EP

Programme des
Nations Unies
pour l'environnement

UNEP(DEPI)/MED WG.316/6
1er juin 2007
FRANÇAIS
Original: ANGLAIS

PLAN D'ACTION POUR LA MÉDITERRANÉE
MED POL

Réunion des Coordonnateurs nationaux du MED POL

Hammamet (Tunisie), 25-28 juin 2007

SYSTÈME D'INFORMATION DU MED POL
POLITIQUE PROPOSÉE POUR LA GESTION DES DONNÉES

(ÉTABLI PAR INFO/RAC)

PNUE/PAM
Athènes, 2007

Table des matières

1. Politique d'accès aux données du MED POL

La partie 1 du présent document est consacrée à la politique proposée pour accéder aux données du MED POL. Une politique convenue permettrait effectivement aux Parties contractantes de disposer d'un processus structuré et cohérent pour obtenir l'accès qui leur est nécessaire aux données du MED POL.

1.1 Justification de la politique d'accès aux données du MED POL

Les activités du MED POL génèrent différents types de données, qui forment un éventail allant des "données brutes" telles que les données ou les mesures de l'environnement obtenues par observation directe jusqu'aux "données informatiques" qui mènent à "l'information" et, finalement, à la "connaissance".

On peut considérer que ces données constituent les résultats fondamentaux des activités du MED POL; c'est uniquement grâce à elles que le MED POL peut effectivement contribuer à formuler les mesures à appliquer pour évaluer et maîtriser la pollution. La gestion et l'accès aux données du MED POL ainsi que leur diffusion auprès du public forment l'essentiel de ce processus. À cet égard, les données brutes ont une importance particulière. Les données peuvent certes être manipulées par les chercheurs pour obtenir du matériel à publier, des rapports, etc., mais elles sont aussi une ressource en elles-mêmes. Bien gérées et bien préservées, elles peuvent éventuellement être utilisées et réutilisées par de futurs chercheurs, des institutions, etc., et exploitées à des fins éducatives.

Les données sur l'environnement sont souvent irremplaçables; elles sont toujours uniques, à ne considérer que le moment où elles sont rassemblées. Leur collecte peut aussi être un exercice extrêmement coûteux. Pour ces raisons, le MED POL attache beaucoup d'importance à ce que le maximum en soit tiré une fois qu'elles sont obtenues.

Le MED POL propose donc une politique formelle d'accès aux données. Il est essentiel que cette politique et ses incidences soient bien comprises au niveau de la direction dans tout le PAM. Il faudra donc veiller à ce que de bonnes directives soient transmises à tous ceux qui en ont besoin dans le cadre de leurs organisations.

La politique du MED POL en matière de données est destinée à servir les objectifs importants ci-après:

- assurer l'accès pleinement contrôlé aux données du MED POL et leur utilisation dans les mêmes conditions;
- assurer la gestion efficace et licite des données du MED POL;
- construire une base de données durable pour le développement à long terme du programme MED POL;
- maintenir une approche intégrée des données dans toutes les Parties contractantes;
- assurer l'accès approprié à l'information sur l'état du milieu marin et de l'environnement côtier dans le domaine d'application de la Convention et des Protocoles et sur les activités menées ou les mesures prises dans le cadre de la mise en oeuvre de la Convention et des Protocoles afin de donner au public la possibilité, le cas échéant, de participer à la prise des décisions concernant l'application de ces instruments.

1.2 Données visées par la politique

La politique décrite dans le présent document porte sur toutes les données du MED POL allant des données brutes à "l'information" et finalement à la "connaissance".

Plus précisément, ces données sont les suivantes:

- Les données de la surveillance de la pollution dans le bassin méditerranéen générées dans le cadre du programme du MED POL relatif à la surveillance continue de l'état et de l'évolution de l'environnement, qui sont au départ présentées au MED POL.
- Les données sur les sources de pollution dans le bassin méditerranéen mesurées dans le cadre des activités de suivi du respect des obligations, qui sont au départ présentées au MED POL.
- Les données se rapportant aux rapports sur la mise en œuvre des Protocoles "tellurique", "immersions" et "déchets dangereux".
- Les autres données et informations qui sont demandées par les Parties contractantes.
- Toutes les données informatiques, sorties de modèles, traçages, documents, etc., produits par les activités du MED POL.

