information confidentielle pendant les inspections sont énoncés au paragraphe 6 du présent chapitre.

Procédures de traitement à suivre en vue de protéger l'information confidentielle

Principes directeurs généraux concernant le traitement et la protection de l'information

- 3.8 Nul ne doit, en aucun cas, commenter ou révéler des questions confidentielles si la sécurité de l'information et son environnement échappent à son contrôle. Le Directeur général établira dans une directive administrative les procédures spécifiques à suivre pour empêcher tout accès non autorisé à l'information ou sa divulgation non autorisée dans le cadre de conversations ou par des moyens de télécommunication, en indiquant le niveau des mesures physiques ou autres mesures de protection correspondant au niveau de sensibilité de l'information, indiqué par sa classification. Le recours, après approbation, aux systèmes de télécommunication pour la transmission d'informations confidentielles sera limité aux cas où cela est manifestement nécessaire pour des raisons opérationnelles.
- 3.9 Sous réserve de l'obligation d'empêcher tout accès non autorisé à l'information, les fonctionnaires du Secrétariat peuvent divulguer des informations confidentielles ou en discuter avec :
- a) les fonctionnaires autorisés du Secrétariat dont il est établi qu'ils ont besoin de connaître;
 - b) les personnes, autres que les fonctionnaires, autorisées à avoir accès à l'information comme prévu aux paragraphes 2.12 et 2.13 du présent chapitre, comme les experts autorisés de l'extérieur, les consultants ou les membres autorisés du personnel des laboratoires désignés qui sont individuellement liés par des engagements de secret; en pareil cas, l'information divulguée, qui sera réduite au minimum, sera fournie selon le principe du besoin de connaître, mais devra être suffisante pour faciliter la tâche pour laquelle l'accès à l'information a été autorisé;
 - c) les représentants autorisés d'un État partie auquel se rapporte l'information et ayant clairement droit à la divulgation de celle-ci, comme expressément prévu par les dispositions de la Convention, ou

bien les représentants dont il a été établi qu'ils y sont autorisés et qu'ils ont besoin de connaître.

3.10 Le Directeur général établit les directives administratives indiquant en détail les procédures concrètes de traitement des supports ci-après afin de garantir la protection de l'information confidentielle qu'ils contiennent pendant toutes les opérations de traitement et de stockage, et le Bureau de la confidentialité et de la sûreté supervise l'application de ces directives :

- documents et dossiers sur papier;
- documents informatiques;
- documents audiovisuels;
- échantillons.

Ces directives administratives doivent tendre à mettre en place des mécanismes pratiques de nature à garantir que tous les principes consacrés dans la présente politique sont respectés.

3.11 Dans le cas des informations confidentielles qui ont trait spécifiquement à des installations inspectées ou déclarées, il est appliqué un système de codage et de stockage qui empêche d'identifier directement l'installation visée dans toute la mesure où cela est compatible avec une vérification efficace.

4. Procédures spécifiques de traitement de l'information confidentielle

Marquage de l'information confidentielle

4.1 Pour assurer le traitement approprié des informations confidentielles de l'OIAC, tous les documents et supports de stockage de l'information sont clairement marqués conformément aux instructions fixées à cet effet dans une directive administrative publiée par le Directeur général, dont l'application est supervisée par le Bureau de la confidentialité et de la sûreté :

- **OIAC RESTREINT**
- **OIAC PROTÉGÉ**
- **OIAC HAUTEMENT PROTÉGÉ**

4.2 Chaque document doit être clairement marqué selon le niveau le plus élevé de sensibilité des données qu'il contient. Lorsque cela peut faciliter la divulgation ou la diffusion ultérieure de parties moins sensibles d'un document, l'on peut suivre une méthode de marquage partiel de sorte qu'une classification différente s'applique aux différentes sections (différents paragraphes) d'un même document selon leur niveau de sensibilité, l'ensemble du document étant clairement marqué comme appartenant à la catégorie de sensibilité la plus élevée. Sinon, on peut rassembler l'ensemble de l'information confidentielle dans une annexe confidentielle à un document qui, autrement, est non classifié, l'ensemble du document étant aussi clairement marqué comme appartenant à la catégorie de sensibilité la plus élevée.

- 4.3 L'Annexe sur la confidentialité stipule que toutes les données et tous les documents obtenus par le Secrétariat doivent être évalués afin d'en déterminer le niveau de confidentialité (alinéa b) du paragraphe 2) et être classés confidentiels s'il y a lieu (alinéa d) du paragraphe 2), ce processus devant être conforme au droit qu'a tout État partie de déterminer quelles sont les informations qu'il fournit qui doivent être considérées comme confidentielles. Le service du Secrétariat destinataire de l'information est chargé de cette tâche et, lorsqu'il l'estime nécessaire, il met en place, avec l'aide du Bureau de la confidentialité et de la sûreté, les procédures nécessaires pour veiller à ce que toutes les informations acquises en dehors du Secrétariat et pouvant être confidentielles soient évaluées et que la classification qui s'impose soit clairement indiquée. La détermination de la classification à appliquer, et les pouvoirs en matière de classification, doivent être conformes au système de classification de l'OIAC. Lorsque l'information semble confidentielle mais n'est pas clairement marquée par sa source, le marquage approprié est effectué par le service responsable de la confidentialité, en appliquant, si besoin est, une classification provisoire. Toute classification provisoire ainsi appliquée doit être confirmée, modifiée ou éliminée sans tarder après consultation de la source de l'information.
- 4.4 Toutes les informations confidentielles générées au sein du Secrétariat doivent être clairement marquées par leur auteur, qui leur attribuera une classification provisoire correspondant à leur sensibilité. Le niveau de cette classification doit être fixé conformément au système de classification de l'OIAC. Les chefs de service exercent le contrôle nécessaire pour veiller à ce que les documents confidentiels de sources internes soient marqués comme il convient, sous la coordination et l'autorité d'ensemble du Bureau de la confidentialité et de la sûreté.
- 4.5 Les informations générées par les inspecteurs à partir des renseignements fournis par un État partie inspecté, comme les rapports ou des parties de rapports d'inspection, sont classées dans la catégorie voulue eu égard au niveau de sensibilité indiqué par l'État partie. En cas de doute, l'information doit être considérée comme **OIAC HAUTEMENT PROTÉGÉ** jusqu'à ce que le niveau de sensibilité ait été déterminé à la suite de consultations avec l'État partie inspecté.

Archivage et enregistrement

- 4.6 Le Secrétariat établira, conformément à une directive administrative publiée par le Directeur général, dont l'application sera supervisée par le Bureau de la confidentialité et de la sûreté, des procédures d'archivage et d'enregistrement pour veiller à ce que la distribution interne et l'archivage des informations confidentielles soient enregistrés. Ces procédures permettront de consigner toute communication de ces informations confidentielles à une personne ou institution ou à un organe extérieur au Secrétariat, y compris à des représentants des États parties.

- 4.7 Toutes les informations confidentielles doivent être stockées et distribuées en interne selon des modalités permettant d'enregistrer chaque fonctionnaire qui y a eu accès, ainsi que la date et l'heure de cet accès. Le Secrétariat mettra aussi en place des procédures d'enregistrement de nature à assurer un suivi continu des informations **OIAC HAUTEMENT PROTÉGÉ** et à déterminer qui a eu ou a actuellement de telles informations en sa possession.

Copie de l'information confidentielle

- 4.8 Par "copie", l'on entend tout processus de reproduction qui peut permettre à d'autres personnes d'avoir accès à l'information. Lorsque des informations confidentielles sont copiées, le nombre de copies doit être maintenu au minimum et doit être fonction de l'étendue de l'accès autorisé et de la diffusion qui doit être donnée à l'information. Le fonctionnaire chargé de copier l'information doit veiller à ce que toutes les copies portent clairement les marques appropriées.
- 4.9 Les informations classées ne peuvent être copiées qu'en respectant des procédures strictes et vérifiables. Des informations classées **OIAC HAUTEMENT PROTÉGÉ** ne peuvent être copiées qu'après obtention du consentement enregistré d'un haut fonctionnaire autorisé autre que celui qui copiera les informations ou seulement conformément aux dispositions d'une autorisation permanente spécifique. Ce consentement peut spécifier que la copie doit être faite sous la supervision d'un autre fonctionnaire. Le nombre de copies faites doit être enregistré et chaque copie numérotée. Les copies doivent être distribuées aux destinataires approuvés, et cette distribution enregistrée. Toute copie en surnombre ou les copies qui ne sont plus utilisées doivent être retournées au commis à l'archivage, lequel les archive ou les détruit, en enregistrant le sort qui leur est réservé.
- 4.10 Les informations qui doivent être communiquées aux États parties conformément à l'alinéa *b* du paragraphe 2 de l'Annexe sur la confidentialité mais qui sont confidentielles sont copiées et diffusées normalement, conformément aux demandes des États parties et conformément à la directive administrative publiée par le Directeur général. Dans le cas des informations **OIAC PROTÉGÉ** et **OIAC HAUTEMENT PROTÉGÉ**, le nombre de copies faites et les destinataires de chacune des copies sont enregistrés.

Élimination et destruction des informations confidentielles

- 4.11 Le Directeur général établira dans une directive administrative les procédures de traitement que le Secrétariat devra appliquer pour que les documents qui contiennent des données confidentielles soient éliminés et détruits dans des conditions de sécurité. Ces procédures porteront sur :
- les méthodes techniques de destruction ou d'élimination de toutes les catégories de supports;
 - l'enregistrement des documents détruits ou éliminés;
 - les procédures à suivre pour que la destruction et l'élimination se fassent en présence de témoins;

- les règles à suivre en ce qui concerne les rapports contenant des données extrêmement confidentielles communiquées par les États parties.

Transmission d'informations confidentielles

4.12 La transmission d'informations confidentielles, en version papier ou électronique, à destination et en provenance du Secrétariat doit se faire en fonction de leur niveau de sensibilité et doit être soumise à des procédures rigoureuses fixées dans une directive administrative publiée par le Directeur général. Ces procédures porteront sur :

- les principes directeurs à suivre pour assurer la sécurité des envois postaux ou de la transmission manuelle ainsi que la remise en main sûre des informations confidentielles;
- les modalités de transmission sécurisée des informations par téléphone, par télécopie et par d'autres moyens de télécommunication.

4.13 Les règles applicables devront être telles que, pour tous les types d'informations confidentielles diffusées :

- l'information est reçue au point de destination approprié;
- seuls les usagers autorisés ont accès aux données transmises;
- le destinataire d'un message peut vérifier que son expéditeur est une personne autorisée.

4.14 Le Directeur général décrira dans une directive administrative les normes fixées pour la sécurité du système de communication utilisé dans le cadre du Système de gestion de l'information (SGI), et ces normes seront consignées dans le manuel d'inspection.

