F

OMPI

SCIT/7/12
ORIGINAL : anglais
DATE : 26 avril 2002

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
GENÈVE

COMITE PERMANENT DES TECHNIQUES DE L'INFORMATION

COMITÉ PLÉNIER
Septième session
Genève, 10 – 14 juin 2002

APERÇU DES POLITIQUES DE L'OMPI
EN MATIERE DE SECURITE DE L'INFORMATION

Document établi par le Secrétariat

INTRODUCTION

1. La mise en œuvre et l'utilisation généralisées des techniques de l'information et de la communication, y compris les réseaux et les environnements répartis de traitement de données, soulèvent de nouvelles questions. Les réseaux offrent une plus grande souplesse d'accès aux informations et aux ressources et de partage de ces informations et ressources et facilitent le traitement au bureau. Toutefois, ces avantages se traduisent par une plus grande diffusion d'informations sensibles et il est donc nécessaire de mettre en œuvre des stratégies afin de garantir la confidentialité, l'intégrité et la disponibilité de l'information et des systèmes d'information.

2. Le présent document donne un aperçu des politiques de l'OMPI en matière de sécurité de l'information et des stratégies utilisées pour les mettre en œuvre.

CHAMP D'APPLICATION

3. Les politiques de l'OMPI en matière de sécurité de l'information s'appliquent à tous les fonctionnaires de l'OMPI, membres du personnel, consultants internes, employés temporaires, et aux fournisseurs externes travaillant avec l'OMPI. Les fonctionnaires de l'OMPI doivent s'assurer que lescontrats passés avec des individus et des entreprises qui, par la nature de leurs relations avec l'OMPI, reçoivent des informations sensibles, sont, sauf autorisation contraire, conformes aux politiques en matière de sécurité. Ces politiques couvrent tous les aspects de la sécurité de l'information, de la conception initiale d'un système d'information à sa mise en œuvre et son fonctionnement. Elles couvrent également tout dispositif utilisé pour mémoriser, traiter ou diffuser l'information relative à l'OMPI. Elles s'appliquent indépendamment de la manière dont l'information est présentée (par écrit, oralement, par impression, par voie électronique ou sous d'autres formes), des techniques utilisées pour la traiter et de son emplacement (par exemple, au bureau, dans un endroit à distance ou dans un avion).

GESTION DE LA SÉCURITÉ

4. La gestion de la sécurité vise à mettre en place une réglementation et des mesures destinées à réduire les risques de perte d'information et de ressources du système, d'altération des données, de perturbation de l'accès aux données et de divulgation non autorisée de l'information. La gestion de la sécurité s'appuie sur la mise en œuvre de politiques efficaces, l'application stricte de normes et de procédures visant à assurer la confidentialité, l'intégrité et la disponibilité de l'information relative à l'OMPI, des logiciels, des systèmes et des réseaux destinés aux utilisateurs autorisés.

Confidentialité

5. La confidentialité concerne la protection de l'information contre tout accès non autorisé, quel que soit l'endroit où elle se trouve ou la manière dont elle est stockée. L'information sensible doit être protégée davantage que les autres types d'information. Les politiques de l'OMPI en matière de sécurité de l'information définissent un cadre permettant de classer les données en indiquant les exigences requises en matière de sécurité.

Intégrité

6. L'intégrité de l'information a trait à la protection de l'information, des logiciels, des systèmes et des réseaux contre toute modification involontaire, non autorisée ou accidentelle. Il est également important de protéger les processus et les programmes utilisés pour manipuler les données. L'information doit être fournie à ses titulaires et utilisateurs de façon sécurisée, précise, complète et dans les délais. Pour assurer cette intégrité, il est essentiel de veiller à l'identification et à l'authentification de tous les utilisateurs qui accèdent à l'information, grâce à une surveillance manuelle et automatisée.

Disponibilité

7. Veiller à la disponibilité de l'information permet d'assurer que l'information et les ressources de l'OMPI sont accessibles aux utilisateurs autorisés. Deux problèmes peuvent se poser à cet égard : le refus de service découlant de l'absence de mesures de sécurité (par exemple, destruction de données ou de matériel, virus informatique) et la perte des services fournis par les ressources en information à la suite de catastrophes naturelles (tempêtes, inondations, incendies). Le refus de service est traité dans le cadre de la gestion de la sécurité. Le problème de la perte de services est abordé dans le cadre des plans de poursuite des opérations.