La politique porte sur tous les produits des activités du MED POL, depuis les données brutes présentées par les Parties contractantes jusqu'aux données et résultats informatiques relatifs à ces activités.

La politique ne s'applique pas aux notes et documents qui sont la propriété personnelle de certains dans le système du MED POL.

Les données ne relèvent de cette politique qu'après avoir été présentées au MED POL.

Les données du MED POL, visées ci-dessus, sont appelées dans le présent document les "données".

1.3 Profils de l'utilisateur visés par la politique

Toute entité (personne physique ou organisation) intéressée par les données est appelée dans ce document "l'utilisateur". L'utilisateur peut être ou ne pas être authentifié, et l'utilisateur qui ne l'est pas est un *utilisateur anonyme*. Un utilisateur peut avoir un ou plusieurs profils. Les utilisateurs font l'objet d'un classement logique selon des profils qui permettent de définir différents niveaux de droits d'accès aux données. L'utilisateur anonyme se trouve au niveau *le plus bas* car c'est celui auquel s'appliquent généralement les conditions d'accès les plus restrictives.

La définition des profils d'utilisateur permet de bien gérer l'accès aux données. Ces profils sont décrits plus loin au titre de la section "Définition des profils d'utilisateurs". La politique s'applique à tous les profils décrits.

1.4 Exposé de la politique proposée

1.4.1 Principes directeurs de l'accès aux données

Les Parties contractantes peuvent s'accorder sur les principes directeurs suivants régissant l'accès aux données:

- L'accès aux données est soumis aux restrictions décrites dans le présent document.
- La restriction de l'accès aux données peut être assurée par le biais du DBMS (système de gestion de base de données) ou de l'application de mesures organisationnelles.
- Les données sont fournies conformément à des normes spécifiques.
- Autant que possible, l'accès aux données ne doit pas être limité afin de faciliter la participation active de la société civile aux activités du MED POL.

Comme indiqué dans le document "CONCEPTION THÉORIQUE DE LA BASE DE DONNÉES DU MED POL PHASE III", (réf. Doc. UNEP(DEC)/MED WG 202/2 (révisé)), le Programme MED POL prévoit la surveillance continue de l'évolution tendancielle des agents contaminants et des charges ainsi que la surveillance des effets biologiques et du respect des obligations. Les données sont collectées conformément à des accords de surveillance continue signés entre le PNUE/PAM et les pays méditerranéens. Ces accords contiennent une description du programme national de surveillance, y compris une liste des stations d'échantillonnage et des variables à suivre, des fréquences de la surveillance, des instituts participants, etc. Aux termes des accords, des rapports périodiques sur les données de surveillance doivent être présentés au MED POL. Les données qui font l'objet de ces rapports sont essentiellement les suivantes:

1) Données de surveillance sur les éléments suivants:

a) Biotes
b) Sédiments
c) Eaux
d) Atmosphère

2) Données supplémentaires:

a) Données certifiées des analyses matières
b) Méthodes utilisées pour l'analyse
c) Données de l'assurance qualité

3) Données de la surveillance du respect de l'obligation: charges

4) Données et informations relatives à la mise en œuvre des Protocoles "tellurique", "immersions" et "déchets dangereux".

À partir de ce classement général, le MED POL a réparti toutes les données en plusieurs sous-ensembles appelés "formats de rapports", qui contiennent des mesures homogènes. Selon le modèle théorique de la base de données actuelle du MED POL, le même classement est utilisé dans la politique d'accès aux données du MED POL, à laquelle est ajouté un indice supplémentaire de classement: le statut des données selon que leur utilisation est publique (catégorie I) ou limitée (catégorie II).

Catégorie I – Données publiques: ce sont les informations ciblées pour le public: par exemple, la teneur des sites web sur l'Internet pour consultation générale et les communiqués de presse.