Sauvegarde de l'information confidentielle

4.15 Les fonctionnaires et autres personnels autorisés conformément aux paragraphes 2.12 et 2.13 ci-dessus, qui utilisent des informations confidentielles ou qui sont responsables de leur sauvegarde doivent prendre toutes les précautions voulues pour empêcher que des personnes non autorisées y aient délibérément ou accidentellement accès. Ils doivent à cette fin, au minimum, suivre toutes les procédures et appliquer les normes établies au sein de l'Organisation pour le traitement et la protection de l'information confidentielle, et veiller à ce que l'information soit continuellement protégée pendant sa diffusion.

4.16 Les informations confidentielles ne doivent pas être utilisées ou placées de manière à être exposées ou rendues accessibles à des personnes qui ne sont pas autorisées à y avoir accès. Le Directeur général a chargé le Bureau de la confidentialité et de la sûreté d'établir des procédures garantissant que les fonctionnaires du Secrétariat réservent à l'information confidentielle le traitement approprié. Le Directeur général devra veiller à ce que lesdites procédures soient intégralement appliquées, à ce que toute violation soit décelée et signalée et à ce que les sanctions disciplinaires appropriées soient imposées conformément au chapitre IX de la présente politique.

Protection physique et stockage

- 4.17 Le Directeur général définira dans une directive administrative les mesures de sécurité physique applicables aux bureaux, laboratoires, zones de stockage de l'information, supports informatiques et documents audiovisuels classés confidentiels, ainsi que les normes applicables aux installations de stockage physique du Secrétariat, y compris en ce qui concerne le verrouillage et la sécurité des zones protégées, des classeurs et des conteneurs scellés. Ces mesures comprendront des procédures applicables pour limiter l'accès aux bâtiments et aux autres locaux de l'OIAC et pour enregistrer la présence des visiteurs et des fonctionnaires pendant et après les heures de travail. Ces procédures définiront également les dispositions spéciales applicables à l'accès de zones particulièrement sensibles du bâtiment et des autres locaux de l'OIAC, comme les zones de stockage des informations confidentielles, les bureaux où sont traités et validés les déclarations et les rapports d'inspection, le centre d'opérations et le laboratoire de l'OIAC.
- 4.18 Les informations confidentielles sont stockées en lieu sûr dans les locaux de l'Organisation. Certains documents ou données peuvent également être stockés par les autorités nationales des États parties. Les informations sensibles, y compris les photographies, plans et autres documents qui sont requis uniquement pour l'inspection d'une installation particulière peuvent être conservés sous clef dans cette installation (alinéa e du paragraphe 2 de l'Annexe sur la confidentialité).
- 4.19 Dans toute la mesure possible, le stockage des informations confidentielles de l'OIAC par les autorités nationales d'États parties ou dans une installation inspectée doit être conforme aux normes minima appliquées par le Secrétariat.

Sortie des informations confidentielles des locaux de l'OIAC

- 4.20 Le Directeur général définira dans une directive administrative les procédures à suivre lorsque des informations confidentielles doivent être sorties des locaux de l'Organisation ou transportées entre les sites inspectés et l'Organisation et entre l'Organisation et les représentants des États parties. Les informations confidentielles ne pourront sortir des locaux de l'OIAC qu'à des fins en rapport avec l'application de la Convention, et uniquement dans la mesure absolument nécessaire pour l'accomplissement de fonctions professionnelles autorisées.

Procédures à suivre en cas de perte d'informations confidentielles

- 4.21 Le Directeur général définira dans une directive administrative les procédures à suivre en cas de perte avérée ou soupçonnée d'informations confidentielles de l'OIAC, qu'elles aient été perdues par un inspecteur, par un fonctionnaire du Secrétariat ou par un représentant d'un État partie, ou bien pendant le transport. Ces procédures spécifieront notamment les règles à suivre en matière de rapports, d'enquêtes et de consultations avec les États parties intéressés. Comme toute perte ou toute perte soupçonnée crée un risque de manquement à la confidentialité, il conviendra d'appliquer les procédures à suivre en cas de manquement avéré ou allégué à la confidentialité.

5. Procédures applicables à certains supports spécifiques

- 5.1 Les procédures de traitement de l'information confidentielle énoncées au paragraphe 4 ci-dessus s'appliquent à toutes les informations confidentielles, quel que soit le support utilisé. Les procédures complémentaires ci-dessous ont trait aux informations stockées sur des supports spécifiques.

Documents audiovisuels

- 5.2 Une directive administrative définira les procédures applicables au traitement de documents audiovisuels contenant des informations confidentielles, la spécification des niveaux de protection conformément aux catégories de classification et l'application rigoureuse des procédures spécifiées pour le traitement des documents contenant des informations confidentielles.

Informations confidentielles contenues dans des ordinateurs et des documents informatiques

- 5.3 L'accès à tous les locaux de l'OIAC et aux éléments clés du SGI, comme serveurs et unités de mémoire de masse, devra être réglementé. Tout le matériel du SGI confidentiel, et spécialement les postes de travail, serveurs, imprimantes et terminaux, devront être protégés, non seulement pour les mettre à l'abri du vol ou de déprédations intentionnelles mais aussi de tout accès physique non autorisé et de toute tentative de fraude. En outre, les activités d'entretien et de réparation du matériel utilisé pour le SGI confidentiel devront être supervisées et enregistrées. L'accès aux matériels (serveurs, imprimantes, dispositifs de sauvegarde et autres moyens d'accès aux données) devra être limité aux fonctionnaires ayant les autorisations voulues.
- 5.4 Les procédures applicables à la protection des données stockées dans le SGI confidentiel et tout autre système de traitement électronique ou de stockage de données devront comprendre les éléments suivants :
- mesures de contrôle visant à empêcher toute utilisation par des usagers non autorisés ou tout accès non autorisé de l'extérieur;
 - séparation des dossiers et des données des divers usagers;
 - vérification des activités des usagers, y compris en ce qui concerne l'accès aux bases de données et les changements apportés aux paramètres des systèmes et aux fichiers. En particulier, tout accès d'un fonctionnaire aux fichiers informatiques contenant des informations confidentielles sera enregistré et ces registres seront régulièrement vérifiés.
- 5.5 Les procédures visant à assurer la sécurité des données, des documents et des informations stockées sur ordinateur devront comprendre des règles détaillées afin de protéger la confidentialité de l'information lors de la création, du traitement, du marquage, de la sauvegarde et de la destruction de toutes formes de fichiers d'ordinateur, de documents informatiques et d'autres documents intéressant des tâches comme l'administration des systèmes et la gestion et le fonctionnement du régime de sécurité dans le domaine informatique.

- 5.6 Les matériels informatiques (y compris les supports portables comme disquettes) et les informations confidentielles stockées dans le SGI de l'OIAC devront être soumis aux procédures de traitement et de stockage qui seront définis, avec les spécifications techniques détaillées voulues, dans une directive administrative du Directeur général.

Échantillons provenant des inspections sur place

- 5.7 Le paragraphe 55 de la deuxième partie de l'Annexe sur la vérification stipule que les échantillons prélevés pendant les inspections peuvent être extraits des sites inspectés pour être confiés à des laboratoires désignés à des fins d'analyse. Le processus de prélèvement d'échantillons concerne essentiellement la vérification du respect de la Convention, mais les échantillons prélevés peuvent aussi, indirectement, receler et fournir d'autres informations qui, en elles-mêmes, n'intéressent pas directement la vérification. En conséquence, le manuel d'inspection devra définir les procédures à suivre pour garantir la protection de la confidentialité des échantillons transportés en vue d'une analyse hors site dans des laboratoires désignés.
- 5.8 La formulation et la mise en œuvre du régime établi conformément au paragraphe 56 de la deuxième partie de l'Annexe sur la vérification en vue de la collecte, de la manipulation, du transport et de l'analyse des échantillons devront tenir compte de la nécessité de protéger la confidentialité de l'information pendant le transport des échantillons jusqu'aux laboratoires désignés et leur stockage par ces derniers. Ce régime devra tenir compte du risque que le processus d'analyse dont l'objectif est de vérifier le respect de la Convention génère d'autres informations confidentielles sans rapport avec la vérification. Toute autre précaution nécessaire en matière de confidentialité devra être prise aussi lors de l'application des procédures de comptabilisation prévues au paragraphe 57 de la deuxième partie de l'Annexe sur la vérification ainsi que des procédures connexes à suivre pour informer l'État partie inspecté que les laboratoires désignés auront détruit les échantillons une fois leur analyse achevée ou les auront restitués au Secrétariat pour que celui-ci leur réserve le sort approprié. Les laboratoires désignés devront prendre des engagements spécifiques de secret confirmant les obligations découlant du régime applicable au processus d'échantillonnage et d'analyse.

6. Traitement et protection de l'information confidentielle pendant les activités de vérification sur place

Procédures d'inspection

- 6.1 L'Annexe sur la confidentialité et les chapitres précédents de la présente politique définissent les principes fondamentaux à suivre pour le traitement et la protection de l'information confidentielle pendant les inspections, qu'il s'agisse des informations acquises ou rassemblées pendant la vérification ou des autres informations, sans rapport avec les buts de la Convention, pouvant être divulguées dans le cadre des activités d'inspection. Le manuel d'inspection de l'OIAC doit définir, sur la base de ces principes, les procédures détaillées à suivre, y compris en ce qui concerne l'utilisation et la protection des données,

des documents et des fichiers et leur accès pendant la conduite des inspections, conformément aux règles stipulées dans l'Annexe sur la confidentialité et aux exigences fonctionnelles des inspecteurs sur le terrain. Ces procédures devront tenir compte des exigences fonctionnelles de protection des données stockées dans des appareils portables ainsi que des règles générales régissant le transport et le stockage d'informations confidentielles.

- 6.2 Du point de vue pratique, les principaux éléments de la protection de l'information confidentielle pendant les inspections ont trait aux procédures d'inspection, à l'utilisation du matériel et au processus de consultations à l'intérieur de l'équipe d'inspection ainsi qu'avec les représentants de l'État partie inspecté. Les procédures d'inspection devront stipuler clairement les voies hiérarchiques à suivre pour les communications à l'intérieur de l'équipe d'inspection pour pouvoir permettre à ses membres de se consulter au sujet des questions pouvant surgir dans le contexte de la confidentialité ainsi que de l'utilisation à faire des informations confidentielles. Conformément à cette structure, les représentants de l'État partie inspecté et de l'installation inspectée et l'équipe d'inspection se consultent, pendant la négociation de l'accord d'installation, les exposés d'information préalables à l'inspection et pendant les inspections initiales et les inspections ultérieures, afin d'établir clairement l'étendue de l'accès à l'information qui sera accordé à chaque membre de l'équipe d'inspection ainsi que le traitement à appliquer aux informations confidentielles divulguées ou rassemblées. Dans le cas des inspections par mise en demeure, les observateurs sont tenus de respecter rigoureusement le caractère confidentiel de toute information à laquelle ils ont accès conformément aux dispositions pertinentes de la Convention et doivent traiter cette information en conséquence.

