Technologie de l'information
Guide de la sécurité
à l'intention du personnel d'ISTC

Industrie, Sciences et Technologie Canada
Industry, Science and Technology Canada

Canada

QA76.9/.A25/I83
Canada. Industry, Science
ISTC staff handbook on
information technology
BTXY c. 2 aa ISTC

DATE DUE - DATE DE RETOUR

ISTC 1551 (2/90)

INDUSTRY CANADA/INDUSTRIE CANADA
61218

Technologie de l'information
Guide de la sécurité
à l'intention du personnel d'ISTC

© Ministre des Approvisionnements et Services Canada 1992

Tous droits réservés. Aucune partie de cet ouvrage ne peut être reproduite, emmagasinée dans un système d'extraction ou transmise sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et l'enregistrement, sans l'autorisation de la Direction générale de la gestion de l'information, à ISTC.

PU 0281-91-03

AVANT-PROPOS

La dépendance croissante à l'égard des ordinateurs et des services de télécommunications dans l'ensemble d'Industrie, Sciences et Technologie Canada (ISTC) nous oblige à protéger convenablement nos ressources documentaires. Le présent guide fait partie d'une série de trois documents qui fournissent les renseignements dont a besoin tout fonctionnaire d'ISTC pour sauvegarder ces ressources.

Ce n'est que grâce à votre appui, c'est-à-dire si vous reconnaissez que la sécurité est une responsabilité individuelle et primordiale, que nous pourrons continuer à protéger convenablement nos renseignements. Je vous encourage à suivre les indications de ce guide et à ne pas relâcher l'attention que vous prêtez aux exigences de sécurité de votre travail.

Le sous-ministre,

H.G. Rogers

REMERCIEMENTS

Les trois guides ont été rédigés en s'appuyant sur des ouvrages de référence provenant des organismes suivants : la Direction des systèmes financiers et de programmes, la Direction générale du contrôleur, la Direction générale de la gestion de l'information et le Bureau fédéral de développement régional (Québec). En outre, les membres du Groupe de coordination de la technique des gestionnaires de services d'informatique ont été consultés.

Le Programme remercie spécialement le comité ministériel d'organisation pour son aide précieuse à la préparation de ces guides.

TABLE DES MATIÈRES

1. Introduction **1**
Objet et portée 1
Ouvrages de référence 3

2. Responsabilités en matière de sécurité **4**
Ensemble du personnel 4
Gestionnaire du centre de responsabilité 5
Gestionnaire des installations communes 5
Responsable des systèmes informatiques 5
Agent de sécurité du Ministère 6
Coordonnateur de la sécurité informatique 6
Administrateur local de la sécurité 6

3. Sécurité du personnel **7**
Autorisation de sécurité et vérification approfondie de la fiabilité 7
Répartition des tâches 8
Formation en matière de sécurité 8
Abandon d'un poste 9

4. Sécurité matérielle **10**
Zones de sécurité et zones de travail 10
Accès aux zones de sécurité 10

5. Sécurité de l'information **12**
Accès sélectif 12
Information et documents 12
Information classifiée ou désignée 12
Mentions sur les documents classifiés ou désignés 13
Exigences en matière de protection des documents classifiés ou désignés 15
Déclassification et reclassification des documents 16
Élimination des rebuts de documents classifiés ou désignés 16

6. Administration de la sécurité informatique **18**
Procédures écrites 18

7. Virus 19
Précautions de base 19
Que faire en cas de détection d'un virus ? 21

8. Contrôles de l'accès aux systèmes informatiques 22
Contrôles matériels de l'équipement et des données 22
- Protection du matériel, des logiciels et des données 22
- Identificateurs 22
- Mots de passe 23
- Administration des contrôles d'accès 24
- Suspension de l'accès 25
- Sortie automatique du système 25

Sauvegarde de documents lisibles par machine 26
- Supports amovibles lisibles par machine 26
- Disques durs fixes 26
- Logiciel original 28

Sécurité des communications électroniques et sécurité informatique ... 29
- Transmission d'information de nature délicate 29
- *Tempest* 29
- Cryptage 30
- Téléchargement de fichiers 31
- Lignes commutées 31

9. Maintenance du matériel et des logiciels 32
Autorisation 32
Maintenance sur place 32
Maintenance hors du lieu de travail 33

10. Entretien des ordinateurs et des supports lisibles par machine 34
Entretien et nettoyage 34

11. Vérification de la conformité 36
Inspections et vérifications 36
Documents et tableau d'*éliminables* 36
Rapport des incidents de sécurité 37

12. Copies de sauvegarde et procédures d'éventualité 39
Sauvegardes quotidiennes 39
Stockage des données et copies de sauvegarde des logiciels 40
Récupération des donnés 41
Procédures d'éventualité 41

13. Droits d'auteur 42
Loi sur le droit d'auteur 42
Responsabilités des membres du personnel 42

14. Ressources 43
Références 43
Personnel-ressource 44

Glossaire 45

Index 53

Observations 57

1. INTRODUCTION

Objet et portée

Le présent manuel est destiné à tous les employés qui utilisent des ordinateurs, notamment aux gestionnaires, aux superviseurs, aux employés embauchés pour une durée indéterminée et aux employés temporaires, aux étudiants et aux entrepreneurs de tous niveaux. Il décrit les normes de sécurité informatique en vigueur au sein d'Industrie, Sciences et Technologie Canada (ISTC) et propose aux employés des façons de protéger l'information et les biens d'équipement du Ministère. Les normes et les lignes directrices énoncées dans le présent document s'applique à la plupart des situations auxquelles les employés pourraient être confrontés, et visent toutes les applications et tout l'équipement utilisés par ISTC.

Quiconque travaille pour le compte d'ISTC **doit** apprendre et respecter les normes de sécurité informatique. Si, en lisant ce manuel, vous vous butez à des termes que vous ne comprenez pas, consultez le glossaire en fin d'ouvrage.

Afin de reconnaître facilement les normes de sécurité impératives du gouvernement et du Ministère, le verbe **devoir** est mis en caractères gras comme c'est le cas ici, dans les énoncés reprenant des normes. Il existe de nombreuses façons de respecter les normes de sécurité, et les gestionnaires locaux peuvent décider de ce qui convient le mieux pour leur lieu de travail. Les lignes directrices recommandent des démarches en vue de résoudre des problèmes de sécurité, et dans ce cas, le verbe « pouvoir » est utilisé au présent ou au conditionnel, et le verbe « devoir » au conditionnel.

Étant donné qu'il porte sur la sécurité informatique, le présent manuel ne reprend des procédures de sécurité générales décrites dans le *Guide sur la politique et les procédures en matière de sécurité* d'ISTC que lorsqu'elles sont nécessaires à des fins de clarification. Il ne remplace pas les procédures de sécurité informatique propres à chaque lieu de travail.

Si vous ne comprenez pas certains concepts ou sujets, ou si vous désirez de plus amples renseignements, consultez votre superviseur, le gestionnaire d'installations communes, le responsable des systèmes informatiques ou l'administrateur local de la sécurité. S'ils ne peuvent vous aider, il faudrait soumettre votre problème au gestionnaire du centre de responsabilité, qui pourra consulter le coordonnateur de la sécurité informatique, la Direction générale de la gestion de l'information ou l'agent de sécurité du Ministère à l'Administration centrale.

Le présent manuel fait partie d'une série de trois volumes. ISTC a également publié *Technologie de l'information — Guide de la sécurité à l'intention des gestionnaires des installations communes et des responsables des systèmes informatiques* d'ISTC et *Technologie de l'information — Guide de la sécurité à l'intention des gestionnaires des centres de responsabilités* d'ISTC. Vous pouvez consulter ces derniers pour obtenir de plus amples renseignements. Ces deux manuels comprennent un index général pour toute la série.

Ouvrages de référence

Le présent manuel s'inspire des sources suivantes :

- *Gestion de l'information et gestion administrative — Sécurité,* manuel du Conseil du Trésor qui comprend la Politique concernant la sécurité du gouvernement et les normes provisoires en matière de sécurité informatique;
- les bulletins sur la sécurité du Conseil du Trésor;
- *Guide sur la politique et les procédures en matière de sécurité* d'ISTC, qui englobe le *Guide de classification et de désignation* (novembre 1991) et les directives du sous-ministre d'ISTC, notamment la directive 102-1 — Sécurité de l'informatique.

2. RESPONSABILITÉS EN MATIÈRE DE SÉCURITÉ

Ensemble du personnel

Dans le cadre de leurs fonctions, tous les employés d'ISTC doivent protéger l'information et l'équipement en leur possession contre toute utilisation abusive, vol ou dommage délibéré, et prendre toutes les précautions raisonnables contre les dommages accidentels. L'équipement informatique et les données qu'il contient sont vulnérables aux dommages causés par des personnes négligentes ou non informées et par des saboteurs. Les articles de valeur, comme les ordinateurs portatifs et les imprimantes, et les fournitures renouvelables, comme les disquettes, tentent les voleurs. Les documents de nature délicate peuvent aussi intéresser les gens curieux ou malveillants.

Certaines responsabilités en matière de sécurité informatique incombent à tous employés d'ISTC. Ces derniers **doivent** :

- respecter les règles en vigueur sur le lieu de travail lorsqu'ils entrent dans les zones de sécurité;
- mettre sous clé l'équipement portatif, les supports lisibles par machine et les documents de nature délicate quand le lieu de travail n'est pas surveillé;
- éviter de divulguer leurs mots de passe et les changer périodiquement;
- aider à éliminer les défaillances permettant un accès non autorisé à l'information en les signalant immédiatement;
- suivre les procédures antivirus et n'utiliser que des logiciels exempts de virus;
- contrôler les photocopies et les imprimés classifiés ou désignés;

- éliminer correctement les rebuts de documents classifiés ou désignés;
- respecter les lois concernant les droits d'auteur;
- faire régulièrement des copies de sauvegarde des logiciels et des données;
- signaler immédiatement les incidents de sécurité.