Catégorie II – Données de diffusion limitée: ce sont les informations qui ne sont généralement pas disponibles pour toutes les Parties, telles que les données brutes (celles fournies par les Parties contractantes au MED POL), les inscriptions à l'annuaire et les sites web internes (Intranet). Dans le classement des données, c'est la catégorie par défaut.

En bref, les données sont classées selon trois indices:

- Indice environnemental: le sujet environnemental auquel les données se rapportent. Le format de rapport du MED POL qui leur correspond et/ou dans lequel elles figurent.
- Indice de pays: le pays auquel les données se rapportent.
- Indice du statut: public ou limité.

Par conséquent, les trois indices permettent de définir différents domaines de données.

Par exemple: un domaine est formé des données de diffusion limitée se rapportant aux mesures des biotes en Espagne, un autre aux données publiques se rapportant aux mesures des sédiments en Tunisie, etc. Un domaine peut aussi comprendre des éléments.

Les intendants d'actif informationnel, en consultation avec les administrateurs de données, sont chargés de définir les éléments des données qui entrent dans chaque domaine.

Les utilisateurs peuvent demander aux intendants d'actif informationnel de revoir les restrictions imposées à un élément de données et/ou au classement des données. Toutes les demandes seront soumises par l'intermédiaire d'un administrateur des données à l'intendant compétent. C'est à l'intendant qu'il appartiendra en dernier ressort de prendre les décisions concernant les questions de restriction et les demandes de droits d'accès aux données.

1.4.2 Accès aux données

Les données sont accessibles aux utilisateurs. L'utilisateur peut avoir un ou plusieurs profils en fonction des droits qui lui sont octroyés. Les différents profils d'utilisateur sont décrits ci-après.

1.4.3 Définition du profil d'utilisateur

Chaque profil d'utilisateur est assorti de droits qui lui permettent de faire quelque chose. Tous les droits prévus dans la présente politique se rapportent à un ou plusieurs domaines définis de données. Selon le modèle théorique de la base de données du MED POL, les droits proposés dans la politique sont les suivants:

- Droit de lire les données (y compris de les décharger), appelé dans le présent document le "droit de lecture". Ce droit se rapporte à un domaine défini de données. Par exemple: lire les données atmosphériques "limitées" de l'Italie, lire les données "publiques" sur les sédiments en Syrie, etc.
- Droit de saisir de nouvelles données, appelé dans le présent document le "droit de saisie de nouvelles données". Ce droit se rapporte à un domaine défini de données. Par exemple: saisir de nouvelles données "limitées"sur les biotes en Grèce, saisir de nouvelles données "limitées" sur les eaux de mer pour la Turquie, etc.
- Droit d'écrire et de modifier des données, appelé dans le présent document le "droit d'écriture". Ce droit se rapporte à un domaine défini de données. Par exemple: écrire les données "limitées" sur les métaux en trace des biotes égyptiens, etc.
- Droit de gérer (activer/désactiver/modifier) l'accès de l'utilisateur à un domaine de données, appelé dans le présent document le "droit de gestion de l'utilisateur". Ce droit concerne la gestion de l'accès de l'utilisateur à un domaine défini de données. Par exemple: le droit de gérer l'accès de tous les utilisateurs aux domaines français des données "limitées" et "publiques", etc.

Les profils d'utilisateur sont les suivants:

- Anonyme:
  - Droits anonymes: droit de lecture des données du domaine public.
- Spécialiste – le profil est assorti des deux attributs suivants:
  - Un domaine particulier de spécialisation en matière d'environnement
  - Une nationalité déterminée
  - Droits du spécialiste: droit de lecture des données de certains domaines définis.
- Partie contractante – le profil est assorti de l'attribut suivant:
  - Une nationalité déterminée

- Droits de la Partie contractante: lecture et saisie de données nouvelles dans son propre domaine national.

- Responsable de l'entrée des données.
  - Droits du responsable: lecture et écriture dans tous les domaines de données.
- Administrateur de données:
  - Droits de l'administrateur de données: gestion de l'utilisateur dans tous les domaines de données.