ROLES ET RESPONSABILITES

8. La responsabilité de la sécurité quotidienne de l'information incombe à tous les fonctionnaires. Les membres du personnel doivent être conscients de la nécessité de protéger les actifs de l'OMPI en matière d'information. Afin de coordonner les activités de l'Organisation dans le domaine de la sécurité de l'information, trois types de rôles ont été définis, chaque fonctionnaire étant susceptible d'endosser au moins l'un de ces rôles. Ces différents rôles visent à déterminer les responsabilités générales au sein de l'OMPI aux fins d'assurer la sécurité de l'information.

1) *Titulaires* - L'OMPI est globalement titulaire de toute l'information, des applications et des systèmes informatiques dans le cadre des politiques en matière de sécurité de l'information. Dans ce contexte, les titulaires sont les individus responsables de l'information ou des systèmes d'information utilisés par leurs unités respectives. Les titulaires comprennent notamment la haute direction, les administrateurs de programme, les chefs de projet ou leurs représentants qui sont chargés de l'acquisition, de la mise au point et de la gestion des systèmes de traitement de l'information relative à l'OMPI. Les titulaires sont chargés de déterminer les droits d'accès et les critères de sécurité relatifs à l'information sous leur responsabilité.

2) *Dépositaires* - Les dépositaires sont en possession physique ou logique de l'information relative à l'OMPI ou de l'information confiée à l'OMPI. Le personnel des services informatiques et les administrateurs de systèmes peuvent être considérés comme les dépositaires. En ce qui concerne l'information mémorisée dans les ordinateurs personnels, les utilisateurs des ordinateurs personnels en seraient les dépositaires. Les dépositaires assument les responsabilités des titulaires en l'absence d'une titularité bien déterminée.

3) *Utilisateurs* - Les utilisateurs sont les individus qui traitent quotidiennement l'information dont des tiers sont titulaires ou dépositaires. Les utilisateurs sont responsables du respect des politiques en matière de sécurité, des normes et des règles établies par les titulaires. En ce qui concerne les questions relatives à l'accès à l'information, les utilisateurs doivent s'en remettre aux titulaires ou aux dépositaires de l'information. Les utilisateurs peuvent être des fonctionnaires, des employés à titre temporaire, des consultants ou des tiers avec lesquels des accords particuliers ont été passés.

9. Compte tenu de la nature sensible et de l'importance des politiques en matière de sécurité de l'information, et aux fins de leur mise en œuvre efficace, la Division des projets informatiques a été organisée selon la structure suivante :

Directeur des services informatiques

10. Le directeur des services informatiques est chargé, dans le cadre de la sécurité de l'information, de faire part à la haute direction des risques commerciaux liés à la mise en œuvre de techniques nouvelles et réparties et de la nécessité d'élaborer les politiques, les procédures et l'infrastructure adéquates en matière de sécurité de l'information.

Administrateur chargé de la sécurité de l'information

11. L'administrateur chargé de la sécurité de l'information est globalement responsable des questions de sécurité. Il est notamment chargé :

- de veiller à ce que l'utilisateur autorisé accède aux données et que les mesures d'authentification soient en place;
- de veiller à ce que les politiques, les normes et les procédures établies en matière de sécurité soient révisées, mises à jour et appliquées;
- d'évaluer les cas de mise en danger, d'utilisation abusive ou de non-respect des mesures de sécurité et de veiller à la mise en œuvre des règles adoptées pour y remédier;
- d'élaborer et de mettre en œuvre un programme de sensibilisation aux questions de sécurité.

Service d'assistance

12. Le service d'assistance est chargé d'apporter une première réponse aux questions relatives à la sécurité en vertu des politiques, normes et procédures en vigueur et, si nécessaire, de les transmettre au chef de division concerné, conformément à la procédure en vigueur à l'OMPI de recours à la hiérarchie en cas d'incident relatif à la sécurité de l'information. Le service d'assistance constitue un service centralisé d'enregistrement des utilisateurs et, au même titre que les administrateurs chargés de la sécurité, assure la gestion des mots de passe.

Chefs de division

13. Dans le présent document, le terme "chefs de division" désigne tous les chefs de programme ou de service de l'OMPI chargés de la mise en œuvre physique ou pratique, dans leur propre domaine d'activité, des politiques de l'OMPI en matière de sécurité de l'information. Les chefs de division sont chargés de mettre en place la stratégie globale en matière de sécurité de l'information dans la division en question. Il s'agit notamment de déterminer la classification de sécurité de l'information appartenant à la division, y compris le degré de sensibilité et de disponibilité requis pour cette information. Il revient également aux chefs de division de déterminer le niveau d'accès autorisé à l'information sous leur responsabilité.