Vous recevrez une explication complète de vos responsabilités en matière de sécurité informatique au cours de votre séance d'information en matière de sécurité (*voir* Formation en matière de sécurité, à la section 3).

Gestionnaire du centre de responsabilité

Le gestionnaire de chaque centre de responsabilité détermine les mesures à prendre pour protéger l'équipement et les systèmes informatiques ainsi que de toutes les données qu'ils contiennent, et s'assure que tous les employés suivent les procédures de sécurité. Les gestionnaires de centres de responsabilité peuvent déléguer ces tâches à d'autres gestionnaires, aux administrateurs locaux de la sécurité ou aux responsables des systèmes informatiques.

Gestionnaire des installations communes

Le gestionnaire de chaque installation commune détermine les mesures à prendre pour protéger une installation de traitement à utilisateurs multiples, comme un réseau local, un gros ordinateur ou un mini-ordinateur, et s'assure que tous les employés qui y ont accès suivent les procédures de sécurité. Si un administrateur local de la sécurité a été nommé, celui-ci assumera certaines des tâches de sécurité qui lui auront été déléguées par le gestionnaire des installations communes.

Responsable des systèmes informatiques

Le responsable de chaque système informatique détermine les mesures à prendre pour le protéger et s'assure que tous les employés qui utilisent le système et ses données respectent les procédures de sécurité.

Agent de sécurité du Ministère

L'agent de sécurité du Ministère est le directeur, Sécurité et Sûreté, Direction générale des services administratifs, à l'Administration centrale, à Ottawa. Cet agent assume des responsabilités particulières en matière de sécurité, responsabilités que lui a déléguées le sous-ministre. Il doit notamment s'assurer qu'ISTC respecte la politique sur la sécurité du gouvernement ainsi que les normes opérationnelles du gouvernement. C'est à lui que devraient être adressées les questions relatives à l'interprétation et à l'exécution de la politique ministérielle en matière de sécurité.

Coordonnateur de la sécurité informatique

Le coordonnateur de la sécurité informatique, qui relève de la Direction générale de la gestion de l'information à l'Administration centrale, aide et conseille l'agent de sécurité du Ministère. Le coordonnateur assume des fonctions particulières dans les domaines de la formation en matière de sécurité et de la vérification de la conformité, et conseille les employés sur la sécurité informatique. Il évalue également les menaces et les risques, et des plans d'urgence pour les importants systèmes informatiques du Ministère exploités sur des ordinateurs administrés par la Direction générale de la gestion de l'information.

Administrateur local de la sécurité

Un gestionnaire local peut attribuer certaines fonctions locales de sécurité informatique à un membre du personnel. S'il n'y a aucun administrateur local de la sécurité sur votre lieu de travail, les responsabilités en matière de sécurité informatique locale seront assumées par un gestionnaire des installations communes ou un responsable des systèmes informatiques.

3. SÉCURITÉ DU PERSONNEL

Autorisation de sécurité et vérification approfondie de la fiabilité

L'agent de sécurité du Ministère procédera à des autorisations de sécurité et à des vérifications approfondies de la fiabilité pour tous les employés — gestionnaires, superviseurs, employés embauchés pour une durée indéterminée ou employés temporaires, étudiants et entrepreneurs — qui doivent avoir accès à de l'information classifiée ou désignée dans le cadre de leur travail. Il s'agit notamment d'administrateurs de réseaux locaux, de programmeurs, de pupitreurs et d'utilisateurs de réseau.

Vous **devez** remplir les documents requis pour l'autorisation de sécurité ou la vérification approfondie de la fiabilité sur demande.

Votre attestation de sécurité sera vérifiée :

- par le responsable des systèmes informatiques ou le gestionnaire des installations communes avant de vous donner l'accès;
- par le gestionnaire responsable de votre contrat avant l'entrée en vigueur du contrat;
- par votre superviseur éventuel avant votre embauche;
- par votre superviseur avant que ne vous soient assignées de nouvelles tâches nécessitant le traitement d'information classifiée ou désignée.

Les procédures d'autorisation de sécurité et de vérification de la fiabilité sont décrites dans le *Guide sur la politique et les procédures en matière de sécurité* d'ISTC.

Répartition des tâches

Pour réduire le risque de dommages aux documents et à l'équipement et d'infractions et de violations de la sécurité, personne ne devrait être responsable de tous les aspects d'un processus important. En fait, certaines responsabilités ne devraient pas être assumées par un même titulaire de poste. A moins que votre lieu de travail ne soit très petit et que vos collègues et vous-même n'utilisiez que des micro-ordinateurs autonomes, vous ne devriez assumer qu'une seule des responsabilités suivantes à la fois :

- l'exploitation de l'équipement;
- la bibliothèque de bandes;
- la programmation;
- le contrôle de la saisie et des sorties.

Formation en matière de sécurité

Les gestionnaires d'installations communes et les responsables des systèmes informatiques doivent veiller à ce que les employés soient informés de leurs responsabilités et des normes ministérielles en matière de sécurité informatique. Vous **devez** participer à de telles séances d'information :

- au moment de votre embauche;
- au cours de l'attribution de nouvelles tâches;
- au cours de l'adoption de nouvelles procédures de sécurité informatique.

Pour approfondir et rafraîchir vos connaissances en sécurité informatique, vous devriez également assister régulièrement à des séances d'information sur la sécurité.

Abandon d'un poste

Au moment où votre contrat prend fin, au moment d'une promotion ou d'une mutation, ou lorsque vous laissez un poste au sein d'ISTC pour toute autre raison, vous **devez** vous soumettre aux procédures suivantes :

- transférer ou envoyer aux archives les documents qui doivent être conservés;
- détruire ou effacer les documents devenus inutiles;
- rendre les clés de la porte, des armoires et du bureau;
- donner les clés de cryptage;
- rendre tout le matériel informatique, tous les logiciels et documents d'ISTC;
- fournir toute information dont le gestionnaire des installations communes a besoin pour annuler vos mots de passe et votre identificateur et fermer votre compte d'utilisateur.

Si vous quittez le Ministère, vous **devez** remplir la formule *Formalités de fin d'emploi,* conformément à la procédure énoncée dans le *Guide sur la politique et les procédures en matière de sécurité* d'ISTC.

4. SÉCURITÉ MATÉRIELLE

Vous **devez** porter un laissez-passer valide quand vous vous trouvez dans les locaux d'ISTC. Vous **devez** le montrer sur demande.

Zones de sécurité et zones de travail

Une zone de sécurité est une zone du lieu de travail fermée ou isolée en vue de protéger l'équipement important et l'information de nature délicate. L'accès aux zones de sécurité est strictement limité aux employés autorisés qui doivent s'y rendre dans le cadre de leurs fonctions.

Les fournitures renouvelables et l'équipement informatique non indispensables aux activités peuvent être conservés dans les zones de travail normales, où l'accès n'est pas limité. Pour une meilleure sécurité dans les zones de travail, vous devriez garder les articles attirants et l'équipement de valeur dans des armoires ou des bureaux fermés à clef. Si cela s'avère impossible, l'équipement de valeur devrait être fixé en permanence au mobilier à l'aide de câbles ou de boulons.

Accès aux zones de sécurité

L'accès des visiteurs aux zones de sécurité, notamment du personnel de nettoyage et de maintenance, est strictement contrôlé. Selon les procédures établies par le gestionnaire local, ces personnes devront peut-être signer un formulaire à leur arrivée et à leur départ. Vous **devez** accompagner tous les visiteurs que vous invitez dans une zone de sécurité ou désigner une escorte.

Si vous notez la présence d'une personne non accompagnée, peut-être non autorisée, dans une zone de sécurité, vous devriez chercher à savoir ce qu'elle fait, et au besoin, la reconduire vous-même à l'extérieur de la

zone de sécurité ou encore appeler un collègue qualifié ou un administrateur de la sécurité pour le faire.

L'entrée délibérée d'une personne non autorisée dans une zone de sécurité constitue une violation de la sécurité. Vous **devez** signaler à l'administrateur local de la sécurité, au gestionnaire local et à l'agent de sécurité du Ministère toute violation ou infraction dont vous avez connaissance ou que vous soupçonnez.

5. SÉCURITÉ DE L'INFORMATION

Accès sélectif

L'accès à l'information de nature délicate **doit uniquement** être accordé aux personnes qui possèdent l'autorisation de sécurité adéquate et qui ont besoin de l'information dans le cadre de leur travail. L'accès à l'information de nature délicate est une exigence professionnelle particulière, et non un privilège reflétant le rang.

Information et documents

Quand vous créez un document, vous recueillez de l'information sous une forme lisible, lisible par machine ou décodable sur papier, ou sur des supports lisibles par machine comme :

- des disquettes;
- des bandes;
- des disques durs fixes ou amovibles;
- des disques optiques;
- des microfiches et microfilms;
- des écrans vidéo.

Information classifiée ou désignée

L'information doit être *classifiée* CONFIDENTIEL, SECRET ou TRÈS SECRET si elle est d'intérêt national et ne peut être diffusée au public en vertu de la *Loi sur l'accès à l'information*. En d'autres termes, si la diffusion non autorisée, la suppression, la modification ou l'interruption de toute information particulière risque de menacer la sécurité publique, la confiance du public ou les relations internationales, cette information doit être classifiée. Par exemple, la correspondance diplomatique traitant d'une entente d'échange technologique avec un gouvernement étranger contient de l'information classifiée. Les documents confidentiels du Cabinet, notamment les présentations au Conseil du Trésor, constituent également de l'information classifiée.