1.4.4 Procédures applicables à la demande d'accès aux données

Les procédures et directives détaillées à suivre pour demander l'accès aux données en application de la présente politique sont exposées dans les procédures d'accès aux données du MED POL. Les documents pertinents seront mis à jour "en tant que de besoin", pour tenir compte de tous changements intervenus dans le processus et/ou les rôles en jeu.

L'intendant d'actif informationnel, en consultation avec les administrateurs de données, est chargé des tâches suivantes:

- Classer et/ou reclasser les éléments de données et les vues
- Accorder l'accès sélectif aux données
- Former les utilisateurs autorisés aux responsabilités associées à l'accès aux données
- Informer les spécialistes technologiques du classement des données pour déterminer les contrôle physiques et/ou logiques nécessaires.

Par ailleurs, il appartient aux utilisateurs autorisés et à leurs services respectifs de protéger les données qui leur sont confiées, en veillant au respect de la présente politique, sous tous ses aspects, et des procédures qui s'y rapportent.

L'accès aux données publiques du MED POL est gratuit sous réserve que l'utilisateur accepte:

- de ne pas utiliser l'information à des fins commerciales;
- de faire état de la source et d'afficher le lien au serveur de données (MED POL ou tout autre serveur figurant sur la liste du service des données). Pour toute information du MED POL disponible gratuitement, l'accusé de réception des données doit se lire: "© MEDPOL, Athens, <production year>"
- d'aider à améliorer la qualité des données en notant et signalant toutes les erreurs ou omissions décelées;
- de contribuer à améliorer la qualité du service des données en donnant des informations en retour sur les fonctionnalités et l'ensemble des données;
- de contribuer à améliorer l'utilisation coordonnée des données en faisant part au MED POL des applications qui utilisent l'information;
- d'aider à améliorer l'efficacité des rapports environnementaux en fournissant au MED POL des copies numériques documentées des données/cartes/graphiques et renseignements découlant de l'information du MED POL, pour que ce dernier puisse les réutiliser en faisant référence à la source;
- de fournir au MED POL une copie de l'adresse URL à toutes les publications et autres produits reposant sur les produits découlant de ses informations et services.

Ni le MED POL, ni les Parties contractantes ou le PAM, ni la personne ou la société qui agit en leur nom ne sauraient être tenus pour responsables de l'utilisation qui pourrait être faite de l'information au service des données. La teneur du produit ne reflèterait pas

nécessairement l'opinion officielle du MED POL/PAM, de ses institutions ou des organisations internationales et des pays qui participent à la préparation du produit.

Les appellations employées dans la présente publication et la présentation des données qui y figurent n'impliqueraient de la part du MED POL/PAM aucune prise de position quant au statut juridique des pays, territoires, villes ou zones ou de leurs autorités.

En aucun cas le MED POL ne saurait être tenu pour responsable des dommages spéciaux, indirects ou autres résultant de la perte de jouissance, de données ou de profits, que ce soit dans le cadre d'un contrat, par négligence ou par tout autre fait dommageable, découlant de l'utilisation ou du fonctionnement de logiciels, de documents, de la prestation ou non-prestation de services, ou d'informations disponibles au service des données. Les liens permettront à l'utilisateur de quitter le site web du MED POL. Les sites liés ne relèvent pas du contrôle du MED POL. Le MED POL n'est pas responsable de la teneur de ces sites ni de leurs modifications ou de leurs mises à jour éventuelles. Le MED POL ne fournit ces liens que par commodité pour l'utilisateur.

L'accès aux données "limitées" serait accordé aux utilisateurs autorisés, à condition qu'ils:

- respectent les restrictions qui s'appliquent aux données sensibles;
- se conforment aux lois, politiques, procédures et directives applicables à l'accès, à l'utilisation ou à la divulgation d'informations.

Sauf dans les cas où le profil de l'utilisateur l'exige, le stockage, la divulgation ou la diffusion non autorisée de données du MED POL par les médias seraient expressément interdits, comme le serait l'accès ou l'utilisation des données du MED POL dans un but lucratif pour soi-même ou pour autrui ou pour satisfaire sa propre curiosité ou celle d'autrui.