MISE EN ŒUVRE

Sources d'information

14. Il convient de protéger les infrastructures des systèmes d'information afin de veiller à ce que des personnes non autorisées ne puissent pas avoir accès au système, ni provoquer de dommage physique ou encore modifier des composantes internes, ce qui pourrait avoir une incidence sur les résultats du traitement de l'information. Les mesures relatives à l'environnement et à la sécurité doivent être adaptées au niveau de risque. Il conviendrait de réaliser une évaluation mettant en balance les risques avec le coût de la mise en œuvre de ces mesures en vue de déterminer les mesures appropriées en matière de sécurité et d'environnement.

15. Les actifs en matière d'information sont classés de manière à constituer un outil permettant d'indiquer le niveau de protection requis. Les exigences relatives à la sécurité de l'information varient en fonction de la sensibilité et du degré d'importance de l'information ou des systèmes associés à cette information.

16. Les utilisateurs sont libres de se conformer au droit d'auteur, au droit des brevets et aux accords de licence en matière de propriété intellectuelle, dont ils connaissent ou doivent connaître le contenu. Les titulaires de l'information doivent veiller à ce que les dépositaires et les utilisateurs soient conscients des dispositions pertinentes des accords de licence.

17. Le titulaire des données, le dépositaire et l'administrateur chargé de la sécurité de l'information doivent examiner régulièrement l'ensemble des droits d'accès en vigueur et mettre à jour les possibilités offertes à chaque individu dans le système, en vue de s'assurer que le niveau d'accès adéquat a été autorisé et qu'aucune modification n'est nécessaire.

Accès aux systèmes et à l'information

18. L'accès à l'information et aux systèmes est fourni en fonction des besoins opérationnels. Les titulaires de l'information, en tant que responsables de la gestion, sont tenus d'examiner toutes les demandes d'accès à l'information ou aux systèmes et de vérifier que cet accès répond à un besoin opérationnel réel. Toute autorisation d'accès doit être communiquée au dépositaire.

19. Toutes les demandes d'information entre divisions doivent satisfaire aux mêmes critères relatifs aux besoins opérationnels. En prenant la décision d'autoriser ou de refuser un accès, le titulaire de l'information doit prendre en considération les intérêts de l'OMPI, le type d'accès requis et les risques encourus.

20. Lorsqu'un accès extérieur à une information confidentielle de l'OMPI est autorisé, des instructions détaillées doivent être données au destinataire en vue de l'informer de toutes les exigences en matière de sécurité, y compris la nécessité de respecter la confidentialité de l'information, de toute restriction relative à la diffusion de l'information au sein de son organisation, et des procédures de destruction ou de retour de l'information après la période d'accès.

21. Lorsqu'un chef de division est informé de la fin du contrat, de la démission ou du transfert d'un fonctionnaire, il doit faire le point avec l'utilisateur sur le déclassement des données d'utilisateur et des fichiers contenus dans les répertoires du réseau et des applications, avant son transfert ou son départ de l'OMPI. Le chef de division doit indiquer par écrit au service d'assistance les fichiers à transférer ou à détruire. Le déclassement des données doit être effectué selon les directives relatives à la conservation des documents ou, en attendant la mise en œuvre de ces directives, selon les orientations définies par le chef de programme et les principes énoncés dans le Guide des politiques de l'OMPI en matière de sécurité de l'information.

Mesures de surveillance

22. Les administrateurs du réseau, du système et des applications sont chargés de mettre en œuvre des mesures appropriées en vue de détecter les tentatives d'atteinte à la confidentialité ou à l'intégrité de l'information ou des systèmes d'information. Lors de la mise en œuvre des mesures de surveillance, les cas dans lesquels une surveillance est nécessaire doivent être pris en considération, compte tenu du risque encouru, des ressources disponibles pour la surveillance et des limites du système qui déterminent la capacité à surveiller les événements en rapport avec la sécurité. À cet égard, il convient de tenir à jour les logiciels de détection de virus dans l'environnement du réseau local, ainsi que dans les systèmes présentant des risques élevés d'infection.

