LE COIN DE LA SÉCURITÉ INFORMATIQUE

SECURITE

Quinze «petits trucs» pratiques à l'intention des utilisateurs du SIGNET

L'exploitation du SIGNET-D, qui constitue le volet non classifié/désigné du SIGNET, n'est autorisée que pour le traitement, le stockage ou la communication (transmission) d'information portant les mentions NON CLASSIFIÉ et PROTÉGÉ. Il ne faut PAS traiter les renseignements qui portent la mention PROTÉGÉ-DÉLICAT ou qui sont classifiés au niveau CONFIDENTIEL ou à un niveau supérieur au moyen du SIGNET-D, qui n'assure pas une protection adéquate à ce type de renseignements.

Les renseignements acheminés par l'intermédiaire du SIGNET-D sont transmis en clair, c'est-à-dire sans être chiffrés. Cela signifie qu'ils ne bénéficient d'aucune protection au moment où ils sont envoyés d'un endroit à un autre (par exemple, d'une mission à l'Administration centrale) ou d'un point à un autre du système (par exemple du poste de travail aux imprimantes), y compris par messagerie électronique. En outre, même lorsqu'un poste SIGNET-D semble fonctionner en mode autonome, il existe encore la possibilité d'un lien avec le réseau, par exemple par l'intermédiaire des imprimantes. Des programmes d'usage courant que l'on peut se procurer sans difficulté peuvent permettre de capter ou d'intercepter de l'information, par exemple des noms d'utilisateurs ou des mots de passe exploités pour accéder au SIGNET-D.

C'est aux employés qu'il revient d'assurer la protection des renseignements qu'ils traitent au moyen du système SIGNET. Voici les recommandations formulées par ISSC pour s'assurer de l'application des modalités adéquates et des précautions appropriées :

1. N'utilisez jamais le SIGNET-D pour traiter de l'information classifiée ou portant la mention PROTÉGÉ-DÉLICAT. On emploiera, pour traiter ces renseignements, un poste de travail autonome TEMPEST muni d'un disque dur amovible (à l'AC SEULEMENT), le SIGNET-C2, le système DUCS, ou un TÉLÉCOPIEUR protégé;

2. Ayez connaissance des consignes de sécurité applicable à l'utilisation du SIGNET-D pour le traitement de l'information importante mais non délicate, et de l'information délicate ;

3. Précisez, à l'intérieur de chaque message ou document traité, stocké ou transmis, la mention de classification ou de désignation qui s'applique;

4. Apposez, sur toute disquette contenant des renseignements d'un niveau de classification supérieur à NON CLASSIFIÉ, une étiquette indiquant le niveau le plus élevé de désignation ou de classification applicable aux données contenues sur la disquette. N'utilisez jamais dans un poste de travail du SIGNET-D une disquette contenant des renseignements protégés délicats ou classifiés.

5. Soyez conscients du fait que des personnes ne possédant pas de nom d'utilisateur ni de mot de passe peuvent accéder directement aux renseignement stockés sur le disque dur d'un poste de travail SIGNET-D.

6. Ne divulguez pas votre mot de passe et modifiez-le fréquemment;

7. Mettez fin à la séance en cours si vous avez l'intention de vous absenter de votre poste de travail et que ce dernier doit rester sans surveillance ;

[Une option connexe utile est l'option de protection avec mot de passe que l'on peut activer en même temps que le programme de mise en veille de Windows]

8. Assurez-vous de posséder des copies de réserve de vos fichiers de données et de vos applications, et de les conserver en un lieu distinct de votre poste de travail;

9. Appliquez les modalités prescrites pour ce qui concerne la destruction des disquettes contenant de l'information délicate. Il est utile de savoir que la commande Supprimer n'efface pas les données, mais ne fait que modifier le nom du fichier en en supprimant la première lettre, de sorte qu'une personne sachant y faire peut aisément récupérer les données avant qu'elles ne soient écrasées par l'introduction d'autres données;

10. Ne consultez pas les fichiers et les programmes pour lesquels vous ne possédez pas d'autorisation expresse d'accès, et incitez vos collègues à en faire autant;

11. Assurez-vous que les logiciels installés sur les serveurs et sur les postes de travail sont tous des logiciels autorisés, car l'exploitation de logiciels (y compris de logiciels que l'on continue d'exploiter alors que la période d'essai a pris fin) sans permis est illégale;

12. N'installez pas de modems et n'établissez pas de liaisons non autorisées avec d'autres ordinateurs ou d'autres réseaux;

13. Manipulez avec prudence toutes les disquettes qui proviennent de sources extérieures (ce qui comprend les disquettes provenant de votre voisin de bureau ainsi que les disquettes neuves préformatées dans des boîtes scellées), car elles pourraient contenir des codes nuisibles. Passez les disquettes au programme de détection de virus avant d'utiliser votre poste de travail;

14. Contrôlez périodiquement votre poste de travail pour déceler la présence de virus;

15. Signalez à ISSC les aspects de la sécurité qui vous préoccupent ainsi que les incidents liés à la sécurité, comme des tentatives d'intrusion ou la détection de virus.

Le *Bulletin du SIGNET* est publié une fois toutes les deux semaines par la Direction des services à la clientèle du SIGNET (STC) et diffusé au Canada et dans les missions à l'étranger à tous les fonctionnaires du ministère des Affaires étrangères et du Commerce international.

Les unités qui veulent faire paraître un avis dans le *Bulletin du SIGNET* sont priées de nous en faire parvenir le texte avec une note de service signée par leur directeur. Tous les lecteurs sont invités par ailleurs à envoyer à la boîte à suggestion du SIGNET les articles qu'ils désirent faire publier.