Les utilisateurs seraient censés respecter les règles énoncées dans la présente politique. Le non-respect de la politique peut entraîner la perte des droits d'accès aux données et le prononcé de sanctions, comme indiqué dans les procédures disciplinaires du MED POL.

Dès son approbation, la politique proposée sera publiée sur le site web du MED POL et largement diffusée auprès des autorités nationales, de la communauté scientifique et des autres parties prenantes.

2. Procédures d'accès aux données du MED POL

La partie 2 sur les procédures d'accès aux données vient directement à l'appui de la *Politique d'accès aux données du MED POL* à laquelle référence doit être faite. Il énonce les directives et procédures à suivre pour demander l'accès aux données du MED POL et, en particulier, aux données "limitées" telles que définies dans la Politique d'accès aux données du MED POL. Les procédures d'accès feront l'objet périodiquement de modifications et de mises à jour, en tant que de besoin, indépendamment de la politique décrite dans la partie 1.

La demande d'accès aux données est gérée par une structure à deux niveaux. Les deux niveaux sont les suivants:

- Demandeurs autorisés,
- Intendants d'actif informationnel.

Le traitement de la demande d'accès aux données relève de la responsabilité de l'administrateur des données.

Les différentes étapes de la procédure de demande d'accès aux données, et les conditions à remplir, sont les suivantes:

a) L'utilisateur présente une demande d'accès aux données. La demande d'accès est adressée au demandeur autorisé par courrier électronique, par télécopie ou par courrier ordinaire ou au moyen d'un formulaire en ligne.

b) Le demandeur autorisé vérifie les conditions individuelles d'accès et adresse la demande d'accès à l'intendant d'actif informationnel compétent. Il est chargé de recevoir les demandes entrantes et d'aider le demandeur à présenter une demande en bonne et due forme.

Afin d'être traitée, la demande doit être présentée comme il convient, c'est-à-dire qu'elle doit répondre aux conditions suivantes:

i) être complète et contenir toutes les informations pertinentes sur l'utilisateur, comme indiqué ci-dessous.

ii) indiquer les droits demandés, droits compatibles avec le rôle du demandeur.

Selon les besoins, les demandeurs autorisés aideront l'utilisateur à présenter une demande d'accès en bonne et due forme.

(c) L'intendant d'actif informationnel examine la demande et décide de l'accepter ou de la rejeter.

Si la demande est acceptée, l'intendant d'actif informationnel, en consultation avec le demandeur autorisé et l'administrateur de données, affecte un profil à l'utilisateur.

L'acceptation est notifiée à l'administrateur pour qu'il puisse activer l'accès aux données.

L'administrateur de données active l'accès de l'utilisateur aux données, l'informe des moyens d'accès à ces dernières en fonction de son profil et notifie qu'il a activé l'accès au demandeur autorisé.

Les administrateurs de données et les demandeurs autorisés conservent des archives électroniques de toutes les demandes.

Les demandes des utilisateurs de statut national sont adressées aux demandeurs nationaux autorisées et examinées par les intendants d'actif nationaux correspondants.

Les demandes des utilisateurs de statut international sont adressées au demandeur autorisé du Secrétariat et sont examinées par l'intendant d'actif du Secrétariat.

La structure établie – demandeurs autorisées, administrateur de données et intendant d'actif informationnel – permet de répartir la tâche entre tous les pays et offre un moyen efficace d'examiner les différentes demandes et de prendre les décisions à leur sujet dans chaque pays.

La structure à deux niveaux permet aussi de répartir la responsabilité de la gestion de l'accès en fonction des aspects techniques (demandeurs autorisés et administrateur de données) et des aspects politiques (intendant d'actif informationnel).

Dans chaque pays, il faudrait au moins un demandeur autorisé qui puisse recevoir les demandes des utilisateurs nationaux.

Il devrait y avoir au Secrétariat un demandeur autorisé qui recevrait les demandes des utilisateurs internationaux.

Dans chaque pays, il conviendrait qu'au moins un intendant d'actif informationnel décide d'accepter ou de rejeter les demandes des utilisateurs nationaux. Ces intendants peuvent être les Coordonnateurs nationaux du MED POL.

