Industrie Canada Industry Canada

Direction générale des services à la clientèle
Secteur de l'agent principal de l'information
Sécurité de la technologie de l'information

Sécurité TI

Sécurité : la clé des TI

http://icweb.ic.gc.ca/946-5555
(613) 946-5555
Courriel : CIOAPI@ic.gc.ca

Canada

Qui sommes-nous?

Les spécialistes de la Sécurité de la technologie de l'information (TI) veillent à ce que les employés d'Industrie Canada puissent travailler dans un environnement technique sécurisé.

L'équipe de la Sécurité de la TI donne des conseils pratiques et assure l'encadrement nécessaire afin que les réseaux informatiques demeurent sécurisés et exempts de virus.

Notre mission

La Sécurité de la TI a pour mission :

- de maintenir des mesures de sécurité de la technologie de l'information et des communications qui soient raisonnables, efficaces et opportunes;
- de prévoir les besoins des employés d'IC et d'établir un cadre sécurisé pour bâtir l'infrastructure;
- de prévenir les menaces et les risques informatiques et de limiter ou atténuer leurs effets;
- de réagir de façon professionnelle et en temps opportun aux incidents qui pourraient compromettre la sécurité de tous les éléments dont la Sécurité de la TI est responsable (personnel, données et matériel).

Notre orientation

Le réseau informatique d'IC est un outil de travail essentiel. La Sécurité de la TI a donc mis en place des mécanismes de protection pour qu'il fonctionne sans problèmes ni interruptions.

Les objectifs de la Sécurité de la TI consistent :

- à améliorer continuellement les pratiques exemplaires en matière de sécurité de la TI;
- à informer les employés des mesures de protection contre les virus ainsi que des alertes au virus lorsque nécessaire;
- à renseigner les employés sur la façon d'assurer la sécurité des documents électroniques protégés;
- à aider les diverses équipes de travail à planifier les évaluations de la menace et des risques ainsi que les énoncés de la nature délicate;
- à promouvoir la communication sécurisée;
- à organiser des séances de sensibilisation portant sur divers sujets pour les nouveaux employés, les différentes équipes de travail, etc.

Conseils pratiques de sécurité de la TI

Mots de passe

Votre mot de passe restreint l'accès à votre poste de travail. Voici donc quelques conseils à ce sujet.

À faire

- Verrouiller l'accès à votre ordinateur au moyen d'un mot de passe, lorsque vous vous absentez de votre bureau.
- Choisir un mot de passe difficile à deviner (à sept caractères, alphanumérique, pas de mots provenant du dictionnaire).

À ne pas faire

- Laisser votre mot de passe écrit près de votre ordinateur.
- Simplement ajouter un numéro à la fin de votre mot de passe, lorsqu'on vous demande de le changer.
- Donner votre mot de passe à quelqu'un.

Polluriels (courriels non sollicités)

Des polluriels qui annoncent un éventail de produits et services, dont du matériel pornographique, s'introduisent chaque jour dans le réseau d'IC.

Vous pouvez être tenté de retirer votre nom de la liste des destinataires des polluriels en répondant à ces derniers. Toutefois, cela peut entraîner une augmentation des polluriels que vous recevrez.

Nous encourageons plutôt les employés d'IC :

- à supprimer les polluriels;
- à réduire les possibilités de recevoir des polluriels;
- à se plaindre auprès du fournisseur de service Internet avec qui l'expéditeur des polluriels fait affaire.

Note : Sous la rubrique Trucs, section MS Outlook, du site Web du Centre d'appels TI-API, vous trouverez des conseils sur la façon de vous débarrasser des polluriels qui vous sont adressés et de porter plainte auprès du fournisseur de service Internet de l'auteur de ces messages.

Sécurité Internet

Industrie Canada a une déclaration sur l'utilisation d'Internet afin de préserver la sécurité du réseau informatique.

Vous devez lire et accepter les termes de cette politique qui s'affiche périodiquement à l'écran de votre poste de travail. Elle expose les règlements interdisant le piratage ainsi que la consultation, l'élaboration et la transmission de contenu pornographique et de littérature haineuse. L'utilisation d'Internet est surveillée et la dérogation à la Déclaration sur l'utilisation d'Internet à Industrie Canada portera à conséquence.

