Cour
Pénale
Internationale

International
Criminal
Court

Instruction administrative
ICC/AI/2007/001

Date: 19/06/2007

POLITIQUE DE PROTECTION DES INFORMATIONS DE LA CPI

Aux fins de l'établissement d'un système de classification et de traitement destiné à protéger les informations internes à la Cour et les informations non classifiées fournies à la Cour, et en application de la Directive présidentielle CPI/DP/2005/001, le Greffe promulgue les dispositions suivantes :

Note explicative

La Cour recueille, conserve, traite et diffuse des informations qui, pour la plupart, sont sensibles en ce sens que leur divulgation ou modification non autorisées peuvent compromettre la Cour, nuire à sa réputation, porter préjudice aux affaires dont elle est saisie, aux témoins, à son personnel, à ses responsables ou à tout autre interlocuteur. Elles doivent donc être protégées de manière systématique.

Actuellement, on n'est pas très sûr de la forme que prendra cette protection. Pour le même type d'information, les pratiques en vigueur diffèrent selon l'unité, la section, la division ou l'organe. La présente instruction administrative vise à définir les informations qui doivent être protégées et à fixer les modalités de cette protection. Comme c'est le cas pour toute instruction administrative, elle s'applique aux membres du personnel mais non aux responsables élus, y compris les membres du personnel directement sous leurs ordres.

La présente instruction administrative ne fait délibérément aucune différence entre les documents « judiciaires » et « administratifs ». Les documents de la Cour peuvent être l'un ou l'autre, ou n'appartenir ni à l'une ni à l'autre de ces catégories. C'est la valeur, et donc le risque inhérent, de l'information qui est à prendre en compte au moment d'établir des mesures de protection étant donné que la compromission peut avoir une incidence sur la crédibilité des juges, des enquêtes, des aspects juridiques, financiers, opérationnels et réglementaires de la Cour, ou sur sa réputation. Le Journal officiel de la Cour exige qu'il y ait un certain niveau de confidentialité pour les archives de la Cour, et pourtant, nombreux sont les documents de l'institution qui ne sont pas officiels car non classés comme tels. Néanmoins, ces documents doivent aussi être protégés.

Aussi, la présente instruction administrative définit-elle quatre niveaux généraux de protection appliqués aux informations quels que soient leur origine ou leur format. Le niveau de protection attribué dépend de la valeur des informations et du risque potentiel associé à ces informations. Un niveau de protection s'accompagne d'un ensemble de mesures dont le but est de réduire l'éventualité (risque) de voir ces informations compromises. Ces niveaux de protection sont alignés sur les niveaux de confidentialité judiciaire de façon à ce que les membres du personnel comprennent comment traiter des informations une fois que les Chambres leur ont attribué un niveau de confidentialité judiciaire.

Il ne faut pas confondre niveau de protection et accès à l'information, ce dernier point étant subordonné au « besoin d'en connaître ». Les niveaux de protection ne sont qu'une indication du type de protection à appliquer en vue de prévenir un accès non autorisé.

Bien que de nombreuses mesures de contrôle aient déjà été mises en place, la présente instruction administrative n'officialise aucune pratique en vigueur. Dans un premier temps, le degré d'adhésion aux

normes sera peu élevé dans certains segments de la Cour vu qu'aucune règle n'avait été fixée au préalable. Une période de grâce est prévue pendant laquelle la Cour s'efforcera de se mettre à niveau. Les membres du personnel recevront des formations, des modèles, des outils et des listes de documents pré-classifiés. On peut déjà trouver sur le site intranet de l'Unité chargée de la sécurité des informations des diagrammes et des manuels qui répondent aux questions courantes des employés et traduisent la présente instruction administrative en directives pratiques.

De par sa nature, la présente instruction administrative doit être exhaustive et pourrait donc s'avérer difficile à lire. En réalité, la grande majorité du personnel n'est concerné que par une petite partie du texte. Cela dit, l'ensemble de la Cour bénéficierait grandement d'une approche systématique de la sécurité et les membres du personnel pourraient ainsi s'adapter rapidement aux conditions requises, en s'aidant de moyens technologiques qui rendront l'organisation de la sécurité plus transparente et facile à comprendre.

Certaines consignes de la présente instruction administrative peuvent être appliquées à l'aide d'outils automatisés tels que des clés USB sécurisées qui permettent aux employés de transporter des informations en toute sécurité ; des serveurs de journalisation qui enregistrent de manière centralisée les activités des utilisateurs sur le réseau ; des logiciels bloquant les ports de façon à contrôler la copie de documents à partir du réseau et des outils empêchant d'échanger via l'internet des documents sensibles non cryptés. Ces outils laissent une grande liberté à l'utilisateur tout en l'obligeant à rendre compte de ses actes.

La rédaction et la mise au point de la présente instruction administrative ont nécessité de nombreuses consultations ainsi que de longs débats qui n'étaient pas prévus. Dans la mesure jugée raisonnable par le fonctionnaire chargé de la sécurité de l'information, les commentaires et les préoccupations de tous ont été pris en compte dans l'instruction administrative.

À noter que la présente instruction administrative n'est pas un texte figé ; elle sera évaluée régulièrement de façon à ce qu'elle continue d'être adaptée aux besoins et au fonctionnement de la Cour.

PARTIE I – INTRODUCTION

Section 1

Définitions

1.1 Administrateurs – Fonctionnaires de la Cour responsables de la tenue et de la gestion du registre des informations classifiées de la CPI.

1.2 Restriction – Mention indiquant les destinataires visés des informations. Les restrictions doivent être traduites et adaptées aux possibilités et à la configuration des applications de la CPI.

1.3 CEN II – Niveau de protection fixé par la norme internationale (EN 1143-2:2001) relative aux unités de stockage en lieux sûrs - Prescriptions, classification et méthodes de test pour la résistance à l'effraction (les coffres-forts par exemple).

1.4 Classification – Attribution d'un niveau de protection à des informations, conformément à la Partie III de la présente instruction administrative.

1.5 Politique de rétention de la classification – Politique précisant la période par défaut pendant laquelle une classification est maintenue jusqu'à ce que la période de rétention soit écoulée ou que les circonstances qui ont justifié la classification aient changé.

1.6 Informations classifiées – Informations assorties d'un niveau de protection supérieur à « NON CLASSIFIÉ ».

1.7 Compromission – Perte, accès ou usage impropre, et divulgation, altération ou destruction non autorisées d'informations.

1.8 Confidentialité – Assurance que les informations ne seront communiquées qu'à des personnes ou à des organisations autorisées.

1.9 Dossiers de la Cour – Dossiers de la Cour déposés auprès du Greffe ou conservés par celui-ci en tant qu'éléments d'une situation ou d'une affaire.

1.10 DIN 32757-1 – Norme du secteur d'activité relative à la destruction de documents.

1.11 Documents – Informations enregistrées quelles que soient leur forme ou leurs caractéristiques. Terme utilisé de manière interchangeable avec « Archives de la Cour » pour faciliter la lecture.

1.12 Codes d'endossement – Marquages permettant de donner des directives supplémentaires sur la manière dont les informations doivent être traitées (« ne pas copier » ou « ne pas diffuser après », par exemple).

1.13 Chef – Chef ou responsable d'organe, de division, de bureau, de section et le ou la délégué(e) qui lui a été attribué pour une certaine tâche.

1.14 Archives de la Cour – Livres, documents sur papier, photos, documents informatiques, cartes ou autres documents d'information, quelles que soient leur forme ou leurs caractéristiques, qui sont en possession de la Cour et ont une valeur documentaire ou de preuve. Ces documents, créés, reçus ou conservés dans le cadre d'une affaire officielle, sont conservés en raison de leur valeur informative comme preuve de l'organisation, de fonctions, de politiques, de décisions, de procédures, d'opérations ou d'autres activités. Les systèmes informatiques portables autonomes (comme les ordinateurs portables et les assistants numériques personnels ou PDA) qui possèdent une mémoire résidente sont considérés comme des archives de la Cour dans le contexte de la présente instruction administrative.

1.15 Registre des informations classifiées de la CPI - Ce registre est maintenu pour gérer le cycle de vie (création, réception, classification, stockage, récupération, modifications, transfert, scanning, copie, destruction, transmission, reclassification et déclassification) des documents marqués « SECRET [CPI] ».

1.16 Système informatique – Ensemble du matériel, des logiciels, des méthodes et des procédures et, si besoin, du personnel utilisés pour traiter les informations.

1.17 Informations – Documents de la CPI sur quelque support ou sous quelque forme que ce soit.

1.18 Dépositaire des informations – Le dépositaire des informations est le chef de l'unité administrative chargée de fournir un soutien opérationnel aux propriétaires des informations en matière de systèmes informatiques en gérant ou en maintenant le système informatique. Le dépositaire des informations met en œuvre les mesures de protection requises par le propriétaire des informations.