Il conviendrait qu'il y ait au Secrétariat au moins un intendant d'actif informationnel qui déciderait d'accepter ou de rejeter les demandes des utilisateurs internationaux. L'intendant peut être un fonctionnaire du Secrétariat.

Il suffit qu'il y ait au Secrétariat un seul administrateur des données qui peut aussi être le demandeur autorisé pour les utilisateurs internationaux.

Le formulaire de demande d'accès aux données doit contenir les informations suivantes:

- Nom de l'institution/organisation
- Nom de l'utilisateur
- Titre
- Numéro de téléphone
- Quelles données/quel rôle et pourquoi (l'administrateur national de données ou celui du MED POL fourniront une aide)
- Date de fin d'accès.

Note: Toute modification ou prolongation de l'utilisation initialement prévue des données demandées (selon la demande initiale d'accès) – par exemple, la mise au point d'une nouvelle application qui fait appel aux données pour lesquelles l'accès a été précédemment demandé – exige la présentation d'une nouvelle demande d'accès contenant des informations explicites sur les changements ou la prolongation.

La présentation du formulaire d'enregistrement se fait par voie électronique (en ligne ou par courriel) ou sur support papier (télécopie ou courrier ordinaire). Le formulaire en ligne et le dossier de téléchargement en PDF se trouveraient sur le site web du MED POL. Le formulaire sur support papier serait adressé par courrier ordinaire sur demande adressée au Secrétariat.

Il convient de rappeler que lorsque l'utilisateur présente le formulaire d'enregistrement, il passe un contrat légal avec le MED POL et accepte de se conformer à tous les règlements.

3. Glossaire

Serveur d'application: L'ordinateur hôte de l'application que le terminal général de l'utilisateur connecte.

Disponibilité: Temps pendant lequel il est possible d'extraire les informations nécessaires. L'indisponibilité de l'information peut être due à une destruction/un effacement, au non-fonctionnement du système ou du réseau ou à la sur-utilisation des sources de données à extraire.

Demandeurs autorisés: Chefs d'unité ou personnes qui ont été habilités à autoriser et à engager les demandes d'accès conformément aux procédures établies par le chef d'unité ou un supérieur hiérarchique dans l'organisation.

Utilisateur (ou utilisateurs) autorisé(s): Personnes ou organisations ayant le droit d'accès aux données du MED POL pour s'acquitter de tâches qui leur sont assignées.

Computer & Network Usage and Security Policy (CNUSP) (Politique de sécurité informatique): La politique GIT qui régit le comportement des personnes et des organisations quant à l'utilisation des ressources des technologies de l'information du MED POL.

Confidentialité: Prévention de la divulgation d'informations à quiconque n'est pas autorisé à voir, copier ou diffuser ces informations.

Politique d'accès aux données: La politique établie du MED POL qui régit le classement des données et les contrôles d'accès nécessaires en fonction de ce classement.

Administrateur de données: Personne chargée d'informer l'utilisateur et d'activer l'accès de ce dernier à un domaine de données du MED POL.

Classement des données:
Les deux catégories de données du MED POL, définies dans la Politique d'accès aux données, sont les suivantes:

- Catégorie I - Utilisation publique: informations ciblées pour le public: par exemple, teneur des sites web sur l'Internet pour une consultation générale et communiqués de presse.
- Catégorie II – Utilisation interne: informations qui ne sont généralement pas disponibles en dehors du MED POL et du PAM: par exemple, données brutes (celles qui sont fournies par les Parties contractantes au MED POL), inscriptions à l'annuaire, minutes de réunions non confidentielles et sites web internes (Intranet). La divulgation publique de ces données causerait un minimum d'ennuis ou d'embarras à l'institution. Dans le classement des données, c'est la catégorie par défaut.

Intendant d'actif informationnel: Personne chargée de l'examen des demandes d'accès aux données.

Vues des données: Collection logique d'éléments de données, provenant éventuellement de plusieurs bases de données physiques, qui sont assemblées et présentées selon une série de règles définies.

Attaque par saturation (DoS): Attaque venant généralement d'un seul système visant à profiter de la vulnérabilité d'un autre système pour provoquer le refus d'un accès légitime au système ou à la ressource.