Programme de sensibilisation à la sécurité de l'information

23. Il est de la responsabilité de la direction de veiller à ce que tous les utilisateurs de l'information soient conscients de la manière de protéger les actifs de l'OMPI en matière d'information (y compris l'information et les sources d'information) et de la manière de se conformer aux politiques, normes et procédures en matière de sécurité de l'information.

24. L'administrateur chargé de la sécurité de l'information, avec l'aide du Département de la gestion des ressources humaines, est responsable de l'élaboration et de la mise en œuvre d'un programme de sensibilisation à la sécurité de l'information visant à mieux faire connaître cette question aux fonctionnaires.

MESURES DE CONTROLE

Évaluation des risques

25. L'évaluation des risques consiste notamment à déterminer le degré de sensibilité et d'importance de l'information et les conséquences pour l'OMPI de la divulgation, de la modification ou de la destruction de l'information. Pour évaluer les risques, on peut appliquer soit les méthodes conventionnelles de détermination de l'incidence financière et opérationnelle d'une atteinte à la sécurité de l'information, soit des techniques d'évaluation moins formelles. Dans un processus d'évaluation des risques, il doit notamment être tenu compte des éléments suivants :

- la détermination d'un inventaire d'actifs en matière d'information qu'il convient de protéger;
- l'évaluation du niveau de sensibilité de l'information et des conséquences si l'information est divulguée;

- l'évaluation de l'importance de l'information et des conséquences pour les méthodes de gestion si l'information et les systèmes de traitement de l'information ne sont pas disponibles;
- la confirmation par la direction des risques qui seront acceptés, limités ou transférés;
- la mise au point d'une stratégie de contrôle des risques;
- la détermination de la conformité avec le classement de l'information à l'OMPI.

26. Il est de la responsabilité de la direction d'évaluer les risques encourus par l'OMPI en ce qui concerne la confidentialité, l'intégrité et la disponibilité de l'information et de prendre les mesures nécessaires pour limiter efficacement ces risques. Les mesures de contrôle des risques doivent porter sur l'information, les processus utilisés pour créer, modifier, communiquer ou diffuser cette information et l'environnement dans lequel ces processus sont mis en œuvre. Il conviendrait également de classer l'information, conformément aux normes de sécurité de l'OMPI, dans l'une des catégories suivantes :

- secrète;
- confidentielle;
- à usage interne uniquement;
- publique.

27. Le Guide des politiques de l'OMPI en matière de sécurité de l'information constitue un cadre de classement des niveaux de confidentialité, d'intégrité et de disponibilité de l'information et des prescriptions en matière de sécurité pour chaque niveau de classement.

Politiques en matière de sécurité de l'information pratique

28. Le Guide des politiques de l'OMPI en matière de sécurité de l'information décrit les politiques en matière de sécurité de l'information pratique. Il définit le cadre dans lequel s'inscrivent la stratégie, l'organisation et la mise en œuvre des politiques de l'OMPI en matière de sécurité de l'information, l'accent étant mis sur les techniques de mémorisation, de traitement et de transmission de l'information, ainsi que sur les méthodes administratives et opérationnelles de protection de cette information sous toutes ses formes, tant à l'intérieur qu'à l'extérieur de l'OMPI. Élaboré par l'administrateur chargé de la sécurité de l'information, ce guide est approuvé par le directeur général.

Normes en matière de sécurité de l'information

29. Le Guide des normes en matière de sécurité de l'information de l'OMPI établit les méthodes permettant d'atteindre les objectifs de sécurité visés dans le Guide des politiques de l'OMPI en matière de sécurité de l'information. Des lignes directrices spécifiques de sécurisation des plates-formes et des applications seront élaborées en fonction de ces normes. Élaboré et tenu à jour par l'administrateur chargé de la sécurité de l'information, ce guide est approuvé par le directeur des services informatiques.

Procédures en matière de sécurité de l'information

30. En vue de mettre en œuvre les politiques et normes de l'OMPI en matière de sécurité de l'information, il conviendra d'élaborer différentes procédures de sécurité. Elles viseront à définir étape par étape les actions à accomplir dans le cadre d'une activité particulière liée à la sécurité de l'information.

Procédures et directives dans chaque division

31. Chaque division doit mettre au point et tenir à jour des procédures et directives internes supplémentaires visant à appuyer les politiques globales en matière de sécurité de l'information, s'il y a lieu de répondre à des besoins spécifiques.

32. Le SCIT plénier est invité à prendre note des informations contenues dans le présent document

[Fin du document]