1.19 Propriétaire des informations – Le propriétaire des informations est le chef de l'unité administrative responsable des informations. La propriété n'implique pas de droit de propriété dans le contexte de la sécurité des informations. La propriété peut si besoin être partagée entre plusieurs chefs. Les propriétaires des informations déterminent l'usage, les droits d'accès et les critères de protection concernant les informations placées sous leur responsabilité.

1.20 Fonctionnaire chargé de la sécurité des informations – Fonctionnaire chargé de la sécurité des informations au sein de la Section de la sécurité, laquelle relève du Greffe.

1.21 Système d'information – Ensemble de l'infrastructure, de l'organisation, du personnel et des éléments nécessaires à la collecte, au traitement, au stockage, à la transmission, à la présentation, à la diffusion et à la suppression des informations.

1.22 AND - Accord de non-divulgation.

1.23 Unité administrative – Organe, division, bureau, section ou unité.

1.24 Émetteur – Personne ou unité administrative au sein de la Cour qui a créé l'information ou l'a reçue d'un fournisseur.

1.25 Fournisseur – Personne ou entité, indépendante de la Cour et externe à elle, qui a fourni l'information à cette dernière.

1.26 Impression sécurisée – Caractéristique de l'imprimante assurant que l'impression est uniquement lancée après que l'utilisateur s'est identifié comme étant physiquement près de l'imprimante.

1.27 Mot de passe fort – Mot de passe composé d'au moins 8 caractères, dont un spécial[1] et un caractère numérique.

1.28 Membre du personnel – Aux fins de la présente instruction administrative, l'expression « membre du personnel » désigne tous les fonctionnaires et personnes associées à la Cour ou ayant des rapports contractuels avec elle tels que les responsables élus, les contractants indépendants, le personnel mis à disposition à titre gracieux, les stagiaires, les consultants, les bénévoles, les interprètes et toutes les autres personnes sous contrat jouissant d'un accès autorisé aux informations de la Cour pour accomplir leur tâches officielles

Note : les responsables élus ne sont pas soumis à la procédure disciplinaire habituelle mais doivent respecter les procédures administratives de la Cour.

Section 2

Généralités

2.1 La présente instruction administrative définit les normes minimales applicables pour protéger la confidentialité des informations dans le cadre des activités de la Cour pénale internationale (« la Cour »), classifier les informations de façon à pouvoir les gérer de manière appropriée.

[1] Les caractères suivants sont considérés comme des caractères spéciaux : ~`!@#$%^&*()_-+={}[]\ |:;?><,./

2.2 La présente instruction administrative s'applique aux informations que la Cour utilise dans le cadre de ses activités et aux membres du personnel en activité ou non.

2.3 Elle s'applique aux informations qui sont générées au niveau interne par la Cour ou fournies à cette dernière et non déclarées ou marquées « secret d'État » par le fournisseur.

2.4 La présente instruction administrative ne s'applique pas aux informations qui ont été fournies à la Cour et déclarées ou marquées « secret d'État » par le fournisseur. Celles-ci doivent être traitées conformément à l'Instruction administrative sur les secrets d'État (« Classification des informations et traitement des informations classifiées fournies par les États et les organisations internationales »).

2.5 Lorsque la présente instruction administrative ne peut être intégralement respectée pour des raisons qui échappent au contrôle des membres du personnel, ces derniers prennent toutes les mesures raisonnables pour en respecter l'esprit.

Note : la disposition ci-dessus confère une certaine flexibilité aux membres du personnel qui sont en mission ou en déplacement et tributaires des réalités de leur environnement. Elle tient compte aussi des cas où des mesures n'ont pas encore été mises en place par la Cour. À noter que pour avoir recours à cette disposition, il faut d'abord prouver que la présente instruction administrative n'est pas applicable autrement.

2.6 La fourniture d'informations à la Cour s'accompagne d'assurances crédibles pour le fournisseur que les mesures adéquates seront prises pour éviter la divulgation non autorisée des informations et que toute information, une fois communiquée à la CPI, fera l'objet d'une protection appropriée.

2.7 Chaque unité administrative établit des procédures administratives pour le contrôle des informations dont elle est responsable, en se fondant sur les dispositions de la présente instruction administrative et sur une évaluation des activités menées par l'unité en question et des risques potentiels. Ces procédures administratives servent à éviter la divulgation non autorisée des informations en contrôlant l'accès aux informations et en assurant le respect des exigences relatives au traitement, au marquage, au stockage, à la transmission et à la destruction telles qu'elles sont définies dans la présente instruction administrative.

Note : chaque unité administrative est responsable de la protection des informations qui lui appartiennent dans le cadre de la Cour ou qui sont (provisoirement) en sa possession. La disposition ci-dessus confère une certaine flexibilité aux unités administratives car elle leur permet d'adapter les dispositions de sécurité générales à leur fonctionnement. Il leur appartient d'organiser cette protection, qui peut être différente pour chacune d'entre elles.

PARTIE II – NIVEAUX DE PROTECTION

Section 3

Niveaux de protection

3.1 Les informations se voient attribuer un niveau de protection en fonction de catégories établies qui correspondent à leur niveau de sensibilité.

3.2 Les facteurs suivants doivent être pris en considération conjointement pour déterminer le niveau de sensibilité des informations :

a) la gravité du préjudice que la divulgation pourrait causer à la Cour, au fournisseur ou à d'autres personnes ;

b) les avantages potentiels que la divulgation pourrait représenter pour la Cour, le fournisseur ou d'autres personnes.

3.3 En s'appuyant sur les principes énoncés dans la sous–section 3.2 ci–dessus et sur les critères de classification spécifiques énoncés à la section 5 ci–dessous, les informations doivent être classées selon quatre catégories, par niveau de sensibilité croissant :

a) « NON CLASSIFIÉ » : informations dont la diffusion publique ne porterait pas préjudice à la Cour, celles qui sont autorisées pour la diffusion publique et celles qui peuvent être obtenues auprès de sources publiques ;

Note : dans le cadre de la Cour, autoriser des informations à être diffusées au public est une décision délibérée. Par conséquent, l'absence de marquage ne doit pas faire penser que les informations en question sont non classifiées. Voir aussi la sous-section 5.15.

b) « RESTREINT [CPI] » : informations qui sont réservées à l'usage interne de la Cour ;

c) « CONFIDENTIEL [CPI] » : informations qui doivent être gardées confidentielles vis–à–vis de certaines parties ;

d) « SECRET [CPI] » : informations qui doivent être gardées secrètes par certaines personnes.

Note : les niveaux de protection attribués aux informations secrètes qui ne sont pas des secrets d'État n'ont pas pour but de correspondre ou d'être parallèles à ceux définis pour les secrets d'État ; les niveaux de protection attribués aux secrets d'État sont complètement indépendants de ceux assignés aux informations secrètes qui ne sont pas des secrets d'État.

3.4 Pour les informations fournies à la Cour, le niveau de protection défini par le niveau de protection assigné par le fournisseur est utilisé pour déterminer le niveau de protection correspondant de la Cour.

Section 4

Classification et impératifs d'efficacité

4.1 Les informations doivent se voir affecter le niveau de protection le plus bas possible mais aussi élevé que nécessaire. Une classification trop élevée risque de limiter l'accès, d'entraîner des contrôles superflus et de nuire à l'efficacité des activités de la Cour. À l'inverse, une classification trop faible peut exposer les informations à une compromission, faute de contrôles appropriés.

4.2 Les informations doivent être classées à leur juste niveau, qui n'est pas nécessairement la classification des informations sur lesquelles celles–ci reposent ou auxquelles elles répondent ou se réfèrent.

4.3 Les informations qui nécessitent un niveau de protection élevé seront, si possible, mises en annexe afin que les textes principaux puissent être distribués à un public plus large et assortis de mesures de sécurité moins strictes.

4.4 Les informations sont classées en fonction de leur contenu et des risques liés à la compromission de leur contenu tels qu'ils sont définis à la section 5.

Section 5

Niveaux de protection et critères d'application

5.1 Le niveau de protection attribué à des informations émanant d'un fournisseur est en rapport avec le degré de sensibilité indiqué par le niveau de protection fixé par le fournisseur.

NON CLASSIFIÉ

5.2 La Cour s'efforce de recevoir et de produire des informations pouvant porter la mention « *NON CLASSIFIÉ* » pour optimiser leur utilité dans la perspective de la réalisation des objectifs de la Cour et disposer d'une liberté d'action quant à leur traitement.

5.3 Les informations qui n'entrent dans aucun des niveaux de protection sousmentionnés sont considérées comme non classifiées et portent la mention « *NON CLASSIFIÉ* », à l'exception des informations visées à la sous-section 7.4.

5.4 Le niveau de protection « NON CLASSIFIÉ » est appliqué aux informations classées « PUBLIC »fournies par les parties à la procédure juridique sauf dispositions autres ordonnées par les Chambres.