L'information doit être *désignée* PROTÉGÉ si sa diffusion, l'interruption de sa diffusion ou sa modification risque de nuire à des particuliers ou à des groupes précis, mais pas à l'intérêt national. Par exemple, les rapports d'évaluation du personnel et les propositions de sociétés pendant une mise en concurrence contiennent de l'information désignée. Certains renseignements désignés ne sont pas nécessairement de nature délicate — les dates de naissance, par exemple — mais ils doivent faire l'objet d'une protection plus attentive car leur utilisation est soumise à des restrictions en vertu de la loi. Certains renseignements désignés sont de nature très délicate car leur diffusion, l'interruption de leur diffusion ou leur modification risque de menacer la réputation, la position concurrentielle ou la sécurité physique d'un particulier, d'une société ou d'un groupe.

Vous **devez** protéger l'information classifiée ou désignée en fonction de sa nature délicate.

Le *Guide de classification et de désignation* d'ISTC indique comment attribuer les niveaux de sécurité adéquats aux documents. Consultez votre superviseur ou l'administrateur local de la sécurité pour obtenir de l'aide.

Mentions sur les documents classifiés ou désignés

Une mention bien en vue **doit** être apposée pour indiquer que les documents sont classifiés ou désignés afin que leurs utilisateurs soient toujours informés de la nature de l'information qu'ils contiennent. La mention **doit** être apposée au moment de la création du document.

Si vous créez un document contenant de l'information classifiée ou désignée, celui-ci **doit** être marqué comme suit :

- pour les documents-papier SECRET ou TRÈS SECRET — sur la couverture et sur chaque page;

- pour les documents-papier PROTÉGÉ et CONFIDENTIEL — sur la couverture et la première page, et sur chaque page si les pages peuvent être séparées facilement;
- pour les écrans de données et les microtextes contenant de l'information de nature délicate de tout niveau de sécurité — sur chaque écran ou texte où l'information de nature délicate est consignée.

Les documents informatiques contenant de l'information de nature délicate devraient être rédigés de sorte que la classification ou la désignation s'affiche :

- à l'écran, quand le document est extrait;
- automatiquement sur les imprimés, conformément au niveau de sécurité.

Quand vous imprimez des documents de nature délicate ou les transférez sur support lisible par machine, vous **devez,** pour préciser le niveau de sécurité, utiliser des chemises ou des étiquettes d'une des couleurs symboliques suivantes :

- TRÈS SECRET — Cadre rouge et croix rouge sur l'étiquette ou au recto et au verso de la chemise
- SECRET — Rouge
- CONFIDENTIEL — Vert
- PROTÉGÉ — Bleu

Quand vous trouvez un document contenant de l'information de nature délicate sur lequel n'est pas mentionné le niveau de désignation ou de classification adéquat :

- si vous êtes le détenteur de ce document, vous **devez** le classifier ou le désigner vous-même, sans oublier de l'entreposer correctement après avoir apposé la mention de sécurité;
- si vous n'êtes pas le détenteur du document, vous **devez** le remettre à son détenteur, à votre superviseur ou à l'administrateur local de la sécurité pour qu'il y appose la mention appropriée et le range convenablement.

Exigences en matière de protection des documents classifiés ou désignés

Les exigences en matière de protection des documents classifiés et des documents désignés sont énoncées à l'annexe F de la directive du sous-ministre 70-1 dans le *Guide sur la politique et les procédures en matière de sécurité* d'ISTC. La plupart des employés auront à manipuler des documents dont l'information désignée ne sera pas de nature très délicate. Si vous avez fini de travailler avec les documents ou les supports amovibles lisibles par machine contenant de l'information désignée, ou encore si vous interrompez votre travail, vous **devez** les ranger dans des armoires fermées à clef. Cependant, vous **devez** ranger les documents classifiés ou de nature très délicate dans des coffres de sécurité adéquats approuvés comme : un meuble-classeur en acier, doté d'une barre de sécurité et d'un cadenas à combinaison Sargeant & Greenleaf.

L'accès aux données emmagasinées dans des ordinateurs et aux systèmes d'information classifiés ou désignés est accordé uniquement aux utilisateurs autorisés (*voir* chapitre 8, Contrôle de l'accès aux systèmes informatiques). Vous **ne devez pas** imprimer des documents classifiés ou désignés sur des imprimantes situées dans des endroits où des personnes non autorisées peuvent voir l'imprimé.

Consultez votre superviseur, l'administrateur local de la sécurité ou le gestionnaire local si vous avez besoin d'aide ou de plus amples renseignements.

Déclassification et reclassification des documents

Quand les circonstances changent et que des documents de nature délicate ne doivent plus être protégés, leur auteur, la personne désignée par lui ou encore celle qui agit en son nom **doit** les déclassifier ou les reclassifier. Vous devriez passer en revue régulièrement les documents de nature délicate en votre possession afin de vous assurer que leur niveau de sécurité actuel est correct.

Élimination des rebuts de documents classifiés ou désignés

Vous **devez** vous assurer que les documents classifiés ou désignés désormais inutiles sont détruits de sorte qu'aucune information de nature délicate ne puisse être récupérée par une personne non autorisée. Le personnel des régions **doit** prévoir leur élimination avec l'administrateur local de la sécurité. L'Administration centrale **doit** organiser l'élimination de concert avec la Direction de la sécurité et de la sûreté.

Vous **devez** faire détruire les documents-papier, les supports lisibles par machine endommagés comme les disquettes et les bandes, et les rubans d'imprimante et les papiers carbone ayant servi à produire des documents de nature délicate. Le déchiquetage, le paillage et le brûlage sont tous de bonnes méthodes permettant d'éliminer les rebuts de documents classifiés et des documents désignés.

Il peut arriver qu'un ordinateur ayant été utilisé pour traiter de l'information de nature délicate doive être converti à d'autres utilisations. Avant d'utiliser un disque dur à d'autres fins, vous **devez** en supprimer tous les documents de nature délicate. Il est recommandé d'utiliser des logiciels qui effacent ou écrasent l'information en la détruisant complètement. Si le disque dur est endommagé ou inutilisable, il peut être impossible de l'effacer et peut-être faudra-t-il le détruire. Consultez l'administrateur local de la sécurité, le gestionnaire des installations communes ou le coordonnateur de la sécurité informatique qui vous recommandera les produits à utiliser et vous donnera des conseils.

6. ADMINISTRATION DE LA SÉCURITÉ INFORMATIQUE

Procédures écrites

Chaque système d'information, base de données, installation partagée ou lieu de travail utilisant des ordinateurs **doit** disposer de procédures écrites portant sur la sécurité informatique.

Consultez les procédures locales de sécurité pour obtenir des renseignements sur les sujets suivants :

- les responsabilités;
- le rapport des incidents de sécurité;
- le contrôle de l'accès à l'équipement informatique et aux données, notamment aux zones de sécurité, aux mots de passe, aux identificateurs et au cryptage;
- le stockage et la transmission de documents et de données;
- la prévention des virus;
- les répertoires, journaux et autres documents informatiques;
- le contrôle de la configuration;
- le contrôle de l'intégrité;
- les copies de sauvegarde des données et du logiciel;
- les bibliothèques;
- les plans d'urgence;
- la maintenance et le transfert du contrôle au personnel d'entretien;
- la mise en route et l'arrêt de l'équipement;
- les pannes et le retour à l'exploitation normale du système;
- l'impression et la diffusion de documents de nature délicate.

7. VIRUS

Un virus est un programme destructif qui peut être chargé sur un ordinateur de deux façons :

- délibérément, par une personne malveillante ou hostile qui désire interrompre ou détruire le système;
- par inadvertance, par une personne qui n'a pas respecté les règles de sécurité.

Les virus se reproduisent et s'ajoutent à d'autres fichiers, programmes ou disquettes, et ils se propagent dès que quelqu'un télécharge un fichier ou un programme infecté ou encore utilise une disquette infectée. Les virus sont parfois conçus pour produire leur effet à la suite d'une opération informatique prévisible, comme le changement d'une date ou une autre opération ordinaire.

Les virus peuvent endommager ou détruire les données, les logiciels et le matériel informatique. Ils sont particulièrement destructeurs quand ils contaminent un réseau ou un gros ordinateur.

Précautions de base

Il n'existe aucune façon pratique d'immuniser les ordinateurs contre les virus. Toutefois, en respectant les normes de sécurité établies, il est presque possible de réduire le risque à néant. Vous **devez** utiliser systématiquement un récent programme recommandé de détection des virus :

- régulièrement, pour tous les supports lisibles par machine en votre possession, notamment les disquettes et les bandes, les disques durs des serveurs, les disques durs amovibles, les micro-ordinateurs et les ordinateurs portatifs;

- avant de copier et d'utiliser toute disquette, notamment celles provenant de votre ordinateur familial, et le nouveau logiciel de série autorisé;
- avant d'utiliser tout fichier et programme reçus par ligne de télécommunications;
- avant d'utiliser le nouvel équipement ou encore l'équipement qui revient de la maintenance.

Quand vous obtenez des disquettes ou des programmes de sources extérieures, vous **devez** :

- utiliser uniquement du logiciel vérifié, ne contenant aucun virus, en particulier quand vous utilisez de l'équipement d'ISTC hors du lieu de travail;
- ne jamais utiliser des programmes dont vous ne connaissez pas l'origine, notamment des copies illégales de logiciel, sur de l'équipement d'ISTC.

Quand vous accédez à des systèmes extérieurs comme des tableaux d'affichage, vous **devez** d'abord consulter le gestionnaire des installations communes. Il est préférable d'accéder aux systèmes publics uniquement à partir d'un micro-ordinateur autonome ou de télécharger les fichiers uniquement sur des disquettes qui seront vérifiées avant l'utilisation.