Certificats numériques: Une forme d'authentification de haute sécurité – l'échange de brefs dossiers chiffrés par les programmes en communication, qui servent à authentifier le client avec le serveur. Il existe tout un système d'organisations et de protocoles qui travaillent ensemble pour créer, authentifier, annuler et utiliser des certificats numériques. L'utilisateur d'un ordinateur permet généralement au(x) programme(s) d'utiliser des certificats numériques en déclinant son identité dans le système ou programme à l'aide d'un identifiant/mot de passe.

Planification en prévision des catastrophes: Élaboration, application et mise à l'essai des plans et procédures pour poursuivre les opérations essentielles de l'organisation même après une catastrophe, comme un tremblement de terre, un ouragan, une inondation, une panne prolongée d'électricité, un acte de terrorisme, etc. Il s'agit généralement de doubler les installations informatiques, les installations de communication, les accords de fournisseurs, les procédures appliquées aux employés.

Attaque par déni de service distribué (DDoS): Attaque informatique par un code malveillant situé sur plusieurs systèmes dans l'intention de submerger un ou des ordinateurs ou les ressources d'un réseau afin d'en bloquer l'utilisation.

Chiffrement: Utilisation de programmes et de mesures pour chiffrer l'information pour qu'elle ne puisse pas être décodée et lue sans clé appropriée – généralement un code propre à l'utilisateur.

Filtrage: Processus qui consiste à examiner un fichier ou une acquisition faite par le réseau ou autrement (par exemple à partir de CD ou de disquette) pour en déceler le contenu nuisible ou malicieux.

Prise d'empreinte (de dossiers) (fingerprinting): Création d'un résumé mathématique du fichier qui est généralement suffisant pour déceler toute modification de ce dernier, mais peut faire l'objet d'un stockage compact (par exemple hachage ou contrôle de redondance cyclique (CRC) de tout le dossier).

Coupe-feu: Dispositif ou programme destiné à contrôler sur le réseau le flot de circulation des données vers un ordinateur ou un segment du réseau.

Hachage: Établissement d'une valeur unique pour un fichier, un programme ou une communication spécifique qui donne l'assurance que l'information est complète et n'a pas été trafiquée. L'objectif consiste en partie à fournir un élément de signature suffisant pour confirmer que l'information est complète sans pouvoir générer l'information réelle à partir du hachage.

Ressources des technologies de l'information: Ordinateurs, périphériques de stockage, matériel et câbles, imprimante et télécopieurs connectés au réseau.

Intégrité: Le degré de confiance qui permet d'assurer que l'information n'a pas été modifiée sans autorisation ou de manière abusive.

Système de détection d'intrusion (IDS): Réseau ou système basé sur un poste de travail utilisé aux fins de détection et de notification quand une attaque est lancée.

Système de prévention d'intrusion (IPS): Un IDS basé sur le réseau qui réagit automatiquement pour empêcher les attaques d'aboutir. Il faut faire tout particulièrement attention avec l'IPS pour que le système n'arrête pas la communication qui doit se faire, même pendant les attaques.

Messagerie instantanée: Méthode de communication immédiate entre utilisateurs.

Mystification de l'IP: Fourniture d'une adresse de réseau (adresse IP) qui n'est pas correctement affectée dans le dessein d'empêcher autrui de localiser la source de certains trafics ou messages du réseau.

ISO 17799: Document de l'Organisation internationale de normalisation qui définit les normes de sécurité informatique. Les vendeurs de cartes de crédit peuvent fonder leurs politiques sur cette norme.

Journalisation: Conservation d'un fichier d'informations à l'entrée à partir du clavier d'un ordinateur. Cela peut être fait sur l'ordinateur ou un dispositif connecté au clavier.

LAWN: Georgia Tech Local Area Wireless/Walkup Network. Cet accès authentifié à un réseau permet d'accéder sans câble au GIT et fournit l'authentification des points d'accès câblés dans certains lieux publics.

Salle d'accès limité: Salle dont un nombre restreint de personnes seulement a la clé et est habilité à gérer le matériel TI qui s'y trouve.