RESTREINT [CPI]

5.5 Le niveau de protection « RESTREINT [CPI] » est utilisé pour les informations dont on peut raisonnablement penser que leur compromission serait défavorable à la Cour. Une telle compromission pourrait notamment :

a) faciliter l'obtention de gains ou d'avantages injustifiés par des personnes ou des organisations ;

b) entraîner des pertes financières limitées pour la Cour ;

c) désavantager la Cour dans des négociations politiques ou commerciales ; ou

d) nuire à l'image de la Cour et au bon déroulement de ses activités.

5.6 Le niveau de protection « RESTREINT [CPI] » requiert un niveau de protection qui évite raisonnablement la compromission des informations.

5.7 Toute information est classée « RESTREINT [CPI] » par défaut, à moins qu'elle ne réponde aux critères des catégories « CONFIDENTIEL [CPI] », « SECRET [CPI] » ou « NON CLASSIFIÉ ».

Note : le marquage « RESTREINT [CPI] » correspond à la mention « à usage interne uniquement » et est essentiellement utilisé pour les documents ayant trait aux opérations et à l'administration de la Cour ainsi qu'à ses procédures. Il n'a pas d'équivalent dans les Chambres et ne peut donc pas être appliqué aux dossiers de la Cour.

CONFIDENTIEL [CPI]

5.8 Le niveau de protection « CONFIDENTIEL [CPI] » est utilisé pour les informations dont on peut raisonnablement penser que leur compromission porterait préjudice aux intérêts de la Cour. Ce préjudice pourrait notamment prendre la forme :

a) d'une atteinte à l'efficacité, à la réputation, à la stabilité ou à la sécurité de la Cour, des États, des organisations intergouvernementales ou des organisations non gouvernementales ;

b) d'une atteinte à l'appui donné à la Cour dans le cadre d'une affaire, d'une situation ou d'un programme ;

c) de conséquences dommageables pour une enquête ou un procès ; ou

d) de conséquences dommageables au bien-être ou à la liberté des personnes.

5.9 Le niveau de protection « CONFIDENTIEL [CPI] » requiert un niveau de protection qui assure :

a) la prévention d'une compromission occasionnelle et délibérée ; et

b) la détection d'une compromission effective ou d'une tentative de compromission.

5.10 Le niveau de protection « CONFIDENTIEL [CPI] » est appliqué aux informations classées « CONFIDENTIEL » fournies par les parties à la procédure juridique sauf dispositions autres ordonnées par les Chambres.

SECRET [CPI]

5.11 Le niveau de protection « SECRET [CPI] » est utilisé pour les informations dont on peut raisonnablement attendre que leur compromission porterait gravement préjudice aux intérêts de la Cour. Ce préjudice pourrait notamment prendre la forme :

a) d'une atteinte grave à l'efficacité, à la réputation, à la stabilité ou à la sécurité de la Cour, des États, des organisations intergouvernementales ou des organisations non gouvernementales ;

b) de conséquences gravement dommageables pour une enquête ou un procès ; ou

d) d'une menace directe ou indirecte à la vie ou de risque de décès, quel que soit le lien avec la Cour.

5.12 Le niveau de protection « SECRET [CPI] » requiert un niveau de protection qui assure :

a) qu'il n'y aura pas de compromission des informations ; et

b) que toute compromission effective ou tentative de compromission des informations sera détectée et leurs auteurs identifiés.

Note : le niveau de protection attribué vise à éviter tout manquement à la sécurité des informations. Néanmoins, il pourra y avoir (et il y aura toujours) des situations entraînant des manquements. Il conviendra alors de les détecter et de mettre en place des mesures de contrôle permettant de recueillir des traces en vue de l'enquête.

5.13 Le niveau de protection « SECRET [CPI] » est appliqué aux informations classées « SOUS SCELLÉS » fournies par les parties à la procédure juridique sauf dispositions autres ordonnées par les Chambres.

GÉNÉRALITÉS

5.14 Les informations qui ne portent aucun marquage sont traitées comme appartenant à la catégorie « RESTREINT [CPI] » par défaut.

5.15 Les informations fournies par la Cour sont assorties de la mention « RESTREINT [CPI] » à moins ou jusqu'à ce que le fournisseur précise un traitement ou un niveau de sensibilité particulier, ou à moins que les informations soient disponibles dans le domaine public.

5.16 La mention « CPI » dans la nomenclature de ces niveaux sert uniquement à faciliter le traitement des informations classifiées en indiquant clairement que les niveaux sont ceux appliqués par la Cour, afin d'éviter tout conflit ou malentendu avec d'autres systèmes de classification.

5.17 L'omission de la mention « CPI » risque d'entraîner une confusion entre l'usage de « RESTREINT [CPI] », « CONFIDENTIEL [CPI] » et « SECRET [CPI] » comme niveaux de protection et l'utilisation de « restreint », « confidentiel » et « secret » comme adjectifs.

5.18 L'utilisation de la mention « CPI » n'implique pas en soi un degré de diffusion particulier.

Section 6

Restrictions et codes d'endossement

6.1 Les restrictions donnent des directives sur la diffusion des informations en précisant quels en sont les destinataires autorisés.

Note : le principe sous-tendant la protection de la confidentialité est d'exclure les utilisateurs non autorisés. Par conséquent, les informations ne sont classées sensibles que si les utilisateurs autorisés sont indiqués. Dans le cas d'informations numériques, les groupes d'accès et des fonctions dans les applications et les dossiers sur le réseau, par exemple, permettent d'appliquer les restrictions.

6.2 Les codes d'endossement permettent de donner des directives supplémentaires sur la manière dont les informations doivent être traitées.

Note : grâce aux codes d'endossement, il est possible d'inscrire des mentions spécifiques afin de donner des instructions aux membres du personnel sur les conditions particulières de traitement d'une divulgation en suspens, par exemple.

6.3 Les restrictions et les codes d'endossement sont assignés lors de la création des informations ou lors de leur enregistrement.

6.4 Le code d'endossement « *ex parte* » est utilisé en combinaison avec une description des destinataires autorisés.

6.5 Les restrictions peuvent être traduites et adaptées aux possibilités et à la configuration des systèmes informatiques.

Section 7

Marquages

7.1 La Cour utilise le marquage des informations pour indiquer :

a) le niveau de classification de sécurité ;

b) les restrictions ; et

c) les codes d'endossement.

Note : le marquage explicite des documents est une pratique courante de la procédure judiciaire. Il est possible de choisir parmi les quatre niveaux définis dans la présente instruction administrative ou leur équivalent judiciaire (voir 5.4, 5.11 et 5.14).

7.2 Les marquages sont appliqués à toutes les copies des informations assorties d'une classification.

7.3 Les niveaux de protection « CONFIDENTIEL [CPI] » et « SECRET [CPI] » sont utilisés en combinaison avec une restriction spécifiant les destinataires autorisés.

Note : les informations n'ont de la valeur que lorsqu'elles sont accessibles aux personnes qui en ont besoin. Le niveau de protection n'est qu'une indication de l'effort déployé pour éviter de nuire à l'intégrité des informations ; encore faut-il préciser les destinataires autorisés (par exemple, *ex parte* ou « Réservé au Bureau du Procureur »).

7.4 Les informations dont la diffusion publique a été autorisée n'ont pas besoin de porter explicitement la mention « NON CLASSIFIÉ » quand leur format indique clairement leur nature publique.

Section 8

Classification des informations

8.1 Les informations sont classées en fonction des niveaux de protection exposés à la section 5 de la présente instruction administrative.

8.2 Chaque unité administrative peut publier des directives explicatives concernant la classification des informations.

8.3 La classification des informations est déterminée par les autorités suivantes :

a) dans le cas d'informations générées par la Cour, l'émetteur des informations attribue un niveau de protection sous la responsabilité du propriétaire ;

b) dans le cas d'informations émanant d'un fournisseur externe, ce dernier est habilité à désigner leur niveau de protection initial ; ou

c) si un fournisseur communique des informations qui semblent avoir un niveau de protection mais sans indiquer un niveau de sensibilité ou de protection, le chef de l'unité administrative qui reçoit les informations applique un niveau de protection conformément à la section 5 ci–dessus et traite les informations en conséquence.

8.4 Au moment de déterminer le niveau de protection en application de la sous-section 8.3.c, l'émetteur peut au besoin consulter le fonctionnaire chargé de la classification de l'unité administrative responsable des informations à classifier.

8.5 Si le destinataire d'informations classifiées suspecte une classification inadéquate ou un marquage de classification inapproprié, il doit en informer l'émetteur, le fournisseur ou le fonctionnaire chargé de la classification de l'unité administrative responsable des informations. Il peut faire une recommandation quant à la classification ou au marquage qu'il juge approprié.

Section 9

Fonctionnaires chargés de la classification

9.1 Chaque unité administrative désigne un fonctionnaire responsable de la classification chargé de fournir aux utilisateurs des conseils quant à la classification des informations. Ce fonctionnaire peut aussi être affecté à une unité administrative par une unité administrative supérieure.