Évaluation et classification de l'information confidentielle

- 6.3 La procédure de classification prévue au paragraphe 2.5 du chapitre V de la présente politique s'applique aux informations rassemblées pendant les inspections. Selon cette procédure, ces informations sont évaluées sans tarder pour déterminer leur caractère confidentiel et recevoir immédiatement une classification initiale et faire l'objet de toutes les mesures de protection voulues en fonction de leur sensibilité, conformément à l'accord d'installation éventuel et en accord avec les représentants de l'État partie inspecté. S'il n'a pas été conclu d'accord pertinent avant l'inspection, l'équipe d'inspection encourage l'État partie inspecté, dans tous les cas où cela est possible, à désigner la catégorie de classification de toute information confidentielle divulguée pendant l'inspection. Si des informations confidentielles sensibles sont divulguées ou révélées à un membre de l'équipe d'inspection sans que leur catégorie de classification soit indiquée, ces informations sont, conformément au système de classification, être soumises aux procédures de traitement et de protection applicables aux informations classées **OIAC HAUTEMENT PROTÉGÉ**, à moins que l'État partie inspecté ne stipule autre chose. En général, en cas de doute ou d'incertitude, l'information confidentielle est soumise au niveau de protection le plus rigoureux qui soit, et les consultations touchant la divulgation et la diffusion de cette information, même à l'intérieur de l'équipe

d'inspection, doivent tenir dûment compte du principe du "besoin de connaître" lorsqu'il s'agit de déterminer l'étendue de l'accès à cette information. Si les informations rassemblées comprennent des informations confidentielles sans rapport avec la Convention, il convient d'appliquer les procédures spécifiques dont il est question au paragraphe pertinent ci-dessous.

Protection des informations confidentielles non pertinentes pendant les activités de vérification sur place

- 6.4 La présente politique stipule clairement les principes à suivre concernant la protection des informations confidentielles sans rapport avec la Convention, ainsi que les responsabilités spécifiques à cet égard⁷. Les activités de vérification doivent par conséquent être conçues, planifiées et exécutées de manière à éviter toute divulgation inutile d'informations confidentielles et à empêcher, sous réserve de la nécessité de faire en sorte que les obligations assumées en matière de vérification soient respectées efficacement et ponctuellement, que des informations confidentielles sans rapport avec l'observation de la Convention soient divulguées dans les documents définissant la portée d'une inspection. Ces principes veulent également qu'aucune information confidentielle sans rapport avec l'observation de la Convention ne soit recherchée, consignée ou conservée; chaque membre de l'équipe d'inspection, et spécialement le chef de l'équipe, a la responsabilité fondamentale de veiller à ce que tel ne soit jamais le cas pendant l'inspection. Il se peut évidemment que, pendant une inspection, des informations confidentielles qui sont en elles-mêmes dépourvues de rapport avec l'objet de l'inspection soient rassemblées ou consignées sous différentes formes (telles que celles-ci sont indiquées dans la définition de l'"information" figurant au chapitre III)⁸, notamment par le biais du matériel d'inspection approuvé, de l'habillement des inspecteurs ou d'articles personnels. De telles informations, si elles sont recueillies au cours des activités d'inspection, ne doivent pas être divulguées sous quelque forme que ce soit, même au sein de l'équipe d'inspection, et doivent être restituées à l'État partie inspecté ou détruites sous la supervision de ce dernier.
- 6.5 L'Annexe sur la confidentialité stipule qu'au cours des activités d'inspection, les États parties "peuvent prendre les mesures qu'ils estiment nécessaires pour protéger la confidentialité de l'information à condition qu'ils s'acquittent de leur obligation de démontrer, conformément aux articles pertinents et à l'Annexe sur la vérification, qu'ils respectent la Convention".⁹ Les équipes d'inspection sont tenues, entre autres, de "prendre en considération les propositions que pourrait leur faire l'État partie inspecté, à quelque stade que ce soit de l'inspection, pour protéger du matériel ou des informations sensibles sans rapport avec les armes chimiques".¹⁰ "Les équipes d'inspection observent strictement les dispositions des articles et des annexes pertinents régissant la

⁷ Énoncées au paragraphe 1.4 du chapitre IV.

⁸ Énoncée au chapitre III, sous la rubrique "Contenu de l'information".

⁹ Annexe sur la confidentialité, paragraphe 13.

¹⁰ Annexe sur la confidentialité, paragraphe 14.

conduite des inspections. Elles respectent pleinement les procédures visant à protéger les installations sensibles et à empêcher la divulgation de données confidentielles".¹¹

- 6.6 Sous réserve de consulter pleinement l'État partie inspecté tant pendant qu'après une inspection (comme prévu pour les inspections par mise en demeure au paragraphe 61 de la dixième partie de l'Annexe sur la vérification), l'Organisation doit confirmer à l'État partie inspecté que les informations rassemblées au cours des activités d'inspection conformément à la Convention, eu égard aux termes du mandat d'inspection, sont en rapport avec l'observation de la Convention. L'équipe d'inspection doit protéger les informations réunies pendant l'inspection conformément au degré de classification prescrit par l'État partie inspecté. Ce dernier ne peut pas, dans le contexte des obligations qui lui incombent s'agissant de démontrer qu'il respecte la Convention, opposer d'objections à l'inclusion dans le rapport préliminaire d'inspection d'informations que l'équipe d'inspection, après l'avoir pleinement consulté, juge être en rapport avec l'observation de la Convention eu égard aux dispositions du mandat d'inspection.
- 6.7 Toute information rassemblée au cours de l'inspection mais ne figurant pas sur la liste établie et communiquée à l'État partie inspecté est présumée être sans rapport avec le mandat d'inspection et doit être traitée comme indiqué au paragraphe 6.4 ci-dessus. Le principe établi est que les membres de l'équipe d'inspection doivent respecter les limites imposées en ce qui concerne l'accès à l'information et la diffusion de celle-ci, par exemple celles convenues dans le cadre d'un régime d'accès réglementé dans le cas d'une inspection par mise en demeure, et qu'aucune information qu'un État partie considère comme confidentielle mais dont il n'a pas reçu copie ne doit sortir du site de l'inspection sans son consentement. Sans préjudice de l'obligation qui incombe à tout État partie de démontrer qu'il respecte la Convention, les procédures élaborées pour mettre en œuvre les principes susmentionnés pourront prévoir notamment :
- que le matériel d'inspection devra faire l'objet d'un nettoyage supplémentaire;
 - que l'habillement devra être changé avant ou après une activité d'inspection déterminée;
 - que tout article personnel devra être laissé à l'extérieur d'une zone déterminée avant d'y pénétrer;
 - que le matériel affecté sera transporté sous scellé commun au Secrétariat pour y être décontaminé sous la supervision d'un représentant de l'État partie inspecté si ce dernier en fait la demande;
 - que les éléments démontables porteurs d'informations confidentielles sans rapport avec la Convention devront être conservés sur place; ou

¹¹ Annexe sur la confidentialité, paragraphe 15.

- après étude de toutes les possibilités, y compris celles visées ci-dessus, que le matériel sera conservé sur place.

Les procédures susmentionnées ne devront pas donner lieu à des abus et devront être appliquées, le cas échéant, conformément à un cadre juridique respectant le régime des immunités établi en vertu de l'alinéa *d* du paragraphe 11 de la deuxième partie de l'Annexe sur la vérification.

- 6.8 Les procédures suivies conformément à ces principes ne devront en aucun cas entraver ou retarder les activités de vérification menées conformément au mandat de l'inspection et aux dispositions de la Convention.

CHAPITRE VII

PROCÉDURES APPLICABLES À LA DIFFUSION DE L'INFORMATION PAR L'OIAC

1. Généralités

- 1.1 Le présent chapitre énonce les principes régissant les procédures que l'Organisation doit suivre pour la diffusion de toute information en sa possession dans le contexte de l'application de la Convention. Par "diffusion" de l'information par l'Organisation, l'on entend la divulgation autorisée d'informations en dehors de l'Organisation elle-même (y compris tous ses éléments constitutants) et en dehors des gouvernements des États parties (plus précisément, en dehors des organisations gouvernementales et des entités ou personnes désignées par les États parties afin de s'occuper de l'application de la Convention). En conséquence, ces principes régissent la diffusion de l'information par l'OIAC à toute autre organisation internationale, au gouvernement d'un État qui n'est pas partie à la Convention, aux organisations privées ou aux organisations gouvernementales sans rapport avec l'application de la Convention ou à toute personne qui n'est pas employée par l'Organisation ou qui ne travaille pas pour celle-ci sous contrat, ou qui n'est pas autorisée par un État partie à s'occuper de l'application de la Convention.
- 1.2 Il y aura, dans le contexte de l'application de la Convention, des cas où l'Organisation devra diffuser des informations afin de s'acquitter de ses obligations. Cette diffusion peut être générale, ou bien de portée limitée, en fonction des circonstances. La nécessité de diffuser des informations peut concerner tant des informations classées confidentielles que des informations non classées. Aucune information obtenue ou générée par l'Organisation dans le contexte de l'application de la Convention ne doit être publiée ni divulguée de toute autre manière si ce n'est conformément aux principes directeurs ci-après.

2. Diffusion publique de l'information

- 2.1 Le Directeur général peut publiquement diffuser toute information qui n'est pas considérée comme confidentielle (y compris les informations qui ne sont plus classées confidentielles conformément aux paragraphes 4.6 et 4.7 du chapitre V) et qui relève de l'une des catégories suivantes :
- a) les informations de caractère général concernant l'application de la Convention qui ne contiennent aucune donnée intéressant spécifiquement un État partie. Cette catégorie exclut les informations spécifiques touchant les activités d'inspection menées ou envisagées sur le territoire d'un État partie. Les types d'informations qui peuvent être publiquement diffusées conformément à la présente disposition seront indiqués dans une liste approuvée par la Conférence; cette liste pourrait

comprendre les détails des règles et des formulaires de déclaration, la documentation générale ou type, des informations sommaires sur le programme de vérification en général et les technologies et méthodes de vérification appliquées dans le cadre des inspections sur place;

- b) les informations organisationnelles de caractère factuel concernant l'Organisation, sauf les informations qui ont trait à la sécurité de l'Organisation ou aux questions relatives au personnel et à la vie privée des fonctionnaires du Secrétariat;
- c) les informations intéressant un État partie qui ne sont pas classées confidentielles et dont l'État partie intéressé a expressément demandé qu'elles soient publiquement diffusées ou y a consenti.

2.2 Le Directeur général examine les différentes demandes de diffusion publique de l'information et décide de la suite à leur donner, à condition que lesdites demandes soient conformes aux dispositions du paragraphe précédent. Les demandes allant au-delà de ces paramètres sont soumises pour décision au Conseil exécutif ou à la Conférence.

2.3 Tous les contacts entre des fonctionnaires du Secrétariat et les médias sont sujets à la présente politique, en particulier au chapitre VII (y compris les présentes procédures concernant la diffusion publique de l'information) et à la politique de l'OIAC à l'égard des médias et en matières de relations publiques. Le Directeur général publiera une directive administrative énonçant la politique à suivre avec les médias, conformément aux présents principes directeurs touchant la diffusion publique de l'information.