Capture de paquets sur le réseau: Capture d'informations destinées à autrui pour les transmettre sur le réseau en vue d'en faire ultérieurement un examen abusif.

Forums: Groupes de discussion en ligne sur certains sujets.

Hameçonnage: Envoi d'un polluriel sur un événement qui exige de la personne qu'elle fournisse directement des renseignements personnels ou qu'elle aille sur un site spécial pour fournir ces informations qui sont utilisées à des fins frauduleuses.

Scannage de ports: Utilisation d'un programme ou examen manuel de tous les ports de réseaux informatiques (65 535 disponibles) ou d'un petit sous-ensemble sur un ou plusieurs ordinateurs.

Page de pré-ouverture: Message qui apparaît devant la personne qui cherche à ouvrir un ordinateur ou un moyen de communication AVANT d'avoir été invitée à entrer un élément d'authentification (identifiant/mot de passe, biométrie, etc.).

Polluriel (ou courriel non sollicité – UBE ou courriel commercial non sollicité – UCE): Courriel envoyé au destinataire sans qu'il le souhaite (et souvent contre son gré) pour promouvoir une offre commerciale. Ce type de courriel a probablement représenté 50 à 70% de tous les courriels sur l'Internet en 2004.

Logiciel espion: Logiciel installé sur un ordinateur (généralement à partir d'un site web) pour suivre l'utilisation de l'ordinateur et faire rapport à ce sujet.

Cheval de Troie (programme): Programme qui consiste en un code malveillant mais qui fait l'objet d'une promotion ou semble être un programme utile qui vise à inciter la personne peu soupçonneuse à exécuter le programme. Ce programme n'est pas auto-propageable et est normalement ciblé sur un individu ou un système.

Autorité technique: Personne (à l'intérieur ou à l'extérieur de l'unité) désigné par le chef de l'unité, qui a les compétences requises pour attester du respect technique des normes publiées de tous les serveurs et postes de travail utilisés par l'unité pour accéder ou stocker les données du MED POL.

Responsable technique: Personne désignée par le chef de l'unité comme étant la première responsable de la planification et de la mise en place du système d'information/de technologie de l'information.

Équipe d'appui technique: Groupe de personnes (le cas échéant) chargé de l'application et de la maintenance des systèmes informatiques, de technologies de l'informations.

Authentification par deux éléments: Méthode d'authentification qui exige deux éléments (en plus de l'identifiant). Ce seront généralement des éléments connus (par exemple, un mot de passe) et disponibles (par exemple, le numéro d'une unité lexicale, une empreinte).

Unité: Groupe de travail fondamental figurant dans l'organigramme officiel de l'organisation.

Chef d'unité: Personne directement responsable d'une unité.

Serveurs des unités: Serveurs qui fournissent des informations essentielles aux unités, ou systèmes auxiliaires d'interface avec les services centralisés tels que: serveurs web, serveurs de fichiers, serveurs d'imprimantes, serveurs de noms de domaines, serveurs de transfert de dossiers, coupe-feux, dispositifs de stockage en réseau, serveurs DHCP, solutions d'accès à distance et autres systèmes auxiliaires.

Virus: Logiciel malveillant exécuté par l'utilisateur. Le virus se propagera à d'autres ordinateurs et/ou programmes.

Voix sur IP (VoIP): Communications téléphoniques acheminées sur un réseau informatique utilisant un IP, au lieu du réseau téléphonique traditionnel.

Développement du web: Conception, mise au point, mise en place et gestion des interfaces frontales pour les applications web.

Point d'accès sans câble (AP): Tout dispositif qui permet de connecter un ordinateur ou un assistant numérique personnel à un réseau ou à un autre ordinateur ou assistant numérique personnel par fréquence radio.

Ver informatique: Programme autonome qui fonctionne sur un système et qui se propage à d'autres systèmes sans intervention de l'utilisateur.

Les définitions ci-dessus peuvent être revues en consultation avec les Coordonnateurs nationaux du MED POL, et en accord avec eux, pour tenir compte de la nature changeante des technologies et de l'évolution de la réglementation.