Note : le fonctionnaire chargé de la classification joue un rôle de conseiller auprès du chef de l'unité administrative en question.

9.2 Le fonctionnaire chargé de la classification dispose à cet effet de directives en matière de classification des types de documents couramment traités au sein de son unité administrative.

9.3 Le fonctionnaire chargé de la classification répond aux demandes de conseils en matière de classification ou peut transmettre ces demandes au fonctionnaire chargé de la sécurité des informations.

9.4 Le fonctionnaire chargé de la classification aide le chef concerné à répondre aux demandes d'information qui n'entrent pas dans le cadre des pratiques standard d'échange d'informations entre l'unité administrative concernée et le demandeur :

a) en effectuant ou en organisant un examen de classification des informations considéré comme répondant à la demande ; et

b) en faisant des recommandations quant à la déclassification ou à l'expurgation des informations avant leur divulgation.

Section 10

Durée de la classification

10.1 Lorsqu'il fournit des informations classifiées, l'émetteur ou le fournisseur peut indiquer la durée de la classification qui s'applique aux informations. Si aucune indication n'est donnée, la durée de la classification est supposée être la même que celle prévue par la politique de rétention de la classification pour le type d'informations fournies. Si aucune politique de rétention de la classification n'est applicable, la rétention de la classification est maintenue jusqu'à ce que les informations soient remplacées ou soient devenues obsolètes.

10.2 Les classifications sont revues une fois la période de rétention écoulée.

10.3 Les classifications sont revues si les circonstances qui les ont justifiées ont changé.

10.4 Les classifications peuvent être périodiquement revues par l'émetteur pour déterminer si elles peuvent être révisées ou si elles peuvent prendre fin.

10.5 La classification des informations ne cesse de s'appliquer que lorsque les informations sont détruites dans leur intégralité et non pas simplement lorsque certains éléments sont détruits.

Section 11

Reclassification

11.1 La reclassification des informations peut être nécessaire lorsque les informations sont modifiées, complétées, remplacées ou révisées, afin de modifier substantiellement leur sensibilité.

11.2 Pour les archives de la Cour, la détermination de la reclassification ne peut être faite que par la chambre compétente.

11.3 En cas de demande de changement du niveau de protection d'informations émanant de la Cour, le fonctionnaire chargé de la classification compétent se prononce sur la demande, en respectant les critères établis pour l'application des niveaux de protection en fonction du besoin opérationnel déclaré.

11.4 La Cour peut demander au fournisseur de modifier la classification des informations fournies. Une telle demande doit reposer sur un besoin opérationnel précis. Avant de confirmer ce changement, la Cour et le fournisseur peuvent procéder à des consultations sur les conséquences du changement proposé.

11.5 Si l'émetteur ou le fournisseur modifie la classification des informations, il en informe tous les destinataires.

Note : la fonction de notification peut être automatiquement intégrée aux procédures par défaut comme c'est le cas, par exemple, pour les décisions des Chambres déposées par les Chambres et les parties aux dossiers de la Cour.

11.6 Si une information classée « SECRET [CPI] » est déclassifiée, le registre des informations classifiées doit être actualisé en conséquence pour faire apparaître la date de la déclassification. La mention dans le registre doit être conservée et les membres du personnel qui possèdent une copie du document doivent être informés de la modification apportée.

11.7 Les informations reclassifiées doivent être marquées de manière visible afin d'attirer l'attention de l'utilisateur qui les traite sur la classification exacte.

Section 12

Périodes de rétention

12.1 Les informations sont conservées pendant la période précisée par le calendrier de rétention de la Cour applicable. Après cette période, ces informations peuvent être archivées suivant les politiques d'archivage applicables, ou détruites.

12.2 Le calendrier de rétention des informations est placé sous la responsabilité du propriétaire des informations.

12.3 La période de rétention par défaut de la Cour est fixée à 10 ans, à moins que les réglementations applicables ne requièrent une période de rétention plus longue ou plus courte.

12.4 Les archives de la Cour sont conservées pour une durée illimitée.

Section 13

Classification des mots de passe, des clés et des systèmes cryptographiques

13.1 Le niveau de protection des mots de passe, des clés et des systèmes cryptographiques doit être identique au niveau le plus élevé des informations protégées par ces mots de passe, clés et systèmes cryptographiques.

PARTIE III – TRAITEMENT DES INFORMATIONS CLASSIFIÉES

Section 14

Dispositions relatives au traitement des informations

14.1 Cette partie de la présente instruction administrative énonce les principes qui régissent l'octroi de l'accès aux informations ainsi que les procédures relatives à leur traitement et à leur diffusion.

14.2 Un niveau de protection ne détermine pas en lui–même l'étendue de l'accès aux informations classifiées mais définit la manière dont elles sont traitées et protégées contre une reproduction ou une diffusion non autorisées.

Section 15

Accès aux informations

15.1 Les personnes qui, du fait de leurs fonctions, ont accès à des informations classifiées doivent être en possession d'une autorisation personnelle d'accès délivrée par l'unité des enquêtes et habilitations de sécurité de la Section de la sécurité de la CPI, ou d'une autorisation externe reconnue par la Cour.

Note : les contractants, les stagiaires, les professionnels invités peuvent avoir besoin d'accéder (ou accèdent déjà) aux informations les plus sensibles comme l'identité des témoins. En conséquence, la Cour a l'obligation de veiller à l'honnêteté des personnes à qui ces informations sensibles sont confiées. C'est pour cela que la Cour a mis en place une procédure d'habilitation mise à exécution par l'Unité des enquêtes et habilitations de sécurité de la Section de la sécurité. Cette procédure est différente des procédures d'habilitation de sécurité menées par les agences de sécurité nationales et équivaut aux types d'habilitation reconnus par les États et l'Union européenne.

Note : la procédure d'habilitation de sécurité permet à la Section de la sécurité de se faire une opinion. Il n'y a pas plusieurs niveaux d'habilitation. La Cour n'en a pas les moyens et ces niveaux ne correspondraient pas aux types d'informations en circulation dans l'institution. Par exemple, de nombreux employés ont accès à des documents classés « Sous scellés » dans le cadre de leurs fonctions à la Cour et une méthode unique visant le niveau le plus élevé de garantie (sous scellés / secret) est donc la plus appropriée.

Note : la procédure d'habilitation de sécurité repose sur plusieurs sources d'information. L'AIVD (renseignements généraux des Pays-Bas) ne figure plus sur la liste des sources potentielles mais un autre organe est en cours d'identification. D'autres sources demeurent pertinentes.

15.2 Les personnes qui ont accès à des informations classifiées signent un accord de non–divulgation à leur entrée en fonction. Les obligations découlant de l'accord de non-divulgation ne prennent pas fin avec la cessation de service.

Note : la Section des ressources humaines gère les accords de non-divulgation du personnel. La Section de la sécurité s'occupe des instructions relatives aux sociétés d'entretien. La Section des achats prépare des dispositions du type accord de non-divulgation pour les contractants.

15.3 Chaque unité administrative peut mettre en œuvre des accords de non-divulgation supplémentaires conformes à la présente instruction administrative afin de mieux réglementer l'accès pour certaines tâches ou à des fins particulières.

15.4 La Section de la sécurité fournit des instructions sur le traitement des informations aux personnes ayant accès à des informations classées « RESTREINT [CPI] » ou à un niveau supérieur, à leur arrivée à la Cour puis à intervalles réguliers.

15.5 Les chefs veillent à informer les personnes ayant accès à des informations classées « RESTREINT [CPI] » ou à un niveau supérieur, à leur arrivée à la Cour puis à intervalles réguliers, sur le traitement de ces informations lorsque ce traitement est spécifique à leur unité administrative.

Section 16

Principes de diffusion

16.1 La diffusion des informations est régie par les principes suivants :

a) l'accès aux informations est réglementé en fonction de leur niveau de protection ; et

b) la diffusion d'informations ne vise que les personnes qui ont effectivement besoin d'y avoir accès. La fonction ou les tâches spécifiques d'une personne sont le critère principal qui détermine si elle est habilitée à avoir accès aux informations, et l'étendue de l'accès aux informations qui en découle.

16.2 Les membres du personnel n'évoquent des informations classifiées ni ne les divulguent à aucune personne hormis celles qui ont reçu l'accès à ces informations par le chef qui en est responsable, auquel cas ces conversations ou cette divulgation portent uniquement sur les informations qu'il est raisonnablement nécessaire d'évoquer ou de révéler pour répondre aux fins pour lesquelles l'accès a été accordé.

Section 17

Communication d'informations à des parties externes

Note : la communication d'informations à des tierces parties a été partiellement réglementée et est conforme à la règle 101-7-b du Règlement et Statut du personnel. La présente section porte sur les conditions de divulgation des informations classifiées.