Consultez le gestionnaire des installations communes afin de savoir si vous devriez vérifier les fichiers que vous avez reçus en annexe de messages transmis par courrier électronique. Consultez ce même gestionnaire ou bien le coordonnateur de la sécurité informatique pour obtenir leur avis sur la façon la plus sûre d'utiliser le modem ou sur les programmes antivirus.

Que faire en cas de détection d'un virus ?

Certains virus s'annoncent en affichant un message ou un graphique inhabituel sur l'écran. D'autres n'affichent rien, mais amènent votre ordinateur à faire des choses inhabituelles. Les virus les plus insidieux manifestent leur présence en laissant uniquement une piste de données altérées, un espace vierge sur le disque là où les données auraient dû se trouver, ou un matériel endommagé.

Si vous croyez que votre ordinateur est contaminé, vous **devez** immédiatement arrêter de l'utiliser et appeler le gestionnaire des installations communes. Si vous travaillez sur un micro-ordinateur autonome, vous **devez** appeler *immédiatement* le coordonnateur de la sécurité informatique ou l'agent de sécurité du Ministère. Il importe d'agir vite; plus vous tardez à signaler un virus, plus celui-ci pourra altérer vos données ou endommager votre équipement.

Quand un virus se manifeste, il est très important de retracer tous les fichiers infectés et, si possible, de trouver la source. Si un virus reste dans un fichier, n'importe où dans votre système, il se manifestera à nouveau.

8. CONTRÔLES DE L'ACCÈS AUX SYSTÈMES INFORMATIQUES

Contrôles matériels de l'équipement et des données

Protection du matériel, des logiciels et des données

Généralement, des mesures de protection limitent le risque de dommages délibérés et accidentels aux ordinateurs, aux logiciels et aux données en limitant l'accès aux ordinateurs et aux données.

Les gestionnaires d'ISTC utilisent diverses méthodes à cet égard, notamment :

- limiter l'accès aux données de nature délicate emmagasinées dans des ordinateurs à utilisateurs multiples aux utilisateurs autorisés identifiés par des identificateurs et des mots de passe;
- exiger de chaque utilisateur qu'il n'ait qu'un seul identificateur et des mots de passe privés – aucun identificateur ou mot de passe de groupe autorisé;
- accorder ces privilèges uniquement aux utilisateurs en mesure de prouver qu'ils en ont besoin, et demander aux utilisateurs de vérifier périodiquement leurs besoins;
- permettre aux utilisateurs à distance de communiquer par modem pour accéder au système uniquement par le biais d'un équipement sûr s'ils traitent des données de nature délicate.

Identificateurs

Un identificateur est un code unique qui vous est attribué de sorte que l'ordinateur puisse vous identifier et vous autoriser l'accès conformément à vos privilèges établis.

Mots de passe

Dans le présent manuel — et dans les activités générales de traitement de données — un mot de passe est une chaîne de caractères unique que vous devez introduire avant que l'ordinateur ne vous donne accès à des données ou à des logiciels particuliers. Il ne s'agit pas de la fonction « mot de passe » de WordPerfect™, qui, en fait, est une forme simple de cryptage.

Vous **devez** changer vos mots de passe :

- au moins une fois par mois, si vous utilisez des données TRÈS SECRET; autrement, au moins une fois par trimestre;
- si le gestionnaire des installations communes vous demande de le modifier.

Outre les règles susmentionnées, vous pouvez et devriez changer votre mot de passe dès que vous en sentez le besoin.

Vous **ne devez pas** divulguer vos mots de passe afin de prévenir tout accès non autorisé.

Si vous quittez le lieu de travail pour toujours, vos mots de passe seront annulés.

Vous **devez** choisir des mots de passe :

- au hasard;
- de cinq caractères ou plus;
- assez difficiles à deviner.

Par exemple, vous pourriez utiliser les trois dernières lettres de deux mots différents, ou les quatre premières lettres d'un mot et deux chiffres au hasard. Vous **ne devez pas** utiliser de dates ou de mots réels, notamment des noms — ils sont trop faciles à trouver.

N'enregistrez jamais les mots de passe dans un format lisible. En d'autres termes, vous **ne devez pas** :

- les emmagasiner dans un ordinateur, sauf sous une forme codée;
- les intégrer dans un code logiciel informatique;
- les inclure dans des procédures d'entrée en communication automatique non protégées d'un ordinateur (consultez le gestionnaire des installations communes si vous désirez de plus amples renseignements);
- les afficher bien en vue, en particulier sur votre bureau ou votre ordinateur (oui, certaines personnes le font);
- les écrire sur un morceau de papier que vous gardez dans vos dossiers, dans votre porte-documents ou votre portefeuille;
- le communiquer à autrui, sauf à votre administrateur local de la sécurité ou, si vous assumez une fonction informatique importante, à un membre de réserve.

S'il vous faut prendre en note vos mots de passe, voici quelques suggestions:

- inscrivez-les sur un morceau de papier que vous glissez dans une enveloppe cachetée, et rangez celle-ci dans un coffre ou dans une armoire fermée à clef;
- demandez à l'administrateur local de la sécurité de les conserver pour vous, selon un contrôle strict et adéquat.

Administration des contrôles d'accès

Quand on vous attribue un identificateur et des mots de passe, en particulier si vous travaillez sur un réseau local, vous **devez** signer une attestation stipulant que vous

acceptez d'obéir aux conditions établies pour votre installation.

Au moins une fois par an, vous serez invité à confirmer par écrit que vous avez encore besoin d'accéder aux ordinateurs et que vous y êtes encore autorisé.

Suspension de l'accès

Il est fortement recommandé que les identificateurs et les mots de passe soient suspendus automatiquement après trois tentatives d'accès infructueuses. En d'autres termes, après le troisième essai en vue d'accéder à des fichiers ou des applications pour lesquels vous n'avez pas de privilèges, tous vos privilèges informatiques peuvent être suspendus tant que durera l'enquête.

De même, si vous n'utilisez pas votre identificateur ou vos mots de passe pendant une longue période, ils peuvent être suspendus automatiquement.

En conséquence, si vous remarquez que votre identificateur ou vos mots de passe ne fonctionnent pas, communiquez avec le responsable des systèmes informatiques ou avec le gestionnaire des installations communes.

Sortie automatique du système

Par mesure de sécurité, les ordinateurs peuvent être programmés afin de mettre fin automatiquement à l'accès si le terminal a été inactif pendant une période prédéterminée. Si l'accès a été interrompu automatiquement, reprenez la procédure d'entrée en communication et l'accès vous sera à nouveau accordé.

Sauvegarde de documents lisibles par machine

Supports amovibles lisibles par machine

Si vous avez en votre possession des supports amovibles lisibles par machine (ordinateurs portatifs, disques durs amovibles, disques optiques, disquettes et bandes) qui contiennent des documents classifiés ou désignés, vous **devez** vous assurer qu'une étiquette indiquant le niveau de sécurité le plus élevé de l'information est apposée. Vous **devez** ranger les supports lisibles par machine contenant des documents de nature délicate dans des coffres de sécurité approuvés et adéquats (*voir* chapitre 5 – Sécurité de l'information).

Le fait d'effacer une information ne l'enlèvera pas complètement des supports lisibles par machine. Vous **devez** vous assurer que les documents de nature délicate sont éliminés ou écrasés, ou que les supports défectueux lisibles par machine sont détruits (*voir* chapitre 5 – Sécurité de l'information).

Les supports amovibles lisibles par machine et contenant de l'information non classifiée et non désignée ne font pas l'objet d'exigences spéciales en matière de stockage, mais l'information est un bien précieux que vous devriez protéger de dangers, tels l'incendie et le vandalisme.

Disques durs fixes

Vous **ne devez pas** stocker de l'information classifiée ou désignée de nature très délicate sur le disque dur de l'ordinateur, même s'il s'agit d'un micro-ordinateur autonome se trouvant dans une zone de sécurité. Il est préférable de la garder sur des disquettes rangées dans un coffre de sécurité approuvé (*voir* chapitre 5 – Sécurité de l'information). Consultez l'administrateur local de la sécurité ou le coordonnateur de la sécurité informatique pour obtenir de l'aide ou plus de renseignements. Même l'information non classifiée ou non désignée emmagasinée

sur des disques durs fixes qui ne se trouvent pas dans des zones de sécurité peut nécessiter une protection spéciale visant à préserver son intégrité et son accessibilité.

Il est possible d'exercer des contrôles du matériel informatique et des logiciels. Toutefois, une personne déterminée peut éviter assez facilement certains contrôles d'accès fondamentaux. Le verrouillage de l'ordinateur offre seulement une sécurité minimale à laquelle vous devriez avoir recours si vous en avez la possibilité. Il peut empêcher les personnes non autorisées d'utiliser votre ordinateur, réduisant ainsi le risque de dommages à vos fichiers causés par des erreurs d'utilisateur ou des virus. Toutefois, il est possible de venir à bout d'un ordinateur verrouillé et des protections fournies par les mots de passe; un disque dur peut même être enlevé de l'ordinateur. Si un ordinateur en votre possession ne dispose pas des protections adéquates, vous **devez** vous assurer que les documents de nature délicate sont éliminés du disque dur ou écrasés.

Le cryptage par un progiciel commercial approuvé par l'agent de sécurité du Ministère peut être une protection adéquate. Si cette méthode est retenue, vous **devez** vous assurer qu'une autre personne qualifiée connaît la clé du code. Consulter le coordonnateur de la sécurité informatique pour obtenir des conseils et connaître les produits recommandés.