3. Diffusion limitée ou non publique de l'information

3.1 Il pourra y avoir des cas où il faudra¹² diffuser des informations en dehors de l'Organisation sans aller jusqu'à les diffuser totalement au public; par exemple à une organisation internationale ou à une organisation gouvernementale à des fins officielles seulement, et sous réserve de certaines conditions. Une telle diffusion non publique peut s'appliquer aux informations classées confidentielles par l'OIAC, ou bien à des informations n'étant pas ou plus classées confidentielles. Les informations classées confidentielles par l'OIAC ne sont divulguées que si le Directeur général confirme que l'Organisation à laquelle elles sont destinées peut les protéger et en assurer la garde comme il convient. Le Directeur général conclut avec les organisations pouvant être appelées à recevoir de telles informations un accord ou des dispositions convenues concernant la manipulation et la protection des informations confidentielles.

¹² Conformément à l'alinéa c du paragraphe 2 de l'Annexe sur la confidentialité.

- 3.2 Il peut y avoir diffusion limitée ou non publique d'informations :
- a) si le Conseil exécutif décide de porter un problème ou une question directement à l'attention de l'Assemblée générale ou du Conseil de sécurité de l'Organisation des Nations Unies conformément au paragraphe 36 de l'Article VIII;
 - b) si la Conférence décide de porter une question à l'attention de l'Assemblée générale ou du Conseil de sécurité de l'Organisation des Nations Unies conformément au paragraphe 4 de l'Article XII;
 - c) si la Conférence ou le Conseil exécutif décide de demander un avis à la Cour internationale de justice, avec l'autorisation de l'Assemblée générale des Nations Unies, conformément au paragraphe 5 de l'Article XIV.
- 3.3 La diffusion limitée ou non publique d'informations non classées confidentielles par l'OIAC peut être autorisée par le Directeur général si l'information dont il s'agit relève des catégories visées au paragraphe 2.1 du présent chapitre. Les demandes de diffusion d'informations non classées confidentielles par l'OIAC mais allant au-delà de ces paramètres doivent être soumises pour décision au Conseil exécutif ou à la Conférence.
- 3.4 Lorsqu'il est proposé de procéder à une diffusion limitée ou non publique d'informations confidentielles, la portée et les conditions de cette diffusion doivent être rigoureusement conformes aux exigences de l'application de la Convention. Le principe du "besoin de connaître" régissant la diffusion de l'information demeure applicable.
- 3.5 Si les informations confidentielles concernent un État partie spécifique et que ce dernier demande expressément qu'elles soient diffusées ou y consent, la diffusion peut être opérée sans autre consultation. Dans tous les autres cas, une décision de la Conférence ou du Conseil exécutif est requise pour que des informations confidentielles puissent être diffusées en dehors de l'Organisation. Une demande tendant à ce qu'une décision en ce sens soit prise peut être soumise à l'un ou l'autre organe, mais elle constitue normalement un élément d'une décision de politique générale de la Conférence ou du Conseil exécutif de soumettre une question liée à un organe extérieur conformément à la Convention, de sorte que la décision concernant la diffusion de l'information sera adoptée par le même organe que celui qui aura à examiner la question de politique générale.
- 3.6 Toute décision tendant à approuver une telle diffusion devrait être basée sur les deux éléments qui suivent :
- a) la conclusion expresse que le destinataire proposé a clairement un besoin de connaître conformément au rôle qu'il joue dans le contexte de l'application de la Convention;

- b) la conclusion que la diffusion envisagée est conforme aux exigences de la Convention.
- 3.7 Lorsqu'il apparaît nécessaire de diffuser des informations confidentielles, le Directeur général établit un projet de proposition à ce sujet qui fait l'objet de consultations et d'un examen par les parties intéressées. Les facteurs à prendre en considération pour déterminer la confidentialité et la classification de l'information doivent être pleinement analysés lors de la formulation de la proposition relative à la diffusion de l'information. Le cas échéant, les informations qu'il est proposé de diffuser sont présentées sous des formes moins sensibles de manière à éviter de divulguer des informations confidentielles sans rapport avec l'objet de la diffusion. En pareil cas, il convient d'appliquer les processus de déclassification ou de reclassification. Si les informations confidentielles ont été obtenues d'un État partie ou le concernent, le Directeur général ou une personne autorisée par lui à cette fin doit obtenir l'assentiment écrit dudit État à la diffusion proposée. Aucun État partie ne refuse un tel consentement de manière à se soustraire aux obligations qui lui incombent en vertu de la Convention.
- 3.8 Lorsqu'il prépare une proposition touchant la diffusion de l'information, le Directeur général peut proposer les conditions ou limites spécifiques auxquelles est assortie cette diffusion afin de veiller à ce que les informations diffusées servent leur but spécifique dans le contexte de l'application de la Convention. Certaines des limites ou des conditions qui peuvent être imposées sont les suivantes :
- a) accès à l'information confidentielle sur une base temporaire seulement, par exemple pour la durée d'une réunion ou pour la durée des services consultatifs à fournir;
 - b) spécification que les informations sont destinées exclusivement à un usage officiel;
 - c) demande de traitement particulier, par exemple demande de destruction ou de restitution de l'information à l'expiration d'un délai spécifié;
 - d) application de contrôles spécifiques à certains éléments sensibles de l'information confidentielle;
 - e) accès visuel à l'information confidentielle, par exemple au moyen d'une projection pendant une réunion.
- 3.9 Après consultation avec les parties intéressées, la proposition de diffusion est soumise pour décision au Conseil exécutif ou à la Conférence.

CHAPITRE VIII

ADMINISTRATION

Le Directeur général

1. Le Directeur général doit mettre en place le régime de protection et de traitement de l'information confidentielle dans le cadre de l'Organisation conformément aux principes énoncés dans l'Annexe sur la confidentialité et la présente politique, et superviser et vérifier l'application de ce régime. À cette fin, le Directeur général publie les directives administratives nécessaires pour donner effet à la présente politique et surveille leur application.
2. Le Directeur général est principalement responsable du respect du régime mis en place et confie aux services appropriés du Secrétariat les tâches spécifiques à exécuter pour appliquer ce régime conformément à la présente politique. Dans des cas exceptionnels, le Directeur général peut déléguer des pouvoirs spécifiques concernant la mise en œuvre du régime de confidentialité à un nombre limité de hauts fonctionnaires du Secrétariat, sous réserve des limites spécifiques fixées dans la présente politique¹³. Le Directeur général doit également superviser personnellement l'activité de ces services, et il demeure personnellement responsable des mesures prises par les hauts fonctionnaires auxquels il a délégué ses pouvoirs.

Administration du régime de confidentialité au sein du Secrétariat

3. Le régime de confidentialité s'applique aux opérations de toutes les unités du Secrétariat. Le Bureau de la confidentialité et de la sûreté aidera les services du Secrétariat destinataires de l'information à évaluer les données et les documents obtenus par le Secrétariat, afin de déterminer s'ils contiennent des informations confidentielles, en appliquant à cet égard les principes directeurs énoncés à l'alinéa a) du paragraphe 2 de l'Annexe sur la confidentialité et au paragraphe 11 du chapitre III de la présente politique. Le Bureau du contrôle interne, dans le cadre de sa fonction d'audit de la confidentialité, procédera à une vérification interne du fonctionnement du régime de confidentialité, cette vérification devant être effectuée par un service fonctionnellement distinct de celui qui aura été chargé de l'application du régime établi.
4. Sous la supervision du Directeur général, le Secrétariat veille à ce que tous les fonctionnaires soient dûment informés, avec des rappels appropriés, de leur obligation de protéger l'information confidentielle et de respecter le régime de confidentialité, ainsi que des principes énoncés dans la présente politique et des procédures requises pour les appliquer, des principes et procédures applicables en matière de sécurité et des sanctions auxquelles ils s'exposeraient en cas de divulgation non autorisée d'informations confidentielles. Les besoins de

¹³ Voir en particulier les paragraphes 2.10 et 2.12 du chapitre VI de la présente politique.

formation sont également pris en compte après chaque restructuration de l'organisation du Secrétariat ayant une incidence sur les fonctionnaires qui traitent l'information confidentielle. Dans ces cas, cette formation supplémentaire est de préférence dispensée dans les trois mois suivant la restructuration, ou à défaut, dès que possible après celle-ci.

CHAPITRE IX

PROCÉDURES EN CAS DE MANQUEMENT À LA CONFIDENTIALITÉ

CHAPITRE IX.1 : PROCÉDURES D'ENQUÊTE EN CAS DE MANQUEMENT À LA CONFIDENTIALITÉ

1. Enquêtes sur les manquements avérés ou allégués à la confidentialité et la violation des obligations en la matière

Le présent chapitre, qui est fondé sur le paragraphe 19 de l'Annexe sur la confidentialité, expose la procédure à suivre par le Directeur général lorsqu'il enquêtera sur un manquement avéré ou allégué à la confidentialité ou sur une violation des obligations connexes de protection de l'information confidentielle.

- Étape 1 : Enquête du Directeur général
- Étape 2 : Mesures provisoires
- Étape 3 : Rapport d'enquête
- Étape 4 : Suite à donner au rapport d'enquête
 - 4a : Sanctions disciplinaires contre les fonctionnaires en exercice du Secrétariat
 - 4b : Sanctions contre d'anciens fonctionnaires du Secrétariat
 - 4c : Mesures à prendre en cas de levée de l'immunité
 - 4d : Autres actions en justice dans le cadre d'une juridiction nationale
 - 4e : Mesures à prendre lorsqu'un État partie semble responsable
 - 4f : Mesures visant à réformer ou à renforcer le régime de confidentialité

2. Définitions

Par manquement à l'obligation de protéger la confidentialité (ci-après dénommé "manquement à la confidentialité"), on entend notamment toute communication non autorisée d'informations détenues par l'OIAC à toute personne, à tout gouvernement ou à toute entité privée, quelles que soient l'intention ou les conséquences de cette divulgation. Il peut également y avoir manquement à la confidentialité lorsque des informations sont utilisées de façon irrégulière pour l'obtention d'un avantage personnel ou pour servir ou léser les intérêts d'une tierce partie. On estime qu'il y a eu violation des obligations de protection de l'information confidentielle lorsqu'il y a eu non-respect des procédures spécifiées pour la manipulation, la protection, la diffusion et la divulgation d'informations confidentielles, et qu'il en résulte un risque manifeste de divulgation non autorisée, que l'information en question ait ou non en fait été divulguée. Dans la pratique, il y a un chevauchement

considérable entre les manquements à la confidentialité et les violations des obligations de protection de l'information confidentielle.

3. Étape 1 : Enquête du directeur général

3.1 Comme prévu par les dispositions de l'Annexe sur la confidentialité, le Directeur général doit ouvrir sans tarder une enquête :

- a) dès lors qu'il y a "suffisamment d'éléments" indiquant une violation d'une obligation de protéger l'information confidentielle de la part d'un fonctionnaire du Secrétariat, de toute autre personne ou entité extérieure au Secrétariat ou de tout agent ou représentant d'un État partie; ou
- b) si un État partie a fait une allégation concernant un manquement à la confidentialité.