17.1 La Cour peut communiquer des informations classifiées à des parties externes dans les conditions suivantes :

a) les informations conservent leur niveau de protection ;

b) la Cour conserve le pouvoir discrétionnaire quant à l'utilisation des informations classifiées ;

c) la partie externe s'engage à protéger et à sauvegarder les informations conformément à ses propres règles de sécurité applicables aux informations assorties d'un niveau de sécurité équivalent ; et

d) les informations ne sont pas utilisées à des fins autres que celles autorisées par la Cour.

17.2 La Cour veille tout particulièrement à ce que les parties externes respectent leur propre réglementation en matière de sécurité.

17.3 La diffusion d'informations ayant un impact sur la vie privée des membres du personnel doit être autorisée par le chef de la Section des ressources humaines, en plus du chef de l'unité administrative concernée. Dans un tel cas, le chef de la Section des ressources humaines veille à ce que l'échange d'information se fasse dans le respect des conditions suivantes :

Note : l'autorisation est implicite quand l'échange se fait à l'initiative de la Section des ressources humaines compte tenu de ses obligations en matière de gestion du personnel.

a) les informations sont traitées de manière équitable et conforme au droit ;

b) les informations sont traitées à des fins limitées et convenues ;

c) les informations fournies sont adéquates, pertinentes et ne sont pas excessives ;

d) les informations sont exactes ;

e) les informations ne sont pas détenues plus longtemps qu'il n'est nécessaire ; et

f) les informations sont transférées à des parties dotées d'une législation satisfaisante en matière de protection des données.

Note : la disposition susmentionnée est conforme aux principes de protection des données établis par l'Organisation internationale du Travail.

17.4 La divulgation d'informations privées concernant des fonctionnaires qui ne relève pas des obligations de la Cour en matière d'opérations, de préservation et de gestion de son personnel, requiert l'approbation du fonctionnaire en question, ou de l'Organe représentatif du personnel quand un nombre élevé de fonctionnaires est concerné.

Note : la présente disposition a pour but de protéger la vie privée des personnes mais aussi d'éviter d'ériger, au nom de la protection des données, des obstacles injustifiés aux relations économiques et au flux transfrontière des données. Seules les informations sortant du cadre administratif de la Cour (par exemple, les opinions personnelles des fonctionnaires recueillies au cours d'enquêtes ou les informations générales requises pour l'habilitation de sécurité) doivent faire l'objet d'une autorisation. À noter que la présente disposition est déjà largement appliquée.

Section 18

Traductions et transcriptions

18.1 Les informations peuvent être traduites ou transcrites, à condition que la traduction ou la transcription conserve le niveau de protection, les marquages et les codes d'endossement des informations d'origine et soit traitée en conséquence.

Section 19

Systèmes informatiques

Note : parce qu'elle dépend totalement des systèmes informatiques, la Cour a fait de la sécurité des informations son cheval de bataille. La présente section vise à garantir que la sécurité des informations soit prise en compte durant tout le cycle de vie d'un système. Elle établit aussi les responsabilités globales entre les personnes chargées de l'information et celles qui fournissent les services nécessaires pour utiliser et protéger cette information.

Note : des exigences plus détaillées pour chaque système informatique (TRIM, RingTail) seront établies à un niveau inférieur, par exemple, au niveau des accords de prestation de services. Ces derniers devront contenir des dispositions précisant les différentes responsabilités. Le projet d'instruction administrative sur les contrôles d'accès fixe les conditions relatives au contrôle et à la responsabilité de l'accès en matière de sécurité des informations.

19.1 La Cour peut utiliser des systèmes informatiques pour le stockage, le traitement et la transmission de ses informations.

19.2 La protection des informations est envisagée, maintenue et fait l'objet d'un suivi tout au long du cycle de vie d'un système informatique.

19.3 On identifie les stades suivants du cycle de vie d'un système informatique : planification, développement et achat, mise en œuvre, fonctionnement, mise à niveau, retrait du service et élimination du matériel.

Note : la sécurité fait partie intégrante de tout système informatique et doit être intégrée à sa conception.

19.4 Le propriétaire des informations responsable des informations traitées par un système informatique veille à ce que ses exigences en matière de sécurité des informations soient définies et portées à la connaissance du dépositaire des informations. Ces exigences peuvent limiter le nombre de solutions applicables et avoir une incidence sur le développement, le fonctionnement et la maintenance des systèmes informatiques, ainsi que sur les besoins en personnel et les coûts.

Note : la Section des technologies de l'information et des communications attribue un niveau global de sécurité aux applications qu'elle administre pour le compte de la Cour. Au cas où des applications nécessiteraient un type différent d'administration (une plus grande accessibilité que celle normalement autorisée, par exemple), cette section doit en être informée.

19.5 Le propriétaire des informations responsable des informations traitées par un système informatique veille à ce que des ressources suffisantes soient disponibles et allouées au dépositaire des informations pour les aspects touchant à la sécurité du système, aux stades appropriés.

19.6 Les exigences en matière de sécurité des informations peuvent avoir une incidence sur le développement, le fonctionnement et la maintenance des systèmes informatiques, ainsi que sur les besoins en personnel et les coûts.

19.7 Les exigences de sécurité des systèmes informatiques prennent en compte le fait que :

a) toute information peut être exposée à un accès par des fonctionnaires ou d'autres personnes non autorisés, à un refus d'accès à des fonctionnaires autorisés, ainsi qu'à une altération, à des modifications non autorisées et à une suppression non autorisée ;

b) le système informatique est généralement complexe, fragile, coûteux et souvent difficile à réparer ou à remplacer rapidement ; et

c) les personnes qui ont accès aux systèmes informatiques n'ont pas toutes besoin de connaître toutes les informations qui sont stockées, traitées ou transmises dans les systèmes informatiques.

Note : ce qui précède n'est pas spécifique à la Cour, il s'agit de mesures de précaution visant à garantir que les risques découlant de la dépendance de la Cour envers les systèmes informatiques soient pris en compte en toutes circonstances.

19.8 Une méthode officielle est utilisée comme schéma directeur permettant d'identifier les points faibles, les risques et les exigences de sécurité des informations.

19.9 La norme ISO/CEI17799 (« Code de pratique pour la gestion de sécurité d'information ») sert de schéma directeur pour le choix de critères en matière de sécurité des informations et les mécanismes de contrôles correspondant (CPI/DP/2005/001, par. 3.9).

Section 20

Système de couleurs

20.1 Lorsque des couleurs sont utilisées pour signaler des niveaux de protection, le système employé doit éviter toute confusion possible avec le système de couleurs existant pour les informations fournies en tant que secrets d'État définies à la sous-section 15.1 de l'instruction administrative intitulée « Politique de protection des informations de la CPI pour les informations classifiées fournies par les organisations gouvernementales et intergouvernementales ».

Ladite sous-section est libellée ainsi :

15.1 Pour signaler les classifications de sécurité par des couleurs, le système suivant est employé :

a) TRÈS SECRET [IPASS] – violet ;

b) SECRET [IPASS] – rouge ;

c) CONFIDENTIEL [IPASS] - jaune

Note : aucun système de couleur n'est prévu pour le type d'informations visées dans la présente instruction administrative. Les unités administratives sont libres d'établir des codes de couleur, fournir des pochettes et des autocollants en couleur pour les documents et veiller à ce qu'ils soient bien utilisés. Toutefois, si cette procédure se révèle utile, elle pourra être adoptée ultérieurement.

Section 21

Système d'abréviations

21.1 Lorsque des abréviations sont utilisées pour identifier des niveaux de protection, le système suivant est appliqué :

a) « IS » est l'abréviation utilisée pour « SECRET [CPI] » ;

b) « US » est l'abréviation utilisée pour « SOUS SCELLÉS » ;

c) « IC » est l'abréviation utilisée pour « CONFIDENTIEL [CPI] » ;

d) « IR » est l'abréviation utilisée pour « RESTREINT [CPI] » ;

e) « UC » est l'abréviation utilisée pour « NON CLASSIFIÉ » ;

f) « PB » est l'abréviation utilisée pour « PUBLIC ».

Section 22

Marquage extérieur

22.1 Les informations portent un marquage indiquant leur niveau de protection.

22.2 Les documents portent un marquage indiquant leur niveau de protection (par tampon, impression ou fixé de manière permanente par une étiquette, une bande adhésive ou un cachet) au centre de leur première et de leur quatrième de couverture.

22.3 Si le marquage n'est pas possible, les documents doivent être accompagnés d'une lettre indiquant leur niveau de protection.

22.4 Les marquages peuvent être éventuellement aussi appliqués aux enveloppes, chemises, boîtes ou tout autre moyen utilisé pour transporter, contenir ou conserver des documents.

22.5 Les restrictions sont mentionnées dans leur intégralité sur la première de couverture des documents.

22.6 Les codes d'endossement figurent dans leur intégralité sur la première de couverture des documents.

22.7 Les marquages sont suffisamment visibles pour attirer l'attention de la personne qui traite les documents sur le fait que ceux–ci sont classifiés.