Certains progiciels, notamment WordPerfect™, peuvent sauvegarder automatiquement les fichiers. D'ordinaire, ils procèdent de l'une des deux façons suivantes :

- par sauvegarde originale, qui mémorise les fichiers de sauvegarde dans l'ordinateur sous un nouveau nom;
- par sauvegarde à intervalles fixes, qui efface automatiquement les fichiers de sauvegarde quand l'utilisateur sort du programme.

Quand vous utilisez ce type de progiciel pour traiter de l'information de nature délicate, et si le programme ne chiffre pas votre document au moment où vous le créez, vous **devez** vous assurer que la sauvegarde automatique se fait sur disquette. Vous **devez** ensuite enlever la disquette et la ranger dans un coffre de sécurité approuvé. Si vous ne travaillez pas avec un logiciel de cryptage et que vous ne pouvez pas choisir le support de sauvegarde, vous **devez** désactiver la fonction de sauvegarde automatique et sauvegarder périodiquement le fichier sur une disquette. Vous **devez** ensuite ranger la disquette dans un coffre de sécurité approuvé.

Le fait d'effacer les fichiers de votre disque dur ne protégera pas l'information de nature délicate qu'ils contiennent. Consultez le gestionnaire des installations communes pour obtenir des renseignements sur les programmes qui éliminent ou écrasent les fichiers, les détruisant complètement (*voir* chapitre 5 — Sécurité de l'information).

Les ordinateurs portatifs sont particulièrement vulnérables car ils sont très attrayants et faciles à emporter. Une fois qu'un ordinateur est volé, le malfaiteur a tout son temps pour trouver comment modifier le matériel et le logiciel pour parvenir jusqu'aux données. Vous **ne devez jamais** laisser un ordinateur portatif sans surveillance, dans un endroit où il pourrait être volé. Il est particulièrement important de prendre, pour les ordinateurs portatifs dotés d'un disque dur, les mêmes précautions que celles qui s'appliquent aux disques durs.

Logiciel original

S'il est possible de faire une copie légale du logiciel original (*voir* chapitre 13 — Droits d'auteur), vous **ne devez pas** utiliser le logiciel original dans le cadre des activités

ordinaires. Dans la mesure du possible, le logiciel original (standard ou personnalisé) doit être entreposé dans un endroit sûr afin de prévenir tout dommage ou toute modification non autorisée.

Sécurité des communications électroniques et sécurité informatique

L'équipement et les lignes de télécommunications qui transmettent des données de nature délicate exigent le même niveau de protection que les ordinateurs qui traitent ces mêmes données. Le courrier électronique est un service qui utilise des lignes de télécommunications.

Transmission d'information de nature délicate

Les lignes téléphoniques offrent peu de protection à l'information de nature délicate, les appels téléphoniques pouvant être interceptés de différentes façons. Les lignes spécialisées sont privilégiées pour communiquer de l'information de nature délicate. Vous **devez** utiliser un cryptage ou une autre protection approuvée par l'agent de sécurité du Ministère quand vous transmettez de l'information classifiée et désignée de nature très délicate, à moins que l'évaluation des menaces et des risques n'indique le contraire.

Consultez le gestionnaire des installations communes ou le coordonnateur de la sécurité informatique au sujet des protections des télécommunications offertes sur votre lieu de travail.

Tempest

L'équipement de communication et de traitement de données est jugé conforme aux critères *Tempest* quand il est construit de sorte à ne pas pouvoir diffuser d'information dans des émissions électromagnétiques pouvant être interceptées par une personne non autorisée. (*Tempest* était le nom de code de la technologie au moment de sa mise au

point.) Normalement, si vous ne travaillez pas dans une casemate — c'est-à-dire une pièce conçue afin de prévenir toute émission électromagnétique — vous **devez** utiliser de l'équipement conforme aux critères *Tempest* pour stocker, traiter et transmettre de l'information classifiée non chiffrée.

Dans certains cas, l'équipement conforme aux critères *Tempest* n'est pas nécessaire pour traiter de l'information classifiée non chiffrée; toutefois, l'agent de sécurité du Ministère **doit** donner son approbation au préalable.

La plupart des renseignements désignés ne doivent pas être traités sur de l'équipement conforme aux critères *Tempest*. Toutefois, certains renseignements désignés de nature très délicate peuvent être traités sur de l'équipement conforme aux critères *Tempest* si vous avez consulté l'agent de sécurité du Ministère et si l'évaluation des menaces ou des risques indique que c'est nécessaire.

Cryptage

Le cryptage est la transformation de données numériques contenues dans un texte en un imbroglio inintelligible par un processus de codage réversible basé sur une clé uniquement connue des personnes autorisées à consulter les données.

Le cryptage est une façon de protéger de l'information de nature délicate pendant la transmission ou l'information en mémoire. Il existe plusieurs applications de cryptage standard, qui fournissent divers degrés de protection. Consultez le coordonnateur de la sécurité informatique pour qu'il vous conseille sur le choix et l'utilisation de produits de cryptage de l'information désignée. Pour les produits de cryptage utilisés pour l'information classifiée, consultez l'agent de sécurité du Ministère, qui approuve tous les produits de cryptage utilisés au sein d'ISTC.

La fonction « mot de passe » de WordPerfect™ est une forme de cryptage simple — le mot de passe est la clé. Elle est facilement contournée et ne permet pas de protéger de l'information classifiée et désignée.

Téléchargement de fichiers

Tous les employés **doivent** respecter les exigences de sécurité établies pour toutes les données qu'ils téléchargent, et s'assurer que l'ordinateur de réception et la méthode de communication satisfont à ces exigences. Consultez le responsable des systèmes informatiques et le gestionnaire des installations communes pour obtenir de plus amples renseignements.

Vous **ne devez** télécharger les documents désignés que sur des systèmes sûrs.

Lignes commutées

Une ligne commutée est, pour un pirate informatique, la façon la plus facile de pénétrer un système informatique. Les ordinateurs d'ISTC dotés de lignes commutées doivent être protégés par le biais de procédures supplémentaires de vérification. Consultez le gestionnaire des installations communes ou le coordonnateur de la sécurité informatique sur l'utilisation des lignes commutées.

9. MAINTENANCE DU MATÉRIEL ET DES LOGICIELS

Autorisation

Les travaux de maintenance ne peuvent être effectués qu'après obtention de l'autorisation adéquate. Quand quelqu'un vient travailler sur l'équipement en votre possession, vous **devez** vérifier si l'autorisation a été donnée. La maintenance de l'équipement conforme aux critères TEMPEST ne peut être effectuée que lorsque l'agent de sécurité du Ministère a donné son autorisation.

Maintenance sur place

Le personnel de maintenance et de soutien qui travaille sur l'équipement utilisé pour traiter de l'information de nature délicate **doit** posséder les autorisations de sécurité pertinentes, qui seront vérifiées par le responsable des systèmes informatiques, le gestionnaire des installations communes ou le gestionnaire du centre de responsabilité.

Avant que le personnel de maintenance ne vienne travailler sur l'équipement utilisé pour traiter des données de nature délicate, vous **devez** retirer de l'équipement toute information de nature délicate ou bien vous assurer qu'elle n'est pas accessible, ne peut être copiée ni modifiée. Par exemple, vous pouvez accompagner le personnel de maintenance et le surveiller de près pendant qu'il est à la tâche.

Vous **devez** accompagner le personnel de maintenance qui travaille sur l'équipement en votre possession qui est indispensable aux activités ou utilisé pour traiter des données de nature délicate. Si vous observez des employés de maintenance non accompagnés travaillant dans une zone de sécurité ou sur un équipement utilisé pour traiter de l'information de nature délicate, vous **devez** appeler votre superviseur ou le gestionnaire des installations communes.

Maintenance hors du lieu de travail

Avant que l'équipement doté de disques durs qui est en votre possession ne soit envoyé hors du lieu de travail aux fins de maintenance, vous **devez** vous assurer que toutes les données de nature délicate en ont été retirées. Consultez le gestionnaire des installations communes, l'administrateur local de la sécurité ou le coordonnateur de la sécurité informatique.

Quand l'équipement vous est retourné après la maintenance, vous **devez** vérifier s'il contient des virus et vous assurer que les fonctions de sécurité n'ont pas été contournées, endommagées ou compromises.

10. ENTRETIEN DES ORDINATEURS ET DES SUPPORTS LISIBLES PAR MACHINE

Entretien et nettoyage

L'équipement informatique est vulnérable à la chaleur, à la poussière, aux liquides, aux surtensions de courant, aux aimants et à de nombreuses autres influences. Voici des conseils et des directives qui vous permettront de garder votre ordinateur propre et sûr.

Vous **devez** :

- protéger tous les supports magnétiques (disquettes, bandes et disques durs) des aimants et de l'équipement électronique contenant des aimants ou induisant des champs magnétiques, comme les haut-parleurs et certains téléphones.

Vous **ne devez pas** :

- laisser traîner les disquettes sans leur pochette de protection;
- plier ou agrafer les disquettes;
- toucher la partie brillante d'une disquette;
- écrire sur une disquette avec un instrument pointu;
- utiliser des agrafes ou des trombones sur une disquette.

Vous devriez :

- utiliser les encoches de protection d'écriture sur les disques non inscriptibles afin de prévenir les dommages aux fichiers;
- garder les papiers et d'autres articles loin des trous d'aération de l'équipement afin de prévenir la surchauffe;
- garder les aliments et les liquides loin des ordinateurs et des supports lisibles par machine;

- couvrir ou emballer l'équipement informatique quand il n'est pas utilisé, quand il est déménagé et quand le milieu de travail est très poussiéreux, pendant des rénovations par exemple;
- suivre les instructions d'entretien préventif données par les fabricants;
- installer des protecteurs de surtension afin de protéger les micro-ordinateurs des variations de tension;
- s'assurer que les têtes d'un disque dur sont bien parquées avant de bouger le disque dur ou l'enveloppe de l'ordinateur.