3.2 En particulier, le Directeur général doit ouvrir une enquête s'il apprend qu'il y a une possibilité raisonnable ou un risque manifeste de diffusion non autorisée d'informations confidentielles d'une façon qui, entre autres :

- a) violerait la politique ou les principes directeurs établis par l'Organisation pour la manipulation, la protection, la diffusion et la divulgation d'informations confidentielles; ou
- b) affecterait l'objet et le but de la Convention ou les intérêts de l'Organisation, d'un État partie ou d'une organisation commerciale ou gouvernementale ou d'un ressortissant d'un État partie, ou apporterait un avantage spécifique ou sélectif à une personne, un État ou à toute autre entité, y compris une entreprise commerciale.

3.3 Le Directeur général a l'obligation d'ouvrir une enquête dès lors qu'un État partie formule une allégation selon laquelle il y a eu manquement à la confidentialité. Une telle allégation devrait être formulée par écrit au Directeur général et, dans la mesure possible, étayée. Si possible, l'allégation devrait indiquer la nature de l'information en cause, le moment et le lieu où le manquement se serait produit et le préjudice réel ou, éventuellement, futur, que le manquement en question pourrait porter aux intérêts pertinents.

3.4 Lorsque le Directeur général a décidé d'ouvrir une enquête, cette décision doit être communiquée immédiatement aux États parties et aux fonctionnaires du Secrétariat impliqués dans le manquement allégué ou dans la violation soupçonnée.

3.5 L'enquête a pour but d'établir s'il y a effectivement eu manquement à la confidentialité ou violation des procédures à suivre pour la manipulation, la protection, la diffusion ou la divulgation d'informations confidentielles, ainsi que de déterminer la gravité de tout manquement, y compris le degré et la nature du préjudice éventuellement causé. L'enquête porte également sur les

moyens de renforcer le régime de confidentialité afin d'éviter que le manquement ou la violation des procédures ne se reproduisent.

- 3.6 Le Directeur général est directement responsable de l'enquête et la dirige personnellement, mais peut désigner un haut fonctionnaire pour mener à bien le travail d'enquête proprement dit. L'enquête commence par un examen préliminaire des circonstances qui ont entouré l'allégation ou l'indication d'une violation ainsi que par une analyse des éléments de preuve ou des renseignements étayant l'allégation, le cas échéant. Le Directeur général, à ce stade, peut conclure qu'il ne semble pas y avoir lieu de pousser l'affaire plus loin; en pareil cas, il peut, à son gré, soit consulter l'État partie qui a fait l'allégation, soit clore l'enquête et déclarer qu'aucune présomption de manquement ou de violation n'a été établie. Lorsqu'une présomption de manquement affectant les intérêts d'un État partie a été établie, le Directeur général informe le Conseil exécutif qu'une enquête sur le manquement en question a été ouverte et, avec l'assentiment de l'État partie intéressé, peut, si la demande lui en est faite, présenter des informations spécifiques au sujet de l'enquête.
- 3.7 La procédure d'enquête à suivre une fois que la présomption de manquement est établie peut comprendre les activités ci-après :
- a) rassemblement et examen d'éléments de preuve dans le cadre de l'OIAC ou de ses organes constituants;
 - b) examen de tout autre élément produit comme preuve par des États parties;
 - c) entretiens confidentiels avec des fonctionnaires du Secrétariat;
 - d) consultations avec les États parties intéressés, y compris avec les représentants de l'industrie ou des entités privées intéressées désignées par les États parties;
 - e) présentation à un État partie d'une demande tendant à obtenir des précisions concernant le traitement de l'information que lui a communiquée l'Organisation.
- 3.8 Le déroulement de l'enquête doit demeurer confidentiel et être soumis à une application rigoureuse du principe du "besoin de connaître". Il faudra veiller tout particulièrement à éviter les effets préjudiciables que la divulgation de l'existence d'une telle enquête pourrait avoir pour les fonctionnaires du Secrétariat ainsi que pour les intérêts des États parties. L'enquête doit être menée de façon objective et dans le plein respect d'une procédure régulière, et il ne doit pas être fait appel à la coercition pour obtenir des informations d'une personne quelconque. Aucun effort ne doit être négligé pour mener l'enquête à bien et pour prendre les mesures qu'appellent les conclusions de l'enquête dès que cela est possible et conformément à une procédure régulière.

3.9 Tous les États parties intéressés et les fonctionnaires du Secrétariat en cause doivent coopérer et appuyer la réalisation de l'enquête dans toute la mesure possible. À cette fin, les États parties peuvent devoir donner des précisions sur les enquêtes internes qui ont été menées, communiquer des éléments de preuve, donner des informations sur les actions judiciaires nationales introduites à propos de la même affaire et indiquer l'étendue et la nature des dommages éventuellement causés par un manquement à la confidentialité. Les fonctionnaires, pour leur part, doivent communiquer toutes les informations factuelles en leur possession en rapport avec les buts de l'enquête et leurs responsabilités professionnelles.

4. Étape 2 : Mesures provisoires

4.1 S'il est établi une présomption de manquement dans laquelle se trouve apparemment impliqué un fonctionnaire en exercice du Secrétariat :

- a) les procédures prévues par le Statut et le Règlement du personnel sont déclenchées afin d'imposer à l'intéressé des mesures restrictives provisoires pendant la durée de l'enquête, par exemple le retrait de certaines fonctions ou le refus de l'accès à certaines informations ou, si l'affaire semble grave, une suspension temporaire conformément au Statut et au Règlement du personnel de l'OIAC;
- b) le Directeur général envisage et peut proposer des mesures immédiates, si besoin est en consultation avec le Conseil exécutif, pour protéger tous les intérêts légitimes auxquels pourrait porter préjudice le manquement avéré ou allégué à la confidentialité, y compris les intérêts d'un État partie ou de l'Organisation;
- c) si l'enquête a été ouverte à la demande d'un État partie, le Directeur général informe ce dernier des mesures provisoires adoptées.

4.2 Un employé soupçonné d'être impliqué dans un manquement doit être informé par lettre recommandée de la décision de prendre de telles mesures provisoires, en indiquant à l'intéressé les raisons de ces mesures et en lui faisant savoir quels sont, le cas échéant, les recours qui lui sont ouverts.

4.3 Si l'étape préliminaire de l'enquête amène à présumer qu'un État partie a pu être responsable d'un manquement ou peut y avoir été impliqué de toute autre manière, le Directeur général envisage et peut proposer des mesures immédiates qui sont soumises au Conseil exécutif pour décision afin de protéger tous les intérêts légitimes auxquels pourrait porter préjudice le manquement à la confidentialité, y compris les intérêts de tout État partie ou de l'Organisation. Le Directeur général peut demander à l'État partie intéressé de donner des précisions concernant le traitement de l'information que lui a communiquée l'Organisation.

4.4 Si l'étape préliminaire de l'enquête amène à présumer qu'une personne physique ou morale se trouvant sous la juridiction d'un État partie a pu être responsable d'un manquement ou a pu y être impliquée, le Directeur général peut consulter ledit État partie et lui demander son aide, si besoin est, après approbation par le Conseil exécutif, pour l'adoption éventuelle de mesures pour protéger tous les intérêts légitimes auxquels pourrait porter préjudice le manquement à la confidentialité.

5. **Étape 3 : Rapport d'enquête**

5.1 Le Directeur général établit un rapport d'enquête qui indique s'il y a eu manquement à la confidentialité ou violation des procédures applicables à la manipulation, à la protection, à la diffusion ou à la divulgation de l'information confidentielle. Le rapport est établi en deux exemplaires : un exemplaire in extenso qui expose en détail les faits établis, et un exemplaire modifié dont les informations confidentielles spécifiques ont été expurgées de manière à veiller à ce que les informations confidentielles en rapport avec un manquement à la confidentialité ne soient pas divulguées plus largement que cela n'est autorisé, ainsi que pour protéger les aspects de la vie privée de fonctionnaires sans rapport avec l'affaire.

5.2 Le rapport in extenso est considéré comme confidentiel et est classifié et traité selon la sensibilité de l'information qu'il contient. Il ne doit être communiqué qu'à tous ceux qui sont directement intéressés par l'enquête, y compris, le cas échéant, les fonctionnaires impliqués dans un manquement avéré ou allégué à la confidentialité, ainsi que tout État partie ayant fait une allégation de manquement. Sous sa version modifiée, le rapport peut être communiqué à tout État partie sur sa demande, et il est résumé dans le rapport annuel sur la confidentialité que le Directeur général présente à la Conférence conformément au paragraphe 3 de l'Annexe sur la confidentialité. Lorsque cela est possible, le rapport doit, dans ses deux versions, contenir des propositions concrètes visant à renforcer le régime de confidentialité. Si le Directeur général a demandé au Conseil exécutif d'approuver des mesures provisoires conformément aux paragraphes 4.1, 4.3 ou 4.4 du présent chapitre, il rend compte directement au Conseil exécutif de l'application de ces mesures provisoires.

5.3 Lorsqu'il est constaté dans le rapport qu'il y a eu manquement à la confidentialité, le rapport doit indiquer le degré de gravité de ce manquement, en se référant aux facteurs ci-après :

- a) la question de savoir si le manquement s'est produit de manière délibérée ou accidentelle ou par une omission fautive;
- b) la question de savoir s'il y a eu violation des obligations prévues par la présente politique et des directives administratives connexes ou d'accords spécifiques comme l'engagement personnel de secret ou un accord d'installation;

- c) l'étendue du préjudice réel ou potentiel, le cas échéant, pour les intérêts de toute partie concernée;
 - d) l'étendue de tout avantage privé obtenu par la divulgation non autorisée ou l'utilisation irrégulière de l'information, en particulier pour ce qui est de promouvoir des intérêts personnels, d'obtenir un avantage compétitif, de procurer un avantage à un tiers ou de vouloir léser les intérêts d'une tierce partie.
- 5.4 Si l'État partie qui a demandé l'ouverture d'une enquête n'est pas satisfait du rapport publié par le Directeur général à la suite de l'enquête, et après que toutes les tentatives raisonnables ont été faites pour régler la question au moyen de consultations, l'État partie a le droit de demander la convocation de la Commission de la confidentialité pour qu'elle examine l'affaire.
- 5.5 Si l'enquête n'est pas achevée dans les trois mois suivant la décision initiale de l'ouvrir, le Directeur général doit présenter un rapport intérimaire aux destinataires du rapport final. Ce rapport doit indiquer les mesures adoptées jusqu'alors et, le cas échéant, les obstacles rencontrés ou les raisons ayant retardé l'enquête. Si, après consultation, il apparaît que ces obstacles ou ces retards ne peuvent pas être aisément surmontés, le Directeur général peut clore l'enquête et, dans son rapport, demander la convocation de la Commission de la confidentialité pour qu'elle examine l'affaire conformément au paragraphe 23 de l'Annexe sur la confidentialité.
- 5.6 Si, à l'issue de l'enquête, il est déterminé qu'il n'y a pas eu manquement à la confidentialité ni violation, le Directeur général, dans son rapport, inclut une formule exonérant le fonctionnaire du Secrétariat accusé ou l'État partie intéressé.