22.8 Les fonctionnaires qui créent, traitent ou diffusent de manière électronique des informations classifiées doivent en indiquer le niveau de protection sous forme électronique afin que l'état de classification des objets électroniques, courriers électroniques, documents, bases de données et pièces telles que les photos et les films puisse être établi sans ouvrir l'objet.

Note : le marquage des informations numériques peut se faire par les métadonnées (les champs de métadonnées dans des applications comme CMS ou TRIM, par exemple).

Section 23

Marquage intérieur

23.1. Pour les informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur, la page intérieure de chaque document doit porter la marque du niveau de protection en haut ou en bas du document. En cas d'impression recto verso, la marque figure sur les deux pages.

23.2 Il n'est pas nécessaire de faire figurer les restrictions et les codes d'endossement à l'intérieur des documents.

23.3 Les marquages doivent être suffisamment visibles pour attirer l'attention du fonctionnaire qui traite les informations sur le fait que celles–ci sont classifiées.

Note : les marquages doivent faire partie des modèles de la Cour mis à la disposition des membres du personnel. Ces modèles ont pour but de préserver le style propre à la Cour tout en facilitant un marquage systématique.

Section 24

Gestion des informations classées « SECRET [CPI] »

24.1 Les informations classées « SECRET [CPI] » sont consignées, affectées d'un numéro de série individuel et entrées dans le registre des informations classifiées de la CPI.

Note : la disposition ci-dessus est en application de la norme 16 du Règlement du Greffe.

24.2 Une mention dans le registre des informations classifiées identifie le document et comporte au minimum (si l'information existe) la date à laquelle le document a été créé ou reçu, son numéro de série individuel, le nombre d'exemplaires, le titre, l'émetteur, l'action effectuée (p. ex. création, modification, transfert, destruction, transmission, attribution d'un niveau de classification inférieur ou reclassification) et la date à laquelle chaque action a été effectuée, ainsi que la personne qui a ordonné ou autorisé l'action.

Note : la disposition ci-dessus est essentiellement appliquée par les fonctions de connexion et de contrôle d'entrée d'applications telles que TRIM et CMS, et du réseau de la Cour.

24.3 Lorsqu'ils traitent des informations classées « SECRET [CPI] », les membres du personnel doivent faire consigner dans le registre des informations classifiées toute action à laquelle il est fait référence dans la sous–section 24.2.

24.4 Les informations auxquelles se rapportent les mentions dans le registre des informations classifiées font l'objet d'une inspection physique ou d'une justification par un administrateur au moins une fois par an, et plus souvent si les circonstances l'exigent.

Section 25

Impression, copie et télécopie

25.1 Les membres du personnel peuvent imprimer, copier ou télécopier les informations classifiées pour un usage officiel.

25.2 Lors de l'impression, de la photocopie ou de la télécopie d'informations classifiées, le nombre de reproductions est minimal et en rapport avec le degré d'accès autorisé.

25.3 Toute impression d'informations classées « SECRET [CPI] » doit faire apparaître l'identité du membre du personnel, de l'imprimante et l'heure de l'impression.

25.4 Les documents classés « SECRET [CPI] » portent un numéro de copie unique sur chaque page, et le nombre total des copies ainsi que le nom du membre du personnel faisant la copie sur la couverture.

25.5 Les informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur doivent être imprimées au moyen d'une imprimante répondant aux conditions suivantes :

a) l'imprimante est à proximité directe ou à portée de vue de la personne qui l'utilise ;

b) l'imprimante est à la seule disposition de l'utilisateur de l'imprimante ; et

c) l'imprimante permet d'effectuer des impressions sécurisées.

25.6 Toute reproduction d'un document a le même niveau de protection que les informations à partir desquelles la reproduction a été faite.

25.7 Les imprimantes, photocopieuses et télécopieuses doivent être placées dans des lieux qui permettent d'assurer le niveau de protection le plus élevé des informations classifiées traitées.

25.8 Les imprimantes, photocopieuses et télécopieuses ne doivent pas être placées dans des lieux ouverts aux visiteurs, dans des lieux qui favorisent les contacts sociaux, dans des lieux placés hors du champ de vision des utilisateurs principaux ou dans des lieux où l'installation d'une imprimante est incompatible avec les règles de sécurité et de santé.

25.9 Les membres du personnel ne doivent pas laisser les impressions, les copies ou les télécopies (ou les originaux) traîner sans surveillance sur les machines en question.

Section 26

Déchiqueteuses

26.1 Tout lieu contenant une imprimante, un télécopieur, une photocopieuse ou un scanner communs et qui n'est pas une salle réservée à du personnel spécialisé doit être équipé d'une déchiqueteuse de documents ou d'une corbeille à papier fournies par la Section des services généraux.

26.2 Les membres du personnel peuvent utiliser les déchiqueteuses pour détruire les informations.

26.3 Les informations classées « CONFIDENTIEL [CPI] » qui sont détruites doivent l'être par une déchiqueteuse conforme au niveau standard 3 ou plus de la norme DIN 32757–1.

Note : les membres du personnel ne sont pas tenus de connaître les normes DIN. Toutefois, il est important de les établir de façon à acheter les fournitures et le matériel de bureau adaptés.

26.4 Les informations classées « SECRET [CPI] » qui sont détruites doivent l'être par une déchiqueteuse conforme au niveau standard 4 ou plus de la norme DIN 32757–1.

26.5 Les déchiqueteuses doivent porter un marquage indiquant le niveau de protection le plus élevé des documents qu'elles peuvent détruire.

26.6 En lieu et place du déchiquetage, les corbeilles à papier fournies par la Section des services généraux peuvent être utilisées pour tous les documents.

Note : le contenu des corbeilles à papier bleues est détruit et déchiqueté suivant une procédure contrôlée.

Section 27

Stockage des informations sur les systèmes informatiques, les systèmes mobiles et les supports de stockage portables

27.1 Les informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur peuvent être stockées, traitées et transmises par ordinateur portable à condition que les informations contenues dans ces ordinateurs portables soient cryptées et uniquement accessibles au moyen d'un jeton et d'un mot de passe ou d'une fonction équivalente.

27.2 Les informations classées jusqu'à « CONFIDENTIEL [CPI] » peuvent être stockées, traitées et transmises par assistant numérique personnel (PDA) à condition que les informations contenues dans ces PDA soient cryptées et uniquement accessibles au moyen d'un mot de passe ou d'une fonction équivalente.

27.3 Les informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur peuvent être stockées sur des clés USB sécurisées fournies par la Cour. Les informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur peuvent être stockées sur d'autres supports portables tels que les disquettes, les DVD et les CD à condition que les informations contenues sur ces supports soient cryptées et uniquement accessibles au moyen d'un mot de passe fort ou d'une fonction équivalente.

27.4 Si les informations classées « CONFIDENTIEL [CPI] » ou à niveau supérieur sont stockées sur des supports portables qui ne répondent pas aux conditions énoncées dans la sous–section 27.3, les supports de stockage portables doivent être considérés comme équivalant aux versions papier des informations qu'ils contiennent, recevoir la classification la plus élevée des informations stockées et être protégés en conséquence.

27.5 Les dossiers sur le réseau ne doivent être utilisés pour stocker les informations que si les applications de la Cour telles que TRIM, CaseMap, RingTail, CMS et SAP n'ont pas la fonction requise.

Note : la disposition ci-dessus tient compte des capacités limitées des dossiers sur le réseau pour la prise en charge des exigences de responsabilité de la Cour et favorise l'utilisation de TRIM, CMS, etc. Toutefois, on est parfois obligé d'avoir recours aux dossiers sur le réseau, les applications ne pouvant pas répondre à tous les besoins. Cette question devra être prise en compte et sera à l'ordre du jour lors de l'évaluation périodique de la présente instruction administrative.

27.6 Les documents contenant des informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur doivent être stockés sous un nom qui ne révèle pas de détails sensibles sur leur contenu.

27.7 Les documents contenant des informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur ne doivent pas être stockés sur les ordinateurs locaux des bureaux extérieurs à condition que ces informations soient cryptées et uniquement accessibles au moyen d'un mot de passe fort ou d'une fonction équivalente. Ces documents peuvent être stockés sur les systèmes informatiques centraux au siège de la Cour.

Note : l'expérience a montré que les bureaux extérieurs doivent parfois être évacués d'urgence et que les ordinateurs et les supports personnels contrôlés à la douane. Par conséquent, il est important que les utilisateurs à distance puissent bénéficier pleinement des applications de la Cour tout en veillant à ce que les informations — bien qu'accessibles à distance — demeurent autant que possible dans les systèmes informatiques centraux de la Cour.

Note : les dispositions ci-dessus sont mises en œuvre au moyen de l'utilisation de « Citrix », outil d'accès à distance qui permet à des personnes externes d'avoir accès au réseau de la Cour et à ses applications.

27.8 Les documents contenant des informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur ne doivent pas être stockés sur les ordinateurs locaux des bureaux extérieurs. Ces documents peuvent être stockés sur les systèmes informatiques centraux au siège de la Cour.