11. VÉRIFICATION DE LA CONFORMITÉ

Tous les employés sont chargés de surveiller la conformité en contrôlant les activités qui relèvent d'eux.

Inspections et vérifications

Afin de s'assurer que les pratiques locales sont conformes aux politiques et normes du gouvernement et du Ministère, les gestionnaires locaux, le coordonnateur de la sécurité informatique, l'agent de sécurité du Ministère et la Direction générale de la vérification des opérations effectuent régulièrement des vérifications et des inspections de la sécurité informatique. L'agent de sécurité du Ministère peut aussi faire appel à l'Équipe d'inspection et d'évaluation de la sécurité de la Gendarmerie royale du Canada.

Parmi les autres aspects des activités menées sur le lieu de travail, les inspecteurs et vérificateurs étudient les habitudes des utilisateurs et le fonctionnement des ordinateurs. Par exemple, ils passent en revue les registres d'accès des utilisateurs et les journaux des transactions, les registres d'activité informatique et les documents de sauvegarde. Les inspecteurs veulent également savoir si des logiciels non approuvés ou illégaux sont utilisés, si les documents de nature délicate portent la mention adéquate et sont entreposés correctement et comment le bureau est aménagé.

Documents et tableaux *d'éliminables*

Le matériel et les logiciels de tous les systèmes informatiques doivent être entretenus sur une base régulière. Quand un problème surgit, quelqu'un doit en découvrir la cause ainsi que le moment où il s'est manifesté pour la première fois, et y trouver une solution. De même, il convient de planifier le passage du matériel et des logiciels à une puissance supérieure. Il faut donc être en mesure de découvrir ce que l'ordinateur a fait et à quel moment.

Ainsi, selon l'importance et la taille du système, les gestionnaires demanderont aux employés de consigner l'information relative à ce qui suit :

- mises à jour du matériel;
- mises à jour du logiciel;
- changements de configuration;
- problèmes et solutions.

Les gestionnaires locaux attribueront les tâches d'analyse et de classement.

Il faudrait établir un tableau d'*éliminables* de sorte que les journaux soient accessibles pour des inspections et des vérifications périodiques de la sécurité, et soient éliminés quand ils sont devenus inutiles. Les journaux **doivent** être conservés pendant au moins trois mois, mais il est recommandé de les conserver de six mois à un an.

Quand ils sont disponibles, les journaux de tentatives d'accès infructueuses **doivent** être analysés régulièrement et maintenus pour les inspecteurs et les vérificateurs.

Rapport des incidents de sécurité

La disparition de documents et de disquettes, et les activités inhabituelles comme les changements inexplicables au logiciel et aux données, constituent des incidents de sécurité. Afin que ceux-ci puissent être enregistrés et faire l'objet d'une enquête, vous **devez** signaler tout incident de sécurité dont vous êtes au courant ou que vous soupçonnez à l'administrateur local de la sécurité, au gestionnaire des installations communes ou au gestionnaire du centre de responsabilité. Suivez les procédures établies pour votre lieu de travail.

Un employé sera nommé afin de consigner les incidents de sécurité et de les signaler à l'agent de sécurité du Ministère. Les incidents qui, pris isolément, semblent dérisoires, peuvent prendre une dimension toute nouvelle

quand on fait le rapprochement avec d'autres incidents survenus sur le lieu de travail ou dans l'immeuble.

Consultez la directive du sous-ministre 78-1 dans le *Guide sur la politique et les procédures en matière de sécurité* d'ISTC pour obtenir la politique complète sur les incidents de sécurité et la façon de les signaler.

12. COPIES DE SAUVEGARDE ET PROCÉDURES D'ÉVENTUALITÉ

Sauvegardes quotidiennes

La sauvegarde est une mesure de sécurité très importante. Tous les utilisateurs **doivent** prendre connaissance du calendrier de sauvegarde établi par le gestionnaire des installations communes ou le responsable des systèmes informatiques.

Vous pouvez perdre des fichiers actifs suite à de nombreux types d'accidents, de défaillances et d'erreurs, ainsi qu'en raison de virus et d'autres formes de dommages délibérés. Vous pouvez sauvegarder vos fichiers et votre logiciel en les copiant; ainsi, en cas de perte ou de dommage, vous pourrez les recréer, au moins à partir de votre dernière copie de sauvegarde. En cas de perte ou de dommage, il faudrait effectuer régulièrement des copies de sauvegarde des données et des logiciels de micro-ordinateurs autonomes afin de prévenir les dommages aux données et la perte de temps requise pour réinstaller et reconfigurer le logiciel.

Certains utilisateurs peuvent avoir besoin de sauvegardes plus fréquentes que celles fournies par le système. Modifiez le calendrier de sauvegarde avec le gestionnaire des installations communes ou avec le responsable des systèmes informatiques, ou demandez à l'un ou l'autre de vous montrer comment faire vous-même les copies de sauvegarde.

Voici quelques autres types de sauvegarde :

- sauvegarde complète, où sont sauvegardés tous les fichiers du système;
- sauvegarde différentielle, où sont sauvegardés tous les fichiers modifiés depuis la dernière sauvegarde complète;

- sauvegarde *incrémentielle*, où sont uniquement sauvegardés les fichiers modifiés depuis la dernière sauvegarde incrémentielle ou complète;
- sauvegarde sélective, qui peut être de l'un des types susmentionnés, incluant ou excluant des fichiers particuliers.

Il est extrêmement important de vérifier si vous avez bien effectué la sauvegarde. D'habitude, un message s'affiche si tout s'est bien passé. Autrement, vous pourriez découvrir trop tard que vos fichiers de sauvegarde sont inutilisables à cause d'une certaine erreur de traitement.

Stockage des données et copies de sauvegarde des logiciels

Vous **devez** entreposer le support de sauvegarde dans un endroit sûr, loin des fichiers actifs. Vous éviterez ainsi de perdre la dernière copie de sauvegarde et les fichiers actifs dans le même incident. Si vous travaillez avec de l'information indispensable à la récupération et aux activités, ou avec de l'information qui serait très difficile à remplacer en cas de désastre sur votre lieu de travail, vous **devez** entreposer une copie de sauvegarde hors du lieu de travail. Le coordonnateur de la sécurité informatique vous aidera à organiser un entreposage sûr, hors du lieu de travail, de tous les supports lisibles par machine.

Vous **devez** consigner avec précision le lieu où se trouvent les copies de sauvegarde des données et du logiciel. Vous devriez également consigner les clés de cryptage et les mots de passe requis pour accéder aux données, conformément aux précautions visant les mots de passe et tout matériel clé (*voir* chapitre 8 – Contrôle de l'accès aux systèmes informatiques).

Vous **devez** garder suffisamment de données de sauvegarde pour pouvoir récupérer les données non altérées. Pensez au temps pendant lequel une erreur ou une défaillance peut passer inaperçue dans votre système. Vous pourriez devoir

traiter de nouveau les anciennes données si vous avez un problème dans votre système depuis un certain temps, et si vous avez détruit trop tôt vos anciennes copies de sauvegarde, vous n'aurez aucune donnée valable à partir de laquelle travailler.

Récupération des données

Vous **devez** tester régulièrement les procédures de récupération des données, et d'office après avoir apporté des modifications aux logiciel et matériel connexes. Même si certaines personnes avaient sauvegardé scrupuleusement leurs données, elles ont parfois perdu des mois de travail car elles ne pouvaient pas les récupérer après qu'une mise à jour ordinaire du logiciel eut rendu les données incompatibles avec leur système.

Procédures d'éventualité

Vous **devez** prendre connaissance des fonctions qui vous incombent en vertu des plans d'urgence préparés pour votre lieu de travail. Le plan d'urgence énonce les procédures à suivre pour limiter les dommages causés par une perte de ressources informatiques. Votre superviseur vous informera de vos responsabilités conformément au plan d'urgence. Les procédures d'éventualité peuvent prévoir des services réduits par le système touché, un service complet par un système de secours, ou un service privé de toute ressource informatique.

13. DROITS D'AUTEUR

Loi sur le droit d'auteur

La *Loi sur le droit d'auteur* limite l'utilisation des logiciels achetés. Quand vous achetez un logiciel légalement, un permis d'utilisation vous est remis; d'habitude, vous pouvez l'installer sur un seul ordinateur à la fois.

Quiconque copie pour un utilisateur non titulaire d'un permis un logiciel dont il détient le permis d'utilisation peut être poursuivi en vertu du *Code criminel.*

Responsabilités des membres du personnel

ISTC respecte les lois sur le droit d'auteur sans exception. Vous **devez** vous conformer aux termes du permis quand vous copiez un logiciel. Vous **ne devez pas** utiliser des copies illégales de logiciel sous permis sur l'équipement d'ISTC.

Quand vous entrez au service d'ISTC ou que l'on vous accorde des privilèges informatiques, vous devrez peut-être signer une promesse de ne copier le logiciel et la documentation du propriétaire que si le permis l'autorise.

14. RESSOURCES

Références

Le *Guide sur la politique et les procédures en matière de sécurité* d'ISTC, qui comprend le *Guide de classification et de désignation* et les directives du sous-ministre, est remis à tous les membres du personnel quand ils entrent au service du Ministère. Vous pouvez obtenir des exemplaires supplémentaires de la Sécurité et Sûreté, et le consulter à la bibliothèque du Ministère.