6. Étape 4 : Suite à donner au rapport d'enquête

Lorsque l'enquête et le rapport constatent qu'il y a eu manquement ou violation, quatre grandes catégories de mesures peuvent être envisagées :

- a) des mesures disciplinaires internes de l'Organisation à l'égard des fonctionnaires en exercice du Secrétariat et des sanctions à l'égard des anciens fonctionnaires;
- b) l'ouverture d'une action en justice dans le cadre de la juridiction nationale d'un État partie, après levée, le cas échéant, de toute immunité de juridiction;
- c) la réforme ou le renforcement du régime de confidentialité de l'OIAC;
- d) d'autres mesures lorsqu'un État partie semble responsable.

7. Étape 4a : Sanctions disciplinaires contre les fonctionnaires en exercice du Secrétariat

- 7.1 Si, à l'issue de l'enquête, il est déterminé qu'un manquement ou une violation a été commis par un fonctionnaire du Secrétariat, le Directeur général applique les mesures disciplinaires appropriées conformément au Statut et au Règlement du personnel de l'OIAC.
- 7.2 Pour déterminer les mesures à appliquer à un fonctionnaire, il est tenu compte de la gravité du manquement et du degré de responsabilité individuelle.
- 7.3 La décision prise par le Directeur général en matière de mesures disciplinaires peut être sujette à révision ou appel, conformément aux procédures établies par le Statut et le Règlement du personnel de l'OIAC.

8. Étape 4b : Sanctions contre d'anciens fonctionnaires du Secrétariat

S'il est déterminé dans le rapport qu'un manquement ou une violation a été commis par un ancien fonctionnaire du Secrétariat, le Directeur général peut décider d'appliquer toutes les mesures pouvant encore être invoquées aux termes du Statut et du règlement provisoire du personnel de l'OIAC. Ces mesures peuvent inclure la perte d'indemnités pécuniaires ou autres droits tels que ceux liés à la Caisse de prévoyance de l'OIAC.

9. Étape 4c : Mesures à prendre en cas de levée de l'immunité

- 9.1 Indépendamment de ces mesures disciplinaires, le Directeur général peut décider de lever l'immunité de poursuites dont peuvent bénéficier aussi bien les fonctionnaires en exercice du Secrétariat que les anciens fonctionnaires qui peuvent continuer de jouir de l'immunité en raison des actes qu'ils ont accomplis dans l'exercice de leurs fonctions au Secrétariat. La levée de l'immunité ne peut être envisagée qu'en cas de manquement grave, lorsque la responsabilité individuelle a été établie et lorsqu'il en est résulté un préjudice; elle doit être précédée de consultations confidentielles quant à l'éventualité de l'application du régime prévu par une juridiction nationale. L'engagement personnel de secret signé par le fonctionnaire devrait être pris en considération pour déterminer s'il peut être utilisé aux fins d'une action en justice.
- 9.2 Toute décision concernant la levée de l'immunité peut être sujette à révision ou à appel conformément aux procédures prévues par le Statut et le Règlement du personnel de l'OIAC.
- 9.3 Dans la mesure du possible, les États parties prennent les mesures juridiques appropriées qu'appelle la levée de l'immunité. Les mesures prises doivent être conformes au chapitre IX.3, y compris pour ce qui est des actions en justice pouvant être ouvertes contre les fonctionnaires en exercice ou anciens fonctionnaires dont l'immunité a été levée. Si le fonctionnaire ou l'ancien fonctionnaire responsable d'un manquement réside sur le territoire ou se trouve sur la juridiction d'un État qui n'est pas partie à la Convention, le Directeur général peut solliciter l'autorisation du Conseil exécutif ou de la Conférence

d'entamer des consultations dans le but d'encourager ledit État à prendre les mesures appropriées ou à faciliter l'adoption de ces mesures en vue d'appuyer les procédures judiciaires auxquelles a donné lieu le manquement dont il s'agit.

10. Étape 4d : Autres actions en justice dans le cadre d'une juridiction nationale

10.1 Si, à l'issue de son enquête, le Directeur général détermine qu'une personne physique ou morale (y compris une entreprise commerciale) relevant de la juridiction d'un État partie semble avoir été responsable d'un manquement à la confidentialité, a tiré un avantage particulier d'un manquement ou, de toute autre manière, a été impliquée dans un manquement à la confidentialité, ledit État partie peut être invité à entamer les actions en justice appropriées conformément au chapitre IX.3.

10.2 Si une personne physique ou morale jugée responsable d'un manquement réside ou se trouve sous la juridiction d'un État qui n'est pas partie à la Convention, le Directeur général peut solliciter l'autorisation du Conseil exécutif ou de la Conférence d'entamer des consultations dans le but d'encourager ledit État à prendre les mesures appropriées ou à faciliter l'adoption de ces mesures en vue d'appuyer les procédures judiciaires auxquelles a donné lieu le manquement dont il s'agit.

11. Étape 4e : Mesures à prendre lorsqu'un État partie semble responsable

11.1 Si, à l'issue de son enquête, le Directeur général détermine qu'un État partie, y compris un représentant d'un État partie, semble avoir été responsable d'un manquement à la confidentialité :

- a) ledit État partie aide le Directeur général à régler la question, dans toute la mesure possible, notamment en fournissant des précisions complètes concernant le traitement et la protection de l'information confidentielle que lui a communiquée l'Organisation;
- b) ledit État partie entame les actions en justice appropriées conformément au chapitre IX.3 de la présente politique;
- c) le Directeur général peut soulever la question auprès du Conseil exécutif et demander l'adoption des autres mesures qu'appelle le rapport d'enquête.

11.2 La responsabilité éventuelle d'un État partie doit être évaluée à la lumière des obligations qui lui incombent en vertu de la Convention, en particulier du paragraphe 6 de l'Article VII et du paragraphe 4 de l'Annexe sur la confidentialité.

11.3 Si l'enquête établit qu'un État partie semble responsable d'un manquement, la Commission de la confidentialité peut être convoquée en cas de différend pour examiner l'affaire conformément au paragraphe 23 de l'Annexe sur la

confidentialité et aux procédures détaillées établies en ce qui concerne le fonctionnement de la Commission.

- 11.4 Si l'enquête établit que le manquement à la confidentialité ne concerne que les intérêts et les actes d'États parties, le Directeur général en informe les États parties intéressés.

12. Étape 4f : Mesures visant à réformer ou à renforcer le régime de confidentialité

- 12.1 Le rapport d'enquête doit contenir des propositions concrètes de réforme ou de renforcement de la protection de l'information confidentielle au sein de l'Organisation, à la fois spécifiquement pour empêcher que tout manquement ou toute violation établi à l'issue de l'enquête ne se reproduise, et sur la base des autres observations pouvant se dégager de l'enquête quant à la protection générale de la confidentialité.
- 12.2 Le Directeur général soumet à la Conférence pour adoption à sa session suivante les éventuelles propositions de réforme ou de renforcement de la présente politique ou des autres documents de base en la matière pouvant se dégager de l'enquête.
- 12.3 Si l'enquête démontre qu'il est nécessaire d'améliorer les procédures de traitement et de protection de l'information ou de modifier à d'autres égards les procédures de fonctionnement du Secrétariat, le Directeur général publie les directives administratives appropriées pour appliquer sans tarder ces changements.

CHAPITRE IX.2 : RÈGLES RÉGISSANT LE FONCTIONNEMENT DE LA COMMISSION POUR LE RÈGLEMENT DES LITIGES RELATIFS À LA CONFIDENTIALITÉ ("COMMISSION DE LA CONFIDENTIALITÉ")

1. Règles régissant la composition de la Commission de la confidentialité

- 1.1 La Commission de la confidentialité en formation plénière est composée de personnes nommées à titre individuel et choisies sur une liste de candidats présentés par les États parties à la Convention. Chaque État partie peut proposer la candidature d'un de ses ressortissants, pour autant que ce dernier soit disponible et ait qualité pour siéger à la Commission. La liste de candidats sera soumise à la Conférence et 20 personnes choisies sur celle-ci seront nommées pour siéger à la Commission pour un mandat initial de deux ans.
- 1.2 Les 20 personnes à nommer seront choisies à la suite d'un processus de consultations avec les groupes régionaux menées sous la direction du Président de la Conférence, compte tenu du principe de la rotation et de la nécessité d'assurer une représentation appropriée des spécialisations pertinentes, étant entendu que les États parties appartenant à chacune des cinq régions définies au paragraphe 23 de l'Article VIII de la Convention désignent quatre candidats. Conformément au paragraphe 18 de l'Article VIII, la Conférence procède à la désignation en bonne et due forme des membres de la Commission au titre des décisions relevant d'une question de fond.
- 1.3 Les États parties doivent proposer leurs candidats sur la base de l'efficacité, de la compétence et de l'intégrité de l'intéressé et de la connaissance qu'il a d'un ou de plusieurs domaines en rapport avec les travaux de la Commission, par exemple les procédures de règlement des différends de divers types, les dispositions de la Convention relatives à la confidentialité et à la vérification, l'industrie chimique, les questions militaires et la sécurité des données, le droit international et les systèmes juridiques nationaux.
- 1.4 La Commission plénière se réunira en session inaugurale pendant la première Conférence et, à cette occasion, elle élira par consensus parmi ses membres son président, pour un mandat initial d'un an. Par la suite, la Commission tiendra sa session ordinaire annuelle en même temps que la session ordinaire annuelle de la Conférence et, à cette occasion, élira son président pour l'année suivante conformément aux règles de procédure approuvées par la Conférence.

2. Litiges dont la Commission de la confidentialité peut connaître

La Commission de la confidentialité peut être appelée à examiner des litiges dans les circonstances ci-après :

- a) lorsqu'elle est invitée à examiner des litiges découlant d'un manquement avéré ou allégué à la confidentialité faisant intervenir à la fois un État partie et l'Organisation;

- b) lorsque, conformément au paragraphe 4 de l'Article XIV de la Convention, la Conférence des États parties la charge d'examiner un litige relatif à la confidentialité autre qu'un litige du type de ceux visés à l'alinéa qui précède;
- c) lorsque deux États parties qui sont parties à un litige sur une question relative à la confidentialité font appel à elle pour régler leur différend conformément au paragraphe 2 de l'Article XIV de la Convention.

3. Règles régissant le fonctionnement de la Commission de la confidentialité

Les règles ci-après, qui ont été approuvées par la Conférence, à sa troisième session, régissent les règles de procédure détaillées de la Commission de la confidentialité.

Ouverture de la procédure de règlement des différends

- 3.1 Au cas où la Commission serait appelée à examiner un litige dans les circonstances énoncées au paragraphe 2 ci-dessus, la question est immédiatement soumise au Président, lequel en informe tous les membres de la Commission. Le Président consulte tous les membres de la Commission sur les délais à fixer et la procédure à suivre pour régler le litige, et peut convoquer selon que de besoin la Commission, conformément aux principes établis par les règles de procédures qui tiennent compte, entre autres, des indications données par l'une des parties au litige concernant la gravité ou l'urgence de l'affaire, la complexité des questions de fond en jeu, l'ampleur de la perte ou du dommage allégué et la nécessité de réduire au minimum la diffusion des informations confidentielles dont il s'agit. À l'issue de ces étapes préliminaires, le Président obtient l'accord de la Commission sur les délais envisagés et la procédure qu'il est proposé de suivre pour résoudre le litige.