Note : les dispositions ci-dessus sont mises en œuvre au moyen de l'utilisation de « Citrix », outil d'accès à distance qui permet à des personnes externes d'avoir accès au réseau de la Cour et à ses applications.

27.9 Les documents contenant des informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur ne doivent pas être stockés sur des ordinateurs non contrôlés par la Cour.

Section 28

Transmission électronique

28.1 Les informations classifiées peuvent être transmises par le biais du réseau de la Cour. Ce réseau comprend le système de courrier électronique de la CPI, qui permet un accès à distance aux utilisateurs.

28.2 Les documents classés « SECRET [CPI] » ne peuvent circuler (sous réserve des dispositions de la section 24) en dehors du réseau de la Cour que si les informations sont cryptées de manière indépendante au moyen d'un certificat numérique.

28.3 Les documents classés « CONFIDENTIEL [CPI] » ne peuvent être transmis en dehors du réseau de la Cour que si les informations sont cryptées de manière indépendante au moyen d'un certificat numérique ou sont protégées par un mot de passe fort.

28.4 Les documents sont diffusés autant que possible par l'envoi d'une référence (lien) permettant d'y accéder plutôt que par l'envoi des documents eux-mêmes.

Note : l'envoi de documents favorise la prolifération et fragilise le contrôle car le nombre d'exemplaires disponibles en est multiplié. En outre, le document attaché à un courriel ne passe pas par le filtre des fonctions de contrôle présentes dans TRIM, CMS, etc. Par ailleurs, il est possible de faire suivre un courriel automatiquement, de partager des boîtes aux lettres avec des membres du personnel inconnus de l'expéditeur, et de mal orthographier les adresses des courriels. Par conséquent, autant que possible, il est prudent d'envoyer des références (liens) vers les documents plutôt que les documents eux-mêmes, surtout pour les informations classifiées.

28.5 Pour les documents classés « SECRET [CPI] », la réception de la transmission doit être consignée par l'expéditeur et confirmée par le destinataire.

Note : dans la plupart des cas, le système utilisé consigne automatiquement la transmission et la réception.

28.6 Le niveau de protection des documents doit accompagner les documents.

28.7 Les documents qui doivent être échangés par voie électronique doivent être dépouillés des métadonnées révélant des discussions et des opérations internes ou des noms, sauf si le destinataire en a besoin.

Note : pour les documents transmis en dehors du réseau de la Cour, il est impératif que les métadonnées soient supprimées étant donné qu'elles peuvent révéler des discussions internes et des expurgations. Cette opération se fera automatiquement.

Section 29

Télécopieurs et télécopies

29.1 Les documents classés « SECRET [CPI] » ne peuvent être envoyés hors des locaux de la Cour qu'au moyen de télécopieurs cryptographiques.

29.2 Les télécopieurs doivent être physiquement protégés pour que seuls les utilisateurs autorisés puissent y avoir accès.

29.3 Pour les documents classés « CONFIDENTIEL [CPI] » ou à un niveau supérieur, la réception des télécopies entrantes et sortantes doit être consignée.

29.4 Une télécopie doit avoir le même niveau de protection que le ou les documents à partir desquels elle a été faite.

Section 30

Transport des documents à l'intérieur des locaux de la Cour

30.1 Les documents classés « CONFIDENTIEL [CPI] » ou à un niveau supérieur qui sont déplacés au sein même des locaux de la Cour (y compris dans tout bureau extérieur) doivent être protégés par une couverture afin que leur contenu ne soit pas visible.

30.2 Les documents classés « CONFIDENTIEL [CPI] » ou à un niveau supérieur qui sont retirés du lieu où ils sont stockés en sécurité doivent rester en tout temps sous la surveillance d'un membre du personnel.

Section 31

Transport des documents à l'extérieur des locaux et entre les locaux de la Cour

31.1 Les informations peuvent sortir des locaux de la Cour lorsque l'on peut raisonnablement s'attendre à ce que le document soit protégé conformément aux dispositions de la présente instruction administrative ou de manière équivalente.

31.2 Les informations classées « RESTREINT [CPI] » ou à un niveau supérieur ne peuvent sortir des locaux de la Cour que lorsque leur transport est nécessaire à la conduite des activités officielles.

31.3 Les informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur sont sous la surveillance constante d'un membre du personnel et sont conservées dans une chemise.

31.4 Les documents classés « CONFIDENTIEL [CPI] » ou à un niveau supérieur ne doivent pas être lus et/ou évoqués dans des lieux publics, où ils risquent de faire l'objet d'un accès non autorisé puisque des personnes peuvent voir leur contenu ou en entendre parler.

31.5 Des reçus doivent être utilisés pour le transport d'informations classées « SECRET [CPI] » hors des locaux de la Cour (y compris dans tout bureau extérieur).

31.6 Les informations classifiées ne doivent être transportées qu'au moyen :

a) d'un service postal national pour les informations classées jusqu'à « RESTREINT [CPI] » inclus ;

b) d'un courrier recommandé via un service postal national pour les informations classées jusqu'à « CONFIDENTIEL [CPI] » inclus ;

c) de la valise diplomatique pour les informations classées jusqu'à « SECRET [CPI] » inclus ;

d) de membres du personnel désignés pour les informations classées jusqu'à « CONFIDENTIEL [CPI] » inclus si ces documents sont ouverts à l'inspection de la douane ou des autorités locales ; ou

e) de membres du personnel désignés pour les informations classées jusqu'à « SECRET [CPI] » inclus si ces documents sont ouverts à l'inspection de la douane ou des autorités locales.

Note : les sous-sections 31.6.d et 31.6.e. prennent en compte le risque inhérent au transport de documents passant la douane par exemple, ou le risque d'ingérence que présenteraient d'autres autorités locales habilitées à contrôler les documents transportés par des membres du personnel. La sécurité de l'information pourrait en être compromise tout comme la filière de conservation et de transmission. Le stockage électronique de ces informations sur des clés USB sécurisées ou dans un ordinateur portable crypté permet de réduire suffisamment le risque. Autrement, la valise diplomatique est la meilleure solution pour les informations ou pièces sensibles (si possible).

31.7 Les conditions suivantes s'appliquent au transport par messager des documents classifiés :

a) les documents classifiés doivent rester en possession du messager sauf s'ils sont stockés dans un endroit sûr, correspondant à leur niveau de classification ;

b) les documents classifiés ne doivent pas être laissés seuls et ne doivent pas être ouverts en route ; et

c) pour les documents classifiés « SECRET [CPI] », les messagers doivent être informés de leurs responsabilités en matière de sécurité et doivent recevoir une autorisation écrite officielle pour les documents qu'ils transportent (voir annexe B).

31.8 Les clés cryptographiques, mots de passe et jetons d'accès doivent être transportés séparément des informations auxquelles ils donnent accès.

Section 32

Conditionnement

32.1 Les documents classés « CONFIDENTIEL [CPI] » ou à un niveau supérieur transmis hors des locaux de la Cour doivent être emballés comme suit pour éviter leur divulgation non autorisée :

a) les informations doivent être enfermées dans deux enveloppes solides et opaques. L'enveloppe extérieure peut être constituée d'une sacoche fermée à clé, d'une boîte fermée à clé ou d'une valise diplomatique scellée ;

b) l'enveloppe intérieure doit être sécurisée, porter mention de la classification ainsi que d'autres marquages et avertissements prescrits, et mentionner la désignation et l'adresse complètes du destinataire ;

c) l'enveloppe extérieure doit porter la désignation et l'adresse du destinataire et un numéro d'emballage à des fins d'accusé de réception ;

d) l'enveloppe extérieure ne doit pas indiquer la classification du contenu ni mentionner qu'elle contient des documents classifiés ; et

e) si elle est transmise par messager, l'enveloppe extérieure doit porter clairement le code d'endossement « Par messager ».

32.2 Les documents classés « RESTREINT [CPI] » doivent au moins être transmis dans une enveloppe ou un emballage opaque simple.

Section 33

Destruction de documents

33.1 Les documents peuvent être détruits après expiration de la période de rétention qui leur a été assignée.

33.2 Les documents peuvent être détruits avant l'expiration de la période de rétention qui leur a été assignée à condition que propriétaire responsable des informations donne son accord.

33.3 Si aucune période de rétention n'a été assignée à un document ou à un type de document, ces documents ne peuvent être détruits qu'après autorisation du propriétaire responsable des informations.

33.4 Les documents marqués « CONFIDENTIEL [CPI] » ou à un niveau supérieur, y compris tous les produits annexes résultant de leur préparation comme les exemplaires abîmés, les projets de travail et les notes doivent être détruits par brûlage, broyage ou déchiquetage, ou réduits par d'autres moyens sous une forme qui ne peut être reconstituée.