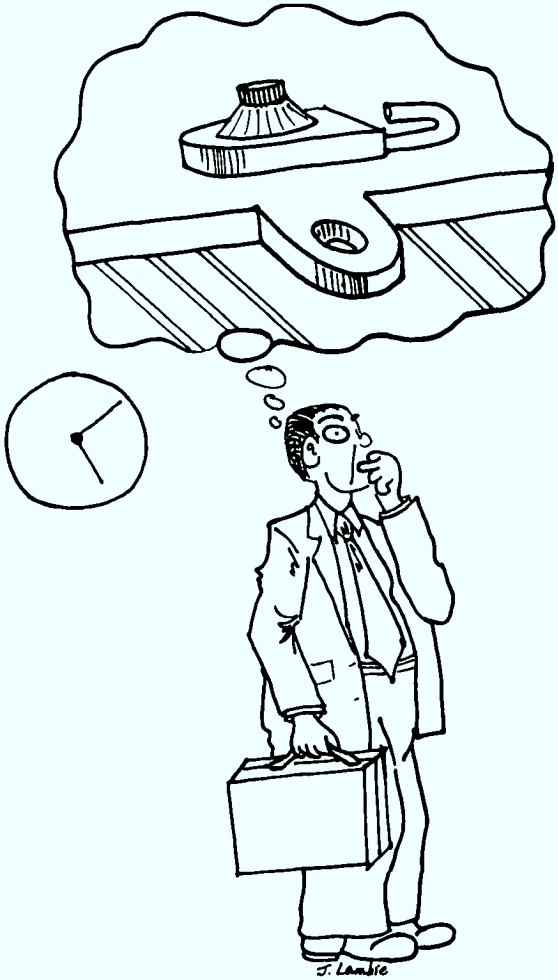
Gestion de l'information et gestion administrative : sécurité, mieux connu sous le nom de Politique sur la sécurité du gouvernement (en fait, le titre de l'une de ses sections), est un manuel du Conseil du Trésor. Il contient également les normes provisoires en matière de sécurité informatique (GES/NGI-14). Vous pouvez également vous le procurer auprès de l'agent de sécurité ou de la bibliothèque du Ministère. La nouvelle ébauche des normes provisoires en matière de sécurité informatique est reprise dans deux manuels disponibles auprès du coordinateur de la sécurité informatique : *Normes de sécurité technique – Technologie de l'information* et *Directives sur la sécurité des petits systèmes.*

Il existe deux autres manuels dans cette série, chacun contenant un index général pour toute la série. *Technologie de l'information – Guide de la sécurité à l'intention des gestionnaires des installations communes et des responsables des systèmes informatiques* d'ISTC et *Technologie de l'information – Guide de la sécurité à l'intention des gestionnaires des centres de responsabilités* d'ISTC sont disponibles auprès de l'agent de sécurité ou de la bibliothèque du Ministère.

Personnel-ressource

Si vous avez des questions sur la sécurité informatique, consultez :

- le gestionnaire des installations communes;
- le responsable des systèmes informatiques;
- le coordonnateur de la sécurité informatique, Direction générale de la gestion de l'information;
- l'agent de sécurité du Ministère.



GLOSSAIRE

Accès sélectif principe selon lequel seuls ceux qui en ont besoin dans le cadre de leurs fonctions officielles peuvent avoir accès à de l'information de nature délicate et en prendre connaissance ou possession.

Administrateur local de la sécurité membre du personnel, d'habitude un gestionnaire des installations communes ou un responsable des systèmes informatiques, auquel le gestionnaire local attribue certaines tâches locales liées à la sécurité informatique.

Agent de sécurité du Ministère Directeur, Sécurité et Sûreté, Direction générale des services administratifs; assume des responsabilités particulières en matière de sécurité, responsabilités que lui a déléguées le sous-ministre.

Authentification procédure permettant de déterminer ou de vérifier l'admissibilité d'un poste de travail, d'un expéditeur ou d'un particulier à accéder à des catégories particulières d'information; procédés qui protègent des transmissions frauduleuses en établissant la validité d'une transmission, d'un message, d'un poste de travail ou d'un expéditeur.

Chambre forte pièce équipée d'un dispositif de détection de l'intrusion et de portes dotées de serrures approuvées, située dans une zone dont l'accès est contrôlé et limité à très peu de personnes.

Chiffrement *voir* Cryptage.

Clé de chiffrement *voir* Clé de cryptage.

Clé de cryptage chaîne unique de caractères qu'un programme de cryptage utilise pour encoder et décoder les données. *Synonyme de clé de chiffrement.*

Coffre de sécurité meuble-classeur approuvé, doté d'une barre de sécurité et d'un cadenas approuvé à combinaison, ou coffre-fort approuvé doté d'un cadenas à combinaison. Pour obtenir des détails plus précis, consulter l'agent de sécurité du Ministère.

Confidentialité terme faisant référence aux données devant être tenues confidentielles; décrit le degré de protection qui doit être accordé à de telles données.

Contrôle d'accès méthodes de contrôle des privilèges et de l'accès d'un utilisateur aux systèmes, aux données et aux logiciels.

Contrôle d'accès logique logiciel d'administration du mot de passe et autres logiciels utilisés pour contrôler l'accès à des données informatisées.

Coordonnateur de la sécurité informatique membre de la Direction générale de la gestion de l'information qui aide et conseille l'agent de sécurité du Ministère; assume des responsabilités particulières dans les domaines de la formation en matière de sécurité et de la vérification de la conformité, et fournit des conseils sur la sécurité informatique au personnel d'ISTC; prépare également les évaluations des menaces et des risques ainsi que les plans d'urgence pour les systèmes informatiques importants du Ministère exploités sur des ordinateurs administrés par la Direction générale.

Cryptage transformation de données simples en une forme inintelligible par l'utilisation d'un processus cryptographique réversible. *Synonyme de chiffrement.*

Disponibilité mesure dans laquelle un système ou une ressource, comme des données, sont prêts au moment opportun.

Document document ou dispositif lisible par machine contenant de l'information; tout papier ou support photographique, magnétique ou électronique sur lequel de l'information est conservée sous forme de mots, photos, chiffres ou caractères codés, ou sous toute forme inintelligible, lisible par machine ou décodable.

Document classifié document qui contient de l'information ne pouvant être diffusée au public conformément à la *Loi sur l'accès à l'information;* document touchant la défense et le maintien de la stabilité sociale, politique et économique au Canada, et dès lors la sécurité du pays; décrit les documents TRÈS SECRET, SECRET et CONFIDENTIEL. Le *Guide sur la politique et les procédures en matière de sécurité* d'ISTC indique quel matériel entre dans cette catégorie.

Document désigné document qui contient de l'information de nature délicate non reliée à l'intérêt du pays, mais qui exige une sécurité accrue; document PROTÉGÉ. Le *Guide sur la politique* et *les procédures en matière de sécurité* d'ISTC indique quel matériel entre dans cette catégorie.

Falsification modification non autorisée qui altère le fonctionnement adéquat d'un système ou d'un appareil de façon à diminuer la sécurité qu'il offre.

Gestionnaire des installations communes personne responsable du matériel, des logiciels des systèmes informatiques, du matériel de transmission connexe et des données d'une installation de traitement à utilisateurs multiples, comme un gros ordinateur, un mini-ordinateur ou un réseau local. Sur certains lieux de travail, les fonctions de sécurité du gestionnaire des installations communes sont confiées à un administrateur local de la sécurité.

Gestionnaire du centre de responsabilité gestionnaire responsable d'un lieu de travail d'ISTC, notamment de tous les biens d'équipement et de l'information, et de toutes les mesures de sécurité prises pour les protéger.

gros ordinateur gros ordinateur exploitant d'ordinaire plusieurs systèmes à la fois et desservant de nombreux utilisateurs situés en divers endroits.

Information de nature délicate information qui doit être protégée car sa divulgation non autorisée, sa perte, son altération ou sa destruction pourrait causer des dommages importants à quelqu'un ou à quelque chose; doit être protégée selon sa nature délicate; doit se voir attribuer un niveau de sécurité et porter la mention adéquate; peut être classée TRÈS SECRET, SECRET ou CONFIDENTIEL, ou désignée PROTÉGÉ.

Information désignée de nature très délicate matériel désigné qui exige des protections spéciales; se référer au *Guide de classification et de désignation* dans le *Guide sur la politique et les procédures en matière de sécurité* d'ISTC pour obtenir les critères exacts; on peut également demander conseil à l'agent de sécurité du Ministère.

Informatique terme générique couvrant tout l'équipement informatique et tous les logiciels et les services utilisés aux fins de collecte, traitement, stockage, transmission, reproduction et présentation de l'information.

Installation équipement informatique; logiciels connexes (système d'exploitation, programmes utilitaires, compilateurs, bases de données, sécurité, communications, autres); bibliothèques de supports (bandes, disquettes, autres); bibliothèques de traitement en direct; matériel de transmission; et équipement de soutien (conditionneurs d'air, systèmes d'alimentation sans coupure, alarmes, autres).

Intégrité exigence requérant que l'information soit précise, complète et fiable; particulièrement importante pour les systèmes financiers et les systèmes d'aide à la décision.

Ligne commutée lien téléphonique d'un téléphone à un ordinateur.

Ligne spécialisée lien fixe entre un ordinateur et un téléphone particulier.

Logiciel terme utilisé pour différencier les programmes d'ordinateur des circuits métalliques (ou matériel) d'un système informatique; série mémorisée d'instructions régissant le fonctionnement d'un système informatique.

Logiciel des systèmes informatiques série de programmes informatiques et autres instructions d'un système d'information qui traite la tâche particulière que l'ordinateur doit accomplir.

Matériel de nature délicate matériel classifié ou désigné ou qui ne devrait pas être accessible à des personnes non autorisées.

Mini-ordinateur ordinateur de taille moyenne dont la capacité de traitement est inférieure à celle d'un processeur central, mais qui est utilisé de la même façon.