Recherche d'un règlement à l'amiable

- 3.2 La Commission s'emploie initialement à éclaircir l'objet du litige et à le régler d'une façon qui soit acceptable pour les parties au litige et qui soit conforme aux droits et aux obligations des États parties et de l'Organisation en vertu de la Convention. Afin de ne négliger aucun effort pour encourager les parties au litige à souscrire à une solution mutuellement satisfaisante, la Commission devrait avoir recours aux moyens de règlement des différends appropriés eu égard aux circonstances, compte tenu, le cas échéant, des préférences communes exprimées par les parties au litige : par exemple, les moyens d'abord utilisés comprendraient de préférence un processus de médiation visant en pratique à parvenir à un règlement à l'amiable par la voie de la négociation.
- 3.3 À cette fin, la Commission peut constituer un comité consultatif chargé d'entreprendre des consultations officieuses à des fins de médiation; ce comité consultatif serait normalement composé de cinq membres de la Commission, dont chacun représentera une région, à moins que les parties au litige ne conviennent d'une autre structure, similaire. Ledit comité devra rendre compte

à la Commission de l'avancement et de l'issue des consultations éventuelles et, le cas échéant, la solution à laquelle ce processus de médiation aura pu aboutir devra être soumise à l'examen de la Commission avant d'être entérinée.

- 3.4 Si la Commission parvient par médiation, par tous moyens appropriés, à un règlement du différend acceptable pour les parties au litige, cette issue est entérinée par la Commission et une communication factuelle rendant compte de l'issue du différend est faite aux parties au litige pour que leur accord soit consigné.

Absence de règlement à l'amiable

- 3.5 S'il n'est pas possible de parvenir à une telle issue, la Commission établit un rapport esquissant les faits essentiels du différend, commentant objectivement celui-ci et recommandant les autres mesures qui pourraient être adoptées pour le régler par les parties au litige elles-mêmes, par la Commission, par la Conférence ou par tout autre organe de l'Organisation, en vertu d'un mandat précis conféré par la Conférence. Ce rapport est remis par la Commission aux parties au litige. Le rapport et les recommandations de la Commission ne lient pas les parties au litige mais pourront servir de base ou de justification aux autres mesures que pourront prendre les parties au litige ou les organes compétents de l'Organisation : en particulier, la Commission peut soumettre la question à la Conférence, ou à tout autre organe de l'Organisation, en vertu d'un mandat précis conféré par la Conférence, si les parties au litige conviennent que cela est nécessaire en raison de l'urgence de l'affaire.
- 3.6 Si deux États parties au litige en conviennent et subordonnent à cette condition la soumission d'un litige à la Commission, cette dernière peut, avec le consentement exprès des parties au litige, décider que le différend sera soumis à un règlement par arbitrage qui liera les parties au litige.
- 3.7 Lorsqu'elle prépare ses rapports et ses recommandations, la Commission doit tenir compte du principe du "besoin de connaître" qui régit l'accès à l'information confidentielle ainsi que des procédures spécifiques qu'elle aura adoptées pour veiller à ce que la confidentialité de l'information demeure sauvegardée dans l'exercice de ses fonctions. Les membres de la Commission sont eux-mêmes tenus par toutes ces obligations prévues par la Convention et par la présente politique en matière de traitement et de protection de l'information confidentielle.

Rapports à la Conférence

- 3.8 La Commission demeure responsable à l'égard de la Conférence et présente un rapport sur ses activités au cours de l'année écoulée à chacune des sessions ordinaires de la Conférence. Ce rapport indique notamment le nombre de règlements obtenus par médiation ou par arbitrage, les catégories de différends examinés et l'issue à laquelle l'examen de la Commission est parvenu, avec tous les détails compatibles avec la nécessité de continuer à protéger la confidentialité de l'information. La Commission présente également un rapport

général sur son activité ainsi que sur son efficacité et son efficience et peut formuler des propositions ou recommandations tendant à les améliorer.

Responsabilités des membres de la Commission de la confidentialité

- 3.9 La Commission de la confidentialité, et ses membres individuellement, n'acceptent dans leurs fonctions ni ingérence, ni instructions, du Secrétariat ou d'autres organes de l'Organisation, mais doivent se conformer au mandat qu'aura pu lui confier la Conférence. Toutefois, le Président peut solliciter et recevoir du Secrétariat, dans l'exercice de ses fonctions, un appui et une assistance au titre des services de conférence et des services logistiques. Les membres de la Commission ayant un intérêt dans la question faisant l'objet du différend s'abstiennent de s'occuper de l'affaire; il leur incombe de se récuser dès qu'un différend leur est notifié. Ils n'exercent aucune autre fonction au sein de l'Organisation ou de ses organes et n'entretiennent aucune relation et n'ont aucun intérêt d'ordre juridique ou financier en rapport avec l'Organisation.

Réunions de la Commission de la confidentialité

- 3.10 La Commission de la confidentialité tient sa session inaugurale et ses sessions ordinaires, à l'occasion des sessions ordinaires de la Conférence, conformément aux dispositions du paragraphe 1.4 du présent chapitre, et elle se réunit aussi souvent que nécessaire pour examiner les différends dont elle est saisie.
- 3.11 À sa session inaugurale et à ses sessions annuelles ultérieures, la Commission :
- a) choisit par consensus un président pour l'année à venir, compte tenu du principe de la rotation entre les régions définies au paragraphe 23 de l'Article VIII de la Convention;
 - b) examine et adopte un rapport à la Conférence sur l'issue des différends qu'elle a examinés pendant l'année écoulée;
 - c) examine et adopte un rapport à la Conférence sur son activité, son efficacité et son efficience, et examine les recommandations ou propositions éventuellement formulées par le Président à ce propos;
 - d) si besoin est, revoit ses règles de procédure et y recommande des amendements;
 - e) établit à l'intention du Président les principes directeurs, ou lui adresse les demandes qu'elle juge appropriées;
 - f) formule toutes autres recommandations ou propositions à la Conférence qu'elle juge appropriées.

Préparation des règles de procédure

3.12 La Conférence approuvera les règles de procédure détaillées de la Commission, en précisant entre autres :

- a) les formalités de convocation des réunions de la Commission;
- b) les modalités selon lesquelles les différends doivent être immédiatement portés à la connaissance du Président, et les modalités selon lesquelles le Président doit en aviser immédiatement tous les membres de la Commission;
- c) les modalités selon lesquelles la Commission doit prendre une décision au sujet des délais et de la procédure de règlement des différends conformément au paragraphe 3.1 du présent chapitre;
- d) les modalités selon lesquelles la Commission doit entériner toute solution à l'amiable d'un différend, et les modalités selon lesquelles l'accord des parties au litige à ce règlement doit être consigné;
- e) les procédures applicables à la préparation et à la présentation des rapports et recommandations formulées par la Commission aux parties au litige et à la Conférence ou à tout autre organe de l'Organisation, conformément aux pouvoirs conférés par la Conférence;
- f) la procédure à suivre pour veiller à ce que la confidentialité de l'information demeure sauvegardée dans l'exercice des fonctions de la Commission, conformément à l'Annexe sur la confidentialité, à la politique de l'OIAC en matière de confidentialité et au principe du "besoin de connaître" régissant l'accès à l'information confidentielle;
- g) la procédure à suivre pour déterminer les délais dans lesquels la Commission doit s'acquitter de ses tâches;
- h) les procédures applicables à l'élection des présidents successifs, à l'élection des membres successifs de la Commission et aux mesures à prendre pour pourvoir les postes devenus vacants, compte tenu des principes posés aux paragraphes 1.1, 1.2 et 1.3 du présent chapitre;
- i) s'agissant des membres de la Commission devant lesquels l'examen d'un différend spécifique est en cours, le mécanisme à appliquer pour qu'ils puissent plus facilement continuer à s'acquitter de leurs tâches pendant tout le processus de règlement du différend, ledit mécanisme devant être conforme et assujéti aux principes énoncés au paragraphe 1 du présent chapitre, qui régissent la composition de la Commission;
- j) une procédure d'évaluation de l'efficacité de la Commission;
- k) une procédure d'amendement des règles de procédure.

Procédure de prise de décisions

- 3.13 Le Président s'efforce de dégager un consensus au sujet de toute décision ou recommandation au sein de la Commission plénière, étant entendu toutefois que celle-ci, au cas où il ne serait pas possible de parvenir à un consensus sur une décision spécifique, peut régler la question à la majorité des deux tiers de tous ses membres.

CHAPITRE IX.3 : RÔLE DES ÉTATS PARTIES EN CE QUI CONCERNE LES PROCÉDURES APPLICABLES EN CAS DE MANQUEMENT À LA CONFIDENTIALITÉ

1. Introduction : obligations prévues par la Convention

1.1 Les dispositions de la Convention qui se rapportent spécifiquement à l'intervention des États parties dans la protection de la confidentialité de l'information stipulent notamment que les différents États parties ont l'obligation :

- a) dans la mesure du possible, de coopérer avec le Directeur général et de l'appuyer dans ses enquêtes sur tout manquement avéré ou allégué à la confidentialité, ainsi que lorsqu'il prend des mesures qui s'imposent s'il est établi qu'il y a eu manquement (paragraphe 21 de l'Annexe sur la confidentialité);
- b) de traiter de façon confidentielle et particulière l'information et les données qu'ils reçoivent en confiance de l'Organisation concernant l'application de la Convention, ainsi que de traiter cette information et ces données exclusivement dans le cadre des droits et obligations qui sont les leurs aux termes de la Convention et en se conformant aux dispositions de l'Annexe sur la confidentialité (paragraphe 6 de l'Article VII);
- c) de traiter l'information reçue de l'Organisation selon le niveau de confidentialité retenu pour cette information (paragraphe 4 de l'Annexe sur la confidentialité);
- d) d'apporter, sur demande, des précisions concernant le traitement de l'information que leur a communiquée l'Organisation (paragraphe 4 de l'Annexe sur la confidentialité).

1.2 En outre, l'application de la disposition relative à la levée de l'immunité figurant au paragraphe 20 de l'Annexe sur la confidentialité signifie qu'une juridiction nationale compétente devrait s'appliquer au cas où un fonctionnaire du Secrétariat aurait commis un manquement grave à la confidentialité.

1.3 Étant donné que la présente politique a trait à l'activité de l'Organisation elle-même et à ses rapports avec les États parties, le présent chapitre n'établit ni ne prescrit les mesures internes spécifiques que chaque État partie peut prendre dans le cadre de la réalisation des objectifs de la Convention en matière de confidentialité, ni la façon dont les États parties s'acquitteront des obligations spécifiques qui leur incombent en la matière, par exemple pour ce qui est de l'application de la juridiction nationale ou du versement d'une indemnisation en cas de manquement à la confidentialité. Si cela est jugé nécessaire ou souhaitable dans des cas particuliers, ces mesures internes ou obligations spécifiques pourront être mentionnées et définies plus en détail dans les

accords bilatéraux ou autres arrangements d'application conclus entre l'Organisation et les États parties.