Section 34

Destruction et réparation de mémoires et de supports de stockage

34.1 Tout appareil (p. ex. télécopieur, imprimante, photocopieuse, scanner, assistant numérique personnel et ordinateur portable) ou support à mémoire ou à capacité de stockage numérique (p. ex. clés USB, cartes mémoires, disquettes, DVD et CD) utilisé pour les informations classées « SECRET [CPI] » doit être nettoyé de toute information classifiée avant d'être remis à une tierce partie pour réparation, entretien ou destruction.

34.2 L'entretien et la réparation doivent si possible se faire sur place.

34.3 Les appareils utilisés pour les informations classées « SECRET [CPI] » doivent être provisoirement éteints lors de leur entretien.

Note : la mise hors tension des appareils permet d'effacer leur mémoire interne. Les données stockées sur des disques durs internes et autres types de mémoire permanente n'en sont pas affectées.

34.4 Les appareils utilisés pour les informations classées « SECRET [CPI] » qui contiennent des mémoires de données doivent avoir été configurés pour écraser les informations stockées ; à défaut, la mémoire doit être retirée manuellement.

Section 35

Sécurité physique des documents

35.1 Les documents classés « CONFIDENTIEL [CPI] » ou à un niveau supérieur ne doivent être retirés du lieu où ils sont rangés que pour être activement utilisés.

35.2 Lorsqu'ils ne sont pas utilisés, les documents classés « RESTREINT [CPI] » doivent être rangés.

35.3 Lorsqu'ils ne sont pas utilisés, les documents classés « CONFIDENTIEL [CPI] » ou à un niveau supérieur doivent être mis sous clé.

35.4 Le membre du personnel applique une politique consistant à :

a) fermer son bureau à clé pendant la journée et à la fin de chaque journée de travail ; ou

b) ne laisser aucun document en évidence sur son bureau à la fin de chaque journée de travail.

Note : les bureaux fermés à clés sont néanmoins accessibles aux collègues, aux membres du personnel et aux contractants dont l'accès est justifié.

Section 36

Exigences en matière de coffres–forts et de chambres fortes

36.1 Les versions papier d'informations classées « SECRET [CPI] » ne peuvent être stockées hors les locaux de la Cour que dans des coffres–forts ou des chambres fortes. Ces coffres–forts et chambres fortes doivent respecter la norme CEN II ou être certifiés au titre de cette norme.

Note : les membres du personnel ne sont pas tenus de connaître les normes CEN. Toutefois, il est important de les établir de façon à acheter les fournitures et le matériel de bureau adaptés.

36.2 Les versions papier d'informations classées « SECRET [CPI] » ne peuvent être stockées dans les locaux de la Cour disposant d'une sécurité physique limitée que dans des coffres–forts ou des chambres

fortes. Ces coffres–forts et chambres fortes doivent respecter la norme CEN II ou être certifiés au titre de cette norme.

Note : la présente disposition concerne les bureaux extérieurs, les parkings et les bureaux provisoires qui n'offrent pas le même niveau de sécurité interne que le bâtiment de l'Arc.

Section 37

Protection physique par des espaces, des salles et des chambres fortes

37.1 Tous les locaux, espaces, bâtiments, bureaux, salles, systèmes de communication et d'information dans lesquels les informations sont stockées et/ou traitées doivent être protégés par des mesures de sécurité physique appropriées. Les informations doivent être conservées dans des zones sécurisées en fonction de leur classification.

37.2 Des contrôles de sécurité sont effectués en fin de journée par la Section de la sécurité pour s'assurer que tous les espaces dans lesquels sont traités ou conservés des documents classés « CONFIDENTIEL [CPI] » ou à un niveau supérieur, ou les espaces qui pourraient être utilisés pour traiter ou conserver de tels documents sont dûment sécurisés.

37.3 Les documents classés « RESTREINT [CPI] » ou à un niveau supérieur sont traités et stockés dans des espaces dont :

a) l'accès général est contrôlé par un laisser–passer ou un système de reconnaissance personnelle.

37.4 Les informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur sont traitées et stockées dans des espaces où, en plus des dispositions de la sous-section 37.3 :

a) les informations, lorsqu'elles quittent leur lieu de stockage sécurisé, restent sous la surveillance constante d'une personne autorisée ou sont conservées dans une chemise ;

b) les visiteurs sont escortés ;

c) l'accès est contrôlé par des clés enregistrées ;

d) les clés non utilisées sont gérées et contrôlées.

37.5 Les informations classées « SECRET [CPI] » sont traitées et stockées dans des espaces qui répondent aux conditions suivantes, en plus des dispositions de la sous-section 37.4 :

a) l'entrée et la sortie de l'espace se fait par un déverrouillage et un verrouillage électroniques spécifiques à l'espace concerné ;

b) les murs, portes, fenêtres, planchers et plafonds périphériques, y compris toutes les ouvertures, sont suffisamment insonorisés pour que les conversations ne puissent être entendues par inadvertance ;

c) il existe une seule porte d'entrée principale. Les portes périphériques sont fermées lorsqu'elles ne sont pas utilisées autrement que dans des situations d'urgence ;

d) les fenêtres raisonnablement susceptibles de permettre une surveillance visuelle des informations traitées à l'intérieur des locaux doivent être occultées ou recouvertes d'un revêtement qui interdit une telle surveillance visuelle ;

e) toutes les fenêtres périphériques du rez–de–chaussée qui ne sont pas situées à l'intérieur de zones gardées et clôturées doivent être munies d'un système de détection des intrusions qui détecte les entrées non autorisées réelles ou les tentatives d'entrée non autorisée ; et

f) l'utilisation de systèmes personnels de reproduction est interdite.

Section 38

Violations et compromission de la sécurité des informations

38.1 Les informations classées « CONFIDENTIEL [CPI] » ou à un niveau supérieur, perdues ou temporairement perdues (y compris les documents qui ne peuvent être localisés lors des inventaires périodiques) sont présumées compromises à moins qu'une preuve du contraire ne soit produite.

38.2 Les suspicions de compromissions doivent être immédiatement signalées au fonctionnaire chargé de la sécurité des informations.

38.3 Le fonctionnaire chargé de la sécurité des informations, en consultation avec le propriétaire des informations, enquête sur la suspicion de compromission pour déterminer :

a) si les informations classifiées ont été divulguées ;

b) à qui les informations classifiées ont été divulguées ;

c) l'impact éventuel de la compromission ;

d) comment la compromission ou la violation de la sécurité a eu lieu ;

e) s'il y a suspicion de négligence ou d'intention malveillante ; et

f) quelles sont les mesures correctives et préventives recommandées.

38.4 Aux fins d'une enquête approfondie et exhaustive, le fonctionnaire chargé de la sécurité des informations, en consultation avec le propriétaire de l'information, et le Greffier si la vie privée de membres du personnel est concernée, peut avoir accès aux sources d'information pertinentes pour son enquête et décider de faire faire des recherches sur ces informations ou sur les personnes transportant ces informations.

38.5 Au cas où une enquête aurait une incidence sur les impératifs opérationnels, financiers ou juridiques de la Cour, le fonctionnaire chargé de la sécurité des informations agit en consultation avec les unités administratives concernées.

38.6 Le fonctionnaire chargé de la sécurité des informations fait rapport au propriétaire des informations et, le cas échéant, au Greffier et au chef du membre du personnel responsable de la suspicion de compromission.

Section 39

Évaluation et audit

39.1 Des contrôles périodiques sont instaurés pour assurer l'application et le respect de la présente instruction administrative :

a) le chef responsable des informations fixe les conditions de respect de la présente instruction administrative et les documents de suivi qui attestent de ce respect ; et

b) le fonctionnaire chargé de la sécurité des informations s'assure du respect de la présente instruction administrative au moins une fois par an.

Section 40

Dispositions finales

40.1 La Cour peut choisir de faire appliquer l'une quelconque ou l'ensemble des dispositions de la présente instruction administrative par des contrôles organisationnels, administratifs, physiques et techniques à caractère préventif, palliatif ou d'investigation.

40.2 La Cour se réserve le droit de consigner, contrôler, examiner ou analyser l'un quelconque ou l'ensemble des aspects de l'utilisation et du traitement des informations aux fins de vérifier le respect des dispositions y afférentes et de garantir en toutes circonstances le maintien de l'intégrité, de la confidentialité et de la disponibilité des informations.

40.3 Le non-respect de la présente instruction administrative ou la compromission des informations peut entraîner des mesures disciplinaires conformément au Statut du personnel, au Règlement du personnel ou à tout autre texte administratif applicable.

40.4 Toute personne qui souhaite demander une exemption pour l'une quelconque des dispositions de la présente instruction administrative doit adresser sa requête par écrit à l'Unité chargée de la sécurité des informations de la Section de la sécurité, par l'intermédiaire de son supérieur.

40.5 La présente instruction administrative sera révisée tous les ans et modifiée au besoin par l'Unité chargée de la sécurité des informations et la Section de la sécurité, dans le cadre du processus de gestion de la sécurité des informations.

40.6 La présente instruction administrative est applicable à partir de la date de sa signature.

Bruno Cathala
Greffier