Politique d'accès à distance

Il vous incombe de vous assurer que vous utilisez une solution d'accès à distance protégé. Voici quelques règles à suivre à cet effet :

1. Aucun poste de travail branché au réseau ministériel ne devrait être doté d'un modem individuel. Les employés dont le besoin d'accès à distance est fondé doivent présenter une courte justification à la Sécurité de la TI, et collaborer avec celle-ci pour assurer que le lien d'accès soit sécurisé.

2. Tous les logiciels d'accès à distance doivent être conservés dans une zone protégée, et dotés de mesures de protection adéquates.

3. Les ordinateurs qui se connectent à distance à notre réseau au moyen d'une connexion Internet haute vitesse, doivent être munis d'un logiciel anti-virus mis à jour régulièrement et d'un coupe-feu personnel.

Ordinateurs portatifs

Les ordinateurs portatifs sont très recherchés par les voleurs à cause de leur taille, de leur valeur et de la possibilité d'accès à des renseignements protégés. Voici quelques façons d'assurer la sécurité de votre ordinateur portatif.

1. Attachez l'ordinateur au moyen d'un câble antivol.
2. Installez un dispositif de localisation.
3. Dotez l'ordinateur d'un mot de passe difficile à deviner.
4. Faites régulièrement une copie de secours des données qui se trouvent sur le disque dur de votre ordinateur.
5. Utilisez une méthode de chiffrement pour protéger vos données.
6. Gardez l'ordinateur dans un classeur ou un coffre-fort lorsque vous ne l'utilisez pas.
7. Ayez toujours en main votre ordinateur portatif lorsque vous montez à bord d'un avion; assurez-vous que sa pile soit chargée.

Attaques de virus

Tous les incidents reliés aux virus sont considérés urgents. Si vous avez un virus sur votre ordinateur :

- coupez immédiatement ce dernier du réseau en débranchant le câble qui ressemble à un cordon téléphonique;
- communiquez avec le Centre d'appels TI-API pour obtenir d'autres instructions.

Alertes TI

Si un virus menace le réseau d'IC, une alerte au virus sera affichée sur le site ICWeb et sur celui du Centre d'appels TI-API.

Il y a trois niveaux d'alerte au virus : vert, jaune et rouge; chacun enclenche un protocole bien précis de protection contre les virus informatiques.

L'alerte rouge signifie que le réseau est l'objet d'une attaque virale; tous les employés doivent éteindre leur ordinateur immédiatement.

Infrastructure à clé publique (ICP)

Tous les employés d'IC peuvent obtenir une clé ICP; celle-ci est nécessaire pour sécuriser les courriels et protéger les données.

Évaluations de la menace et des risques

Il faut communiquer avec la Sécurité de la TI avant d'implémenter toute application en ligne, nouvelle ou mise à jour, au sein de votre équipe de travail. La Sécurité de la TI vous aidera à planifier les évaluations de la menace et des risques ainsi que les énoncés de la nature délicate.

Sécurité des communications

La sécurité des communications (COMSEC) est la responsabilité de la Sécurité de la TI. C'est au personnel de cette équipe que vous devez vous adresser si vous avez besoin de téléphones STU-III, de comptes de réseau privé virtuel et d'autres moyens de communication sécurisés.

Sensibilisation à la sécurité de la TI

La Sécurité de la TI offre des séances de sensibilisation à la sécurité de la TI traitant de divers sujets spécialisés.

Sur demande, il est possible d'organiser des séances de sensibilisation pour les nouveaux employés, ou encore des présentations adaptées tenues à l'occasion de réunions du personnel de votre équipe de travail, ou de journées de réflexion.

Comment communiquer avec nous

Vos commentaires, préoccupations, questions ou suggestions sont les bienvenus. Pour en apprendre davantage sur les sujets abordés dans ce dépliant, n'hésitez pas à communiquer avec nous.

Adresse : Immeuble C.D. Howe
235, rue Queen
Ottawa (Ontario) K1A 0H5

Télécopieur : (613) 946-3367

Site Web : http://icweb.ic.gc.ca/946-5555

Pour obtenir des renseignements ou pour des questions urgentes

Téléphone : (613) 946-5555

Courriel : CIOAPI@ic.gc.ca

Pour signaler un incident de sécurité ou pour discuter de questions confidentielles

Téléphone : (613) 998-3209 ou (613) 957-8625

Courriel : SecuriteTI@ic.gc.ca

La sécurité de la TI, chacun en est responsable.

53662B
Mars 2002

Contient 10 p.100 de matières recyclées