2. Situations possibles

Les obligations qui incombent à un État partie en matière de confidentialité peuvent être mises en jeu dans différentes situations pratiques, et en particulier dans le contexte :

- a) d'une enquête de l'OIAC sur un manquement avéré ou allégué à la confidentialité;
- b) de la levée de l'immunité par le Directeur général de l'OIAC en cas de manquement grave à la confidentialité;
- c) d'un manquement à la confidentialité dont un État partie est directement responsable;
- d) d'un manquement à la confidentialité de la part d'une personne physique ou morale relevant de la juridiction d'un État partie.

3. Enquête sur les manquements à la confidentialité

Indépendamment de l'obligation générale prévue au paragraphe 7 de l'Article VII de la Convention de fournir une assistance au Secrétariat, chaque État partie a une obligation spécifique d'aider le Directeur général dans ses enquêtes sur tout manquement avéré ou allégué à la confidentialité (comme indiqué à l'alinéa *a* du paragraphe 1.1 du présent chapitre). Dans le cadre de ses obligations, la nature de l'appui et de la coopération que les États parties doivent apporter dans le contexte d'une enquête spécifique devra être déterminée dans chaque cas particulier.

4. Levée de l'immunité en cas de manquement grave à la confidentialité

- 4.1 La Convention (paragraphe 20 et 21 de l'Annexe sur la confidentialité) présume qu'une juridiction doit s'appliquer si l'immunité de juridiction est levée dans le cas d'un fonctionnaire du Secrétariat ayant commis un manquement grave à la confidentialité. Si le Directeur général décide de lever l'immunité en pareil cas, le fonctionnaire pourra, sur la demande du Directeur général ou d'un État partie affecté par le manquement grave à la confidentialité, faire l'objet d'une procédure judiciaire en vertu d'une juridiction compétente d'un État partie. Les États parties devront prendre toutes les mesures administratives et juridiques qui s'imposent pour faire en sorte que ce mécanisme puisse être appliqué efficacement.
- 4.2 Les États parties demeureront responsables au premier chef de la détermination de l'applicabilité de la juridiction nationale dans chaque cas particulier. La Conférence pourra aussi examiner des propositions tendant à mettre en place un mécanisme de nature à appliquer un système cohérent et complet de

sanctions au cas où les fonctionnaires du Secrétariat manqueraient gravement à leurs obligations en matière de confidentialité.

5. Manquements imputés à un État partie

Si les informations que l'Organisation communiquent en confiance à un État partie sont divulguées à des destinataires non autorisés ou si ledit État partie, de quelque autre manière, enfreint leur caractère confidentiel, ledit État aura manqué aux obligations qui lui incombent en vertu du paragraphe 6 de l'Article VII de la Convention et du paragraphe 4 de l'Annexe sur la confidentialité. Le fait d'appliquer un traitement confidentiel aux informations reçues en confiance est d'ailleurs un élément essentiel à une application efficace de la Convention dans son ensemble. En pareil cas, un manquement à la confidentialité pourra être imputé à l'État partie en question, lequel sera considéré comme ayant contrevenu à ces obligations. Tel pourra être le cas à l'issue de l'enquête menée par le Directeur général au sujet d'un manquement avéré ou allégué à la confidentialité¹⁴, auquel cas la question serait soumise aux mécanismes de règlement des différends prévus par la Convention, et en particulier à l'examen de la Commission de la confidentialité¹⁵, sous l'autorité de la Conférence.

6. Autres cas d'application de la juridiction nationale

Comme indiqué au paragraphe 5 ci-dessus, le fait pour un État partie de divulguer des informations qui lui ont été communiquées en confiance par l'Organisation en manquant à respecter leur confidentialité serait contraire aux obligations qui incombent aux États parties conformément au paragraphe 6 de l'Article VII de la Convention et au paragraphe 4 de l'Annexe sur la confidentialité. Les États parties sont par conséquent tenus de prendre les mesures administratives et juridiques appropriées qu'ils jugent nécessaires pour veiller à ce que ces obligations soient respectées comme il convient, notamment par tous agents opérant avec leur autorisation ou sous leur parrainage.

¹⁴ Conformément à l'étape 4e des procédures d'enquête en cas de manquement à la confidentialité prévue dans le chapitre IX.1

¹⁵ Voir le chapitre IX.2.

CHAPITRE X

RAPPORT ANNUEL SUR L'APPLICATION DU RÉGIME RÉGISSANT LE TRAITEMENT DE L'INFORMATION CONFIDENTIELLE PAR LE SECRÉTARIAT

1. Le Directeur général est tenu de faire rapport annuellement à la Conférence sur l'application par le Secrétariat du régime régissant le traitement de l'information confidentielle (paragraphe 3 de l'Annexe sur la confidentialité). Le rapport devra porter sur les points indiqués ci-dessous, mais de manière à éviter de compromettre de quelque façon que ce soit le caractère confidentiel des informations communiquées au Secrétariat ou traitées ou détenues par ce dernier et soumises aux principes de la présente politique.
2. Dans son rapport, le Secrétaire général rend compte plus particulièrement des aspects pratiques du traitement de l'information confidentielle par les fonctionnaires du Secrétariat (paragraphe 3 de l'Annexe sur la confidentialité) au cours de l'année écoulée, et notamment :
 - 2.1 des ressources nécessaires pour mettre en œuvre le régime de confidentialité, avec une estimation du volume des informations confidentielles traitées par le Secrétariat;
 - 2.2 des principales mesures adoptées pour mettre en œuvre le régime de confidentialité, notamment pour ce qui est des principaux changements apportés aux procédures ou en matière de personnel, ainsi que des programmes de formation et de sensibilisation du personnel exécutés pour faire en sorte que les fonctionnaires du Secrétariat se conforment au régime établi;
 - 2.3 des manquements avérés ou allégués à la confidentialité et des mesures prises pour faire enquête à leur sujet et y remédier;
 - 2.4 des problèmes ou des questions de politique générale qui ont surgi dans le contexte du régime de confidentialité.
3. Sans que ceci limite la portée du rapport, ce dernier devra traiter en particulier, en détail, des éléments suivants :
 - 3.1 le nombre approximatif d'informations confidentielles reçues, générées, conservées et diffusées par le Secrétariat;
 - 3.2 le nombre d'informations confidentielles diffusées au cours de l'année précédente, les destinataires desdites informations et les modalités de leur

- diffusion¹⁶, et l'accès accordé à des destinataires autorisés associés à l'Organisation¹⁷;
- 3.3 le nombre d'autorisations accordées en vue de l'accès à l'information confidentielle conformément au paragraphe 11 de l'Annexe sur la confidentialité, et les changements apportés, le cas échéant, aux postes des fonctionnaires de rang supérieur chargés de la mise en œuvre du régime de confidentialité;
 - 3.4 les ressources nécessaires et les exigences opérationnelles, et les problèmes de politique générale découlant de l'application des procédures de protection de l'information confidentielle dans le cadre des activités de vérification et du SGI;
 - 3.5 le cas échéant, les changements apportés aux directives administratives publiées pour mettre en œuvre la présente politique, y compris les changements éventuellement apportés aux directives administratives en vigueur à la suite d'amendements à la présente politique approuvés par la Conférence;
 - 3.6 le cas échéant, toute perte déclarée d'informations confidentielles;
 - 3.7 le cas échéant, les manquements avérés ou allégués à la confidentialité faisant intervenir des fonctionnaires du Secrétariat, les enquêtes menées par le Directeur général et les mesures adoptées à l'issue de ces enquêtes;
 - 3.8 le cas échéant, les changements apportés au SGI ayant des incidences substantielles sur la sécurité des informations confidentielles contenues dans le système;
 - 3.9 la réalisation de programmes de formation et de sensibilisation du personnel concernant l'obligation de protéger l'information confidentielle et de respecter le régime de confidentialité, et la diffusion d'instructions, de conseils et de rappels périodiques à tous les fonctionnaires du Secrétariat concernant les principes énoncés dans la présente politique et les procédures à appliquer pour la mettre en œuvre, ainsi que les principes et procédures applicables en matière de sécurité et les sanctions auxquelles ils s'exposeraient en cas de divulgation non autorisée d'informations confidentielles;
 - 3.10 le nombre d'informations confidentielles auxquelles des destinataires autorisés associés à l'Organisation ont eu accès, conformément aux principes énoncés au paragraphe 2.12 du chapitre VI de la présente politique.

¹⁶ Par "diffusion" de l'information, l'on entend la divulgation autorisée d'informations à l'extérieur de l'Organisation elle-même (y compris tous ses éléments constituants) et des gouvernements des États parties (plus précisément, en dehors des organisations gouvernementales et des entités ou personnes autorisées relevant des États parties et chargées de la mise en œuvre de la Convention (paragraphe 1.1 du chapitre VII de la présente politique).

¹⁷ Conformément aux principes énoncés au paragraphe 2.12 du chapitre VI de la présente politique.

CHAPITRE XI

PROCÉDURE D'AMENDEMENT

1. Tout État partie ou le Directeur général peut proposer des amendements à la présente politique. Le Directeur général soumet les amendements proposés, par l'intermédiaire du Conseil exécutif, à l'examen et à l'approbation de la Conférence des États parties conformément au règlement intérieur de cette dernière.
2. Le Directeur général publie sans tarder les changements qu'il faudrait apporter aux directives administratives en vigueur du fait des amendements à la présente politique qu'aurait approuvés la Conférence, et il rend compte desdits changements au Conseil exécutif et à la Conférence dans son rapport annuel sur l'application du régime de confidentialité. Le Directeur général veille à ce que tous les membres du personnel de l'Organisation soient immédiatement informés de tels amendements et reçoivent toute la formation appropriée, de préférence dans un délai de trois mois après l'entrée en vigueur des amendements, ou à défaut dès que possible après celle-ci.

Glossaire

"La Convention" : la Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction

"L'Annexe sur la confidentialité" : l'Annexe sur la protection de l'information confidentielle (annexe à la Convention)

"L'Organisation" ou l'"OIAC" : l'Organisation pour l'interdiction des armes chimiques, créée en application du paragraphe premier de l'Article VIII de la Convention

"La Conférence" : la Conférence des États parties, constituée en application du paragraphe 4 de l'Article VIII de la Convention

"Le Secrétariat" : le Secrétariat technique, établi en application du paragraphe 4 de l'Article VIII de la Convention

"La Commission de la confidentialité" : la Commission pour le règlement des litiges relatifs à la confidentialité, évoquée au paragraphe 23 de l'Annexe sur la confidentialité

"Manuel des procédures de confidentialité" : aucune abréviation en français

"Bureau de la confidentialité et de la sûreté" : aucune abréviation en français

"SGI" : système de gestion de l'information utilisé au sein du Secrétariat technique

--- 0 ---