Mot de passe chaîne unique de caractères utilisée pour valider une identité; le mot de passe est privé, contrairement à l'identificateur.

Personne non autorisée personne à qui l'accès à une information classifiée ou désignée n'a pas été spécialement accordé.

Pirate informatique terme commun désignant une personne qui compromet ou contourne les mesures de protection pour obtenir un accès non autorisé aux ordinateurs.

Plan d'urgence énoncé détaillé et cohérent de toutes les mesures à prendre avant, pendant et après un désastre (situation d'urgence); s'il est respecté, le plan assurera la disponibilité requise des ordinateurs et des données afin de poursuivre les activités en cas d'urgence.

Politique énoncé d'une intention, d'un résultat escompté ou d'une mesure requise; oriente souvent les mesures à prendre; établit des règles qui régissent les normes, les lignes directrices et les procédures.

Procédure document décrivant les responsabilités particulières qui dictent comment mener à bien certaines tâches à des endroits donnés.

Réseau local système de dispositifs interconnectés par un support continu de sorte que l'équipement et les applications (machine de traitement de l'information ou de texte, courrier électronique) puissent fonctionner grâce à une seule série de câbles; utilisable dans une région géographique limitée, d'ordinaire dans un rayon maximum de 50 kilomètres.

Responsable des systèmes informatiques personne chargée des décisions sur les fonctions, la conception, les activités et les données du système.

SECOM sécurité des communications électroniques; protection résultant de l'application de mesures de sécurité cryptographique et de sécurité des transmissions et des émissions aux moyens de télécommunications ou autres et au matériel de traitement de l'information.

Sécurité du personnel procédures visant à assurer que tous les employés ayant accès à de l'information de nature délicate possèdent les autorisations de sécurité nécessaires.

Sécurité matérielle procédures visant à localiser et aménager les locaux et à établir les procédures matérielles afin de prévenir et déceler tout accès non autorisé et à y faire face; distincte des mesures de sécurité sur le matériel et le logiciel.

Système d'information matériel, logiciel, processus et procédures qui, ensemble, permettent de réaliser des objectifs commerciaux particuliers; utilise des données comme paramètres.

Tableau d'*éliminables* calendrier précisant la durée de conservation des documents, notamment les registres d'accès à l'ordinateur, et le moment de leur destruction.

Télécharger transférer des fichiers d'un ordinateur à distance à l'ordinateur (et vice-versa) par des lignes de télécommunications.

Vérification à rebours journaux de transactions qui offrent la preuve documentaire du traitement; la vérification à rebours permet de suivre, pas à pas ou à rebours, les transactions originales jusqu'aux documents et rapports reliés.

Vérification des virus utilisation d'un programme informatique pour détecter des virus dans des fichiers, des supports lisibles par machine ou de l'équipement informatique.

Virus programme inséré dans un système à des fins malveillantes ou criminelles; capable de se reproduire et d'infecter d'autres fichiers; peut produire son effet à la suite d'une activité prédéterminée ou à une date préétablie.

Visiteur toute personne autre qu'un employé du lieu de travail.

INDEX

A

Accès
- limites d' 22
- tentatives infructueuses 25, 37

Accès sélectif 12

Accessibilité 27

Administrateur local de la sécurité, responsabilités 6, 11, 15, 16, 24, 33, 37

Agent de sécurité du Ministère, responsabilités 6, 7, 21, 27, 29, 30, 32, 36, 37, 43

Attestations (signatures) 24, 42

Auteur, responsabilités 13, 16

C

Casemate 30

Changements de configuration 37

Classifications
- CONFIDENTIEL 12
- SECRET 12
- TRÈS SECRET 12, 23

Clé du code 27

Code criminel 42

Compte d'utilisateur, annulation 9

Coordonnateur de la sécurité informatique, responsabilités 6, 17, 20, 21, 26, 27, 29, 30, 33, 36, 40, 43

Courrier électronique 29
- fichiers reçus par 20

Cryptage 27, 29
- définition 30

D

Désignation, PROTÉGÉ 13

Direction de la sécurité et de la sûreté 6, 16, 43

Direction générale de la vérification des opérations, responsabilités 36

Disques durs
- effacement 17, 26, 28, 33
- parquage des têtes 35
- stockage de l'information de nature délicate 26

Disques optiques, rangement 26

Disquettes
- disques non inscriptibles 34
- entretien 34
- rangement 26

Documents ou information classifiés
- accès 15
- correction du niveau de classification 14
- déclassification 16
- effacement 26, 28
- impression 15
- mention du niveau de sécurité 13, 36
- protection 15
- reclassification 16
- revue régulière 16
- sauvegarde 22
- traitement 30
- transmission 29

Documents ou information désignés
accès 15
correction du niveau de désignation 14
documents de nature très délicate, protection 14, 15, 26
documents de nature très délicate, traitement 30
documents de nature très délicate, transmission 29
effacement 26, 28
impression 15
mention du niveau de sécurité 13, 36
protection 15
revue régulière 16
sauvegarde 26
téléchargement 31
traitement 30
transmission 29
Documents-papier, mention du niveau de sécurité 13
Droit d'auteur, Loi sur le 42

E

Effacement 28
Émissions électromagnétiques 29
Encoches de protection d'écriture 34
Entrée en communication automatique 24
Équipe d'inspection et d'évaluation de la sécurité 36
Équipement
conforme aux critères *Tempest* 29, 30, 32
indispensable 10, 32
vulnérable 34

F

Fonction informatique importante 24

G

Gestionnaire des installations communes, responsabilités 5, 8, 20, 23-25, 28, 29, 31-33, 37, 39, 44
Gestionnaire du centre de responsabilité, responsabilités 5, 32, 37

I

Identificateurs
annulation 9, 25
définition 22
uniques 22
Information de nature délicate, accès à l' 12
Information indispensable, entreposage 40
Intégrité 27

L

Laissez-passer 10
Lignes commutées, protection 31
Lignes téléphoniques
risques 29
spécialisées 29
Logiciels
entreposage 29
illégaux 36, 42
limites d'utilisation des copies originales 42
mises à jour 37
originaux 28, 42
Loi sur l'accès à l'information, exemption 12

M

Maintenance
- autorisation 32
- sur une base régulière 36

Membre de réserve 24

Mises à jour du matériel 37

Modem 20, 22

Modifications, vérifications des 41

Mots de passe
- annulation 9, 23, 25
- changement 23
- choix 23
- définition 23
- inscription 24
- protection 23, 24

N

Normes provisoires en matière de sécurité informatique 3, 43

O

Ordinateurs portatifs, rangement 4, 26, 28

P

Passage à une puissance supérieure, planification 36

Plans d'urgence 6, 41

Politique concernant la sécurité du gouvernement 3, 43

Présentations au Conseil du Trésor 12

Privilèges
- limites d'accès 22
- suspension 25
- vérification périodique 22, 25

Problèmes et solutions, registres sur les 37

Processus important 8

Protecteurs de surtension 35

R

Rangement des bandes 26

Rebuts des documents classifiés, élimination 16

Rebuts des documents désignés, élimination 16

Récupération des données, vérification des procédures 41

Références
- directives du sous-ministre d'ISTC 3, 15, 38, 43
- *Gestion de l'information et gestion administrative : sécurité* 3, 43
- *Guide de classification et de désignation* d'ISTC 3, 13, 43
- *Guide sur la politique et les procédures en matière de sécurité* d'ISTC 2, 3, 7, 9, 15, 38, 43
- *Directives sur la sécurité des petits systèmes* 43
- *Normes de sécurité technique — Technologie de l'information* 43
- *Technologie de l'information — Guide de la sécurité à l'intention des gestionnaires des centres de responsabilités d'ISTC* 2, 43
- *Technologie de l'information — Guide de la sécurité à l'intention des gestionnaires des installations communes et des responsables des systèmes informatiques d'ISTC* 2, 43

Registres
accès des utilisateurs 36
activités informatiques 36
documents de sauvegarde 36
tableaux d'*éliminables* 37
transactions 36
Réseau local, accès 24
Responsable des systèmes informatiques 5, 8, 25, 31, 32, 39, 44

S

Sauvegarde
à intervalles fixes 27
automatique 27
complète 39
différentielle 39
incrémentielle 40
originale 27
quotidienne 39
sélective 40
vérification de la 40
Sécurité
autorisations 7, 32
coffres de sécurité approuvés 15, 26, 28
contours des fonctions de 33
des communications 29
formalités de fin d'emploi 9
formation 8
inspections et vérifications 36, 37
lignes directrices 1
normes 1, 8, 36
politique 3, 38
procédures 7, 10, 38
rapport des incidents 37
responsabilités en matière de sécurité informatique 4, 8
séances d'information 5, 8
sécurité matérielle 10
violation de la 11, 37
zones de 4, 10, 27, 32
Sortie automatique du système 25
Support de sauvegarde
destruction prématurée 41
entreposage 40
Supports lisibles par machine 12
amovibles, stockage 26
destruction 16, 26
mention du niveau de sécurité 14
protection 34

T

Tableaux d'affichage
accès aux 20
Tâches, répartition 8
Téléchargement 31

V

Vérification approfondie de la fiabilité 7
Vérifications 36, 37
Verrouillage de l'ordinateur 27
Virus 19, 39
détection 19-21, 33
prévention 19
Visiteurs
escortes 10, 32
zones de sécurité 10

W

WordPerfect™, mot de passe 23, 31

Z

Zones de travail 10

OBSERVATIONS

Vos observations nous aideraient à améliorer les présentes normes et lignes de conduite. Veuillez remplir la présente feuille, la détacher et l'envoyer au coordonnateur de la sécurité informatique, Direction générale de la gestion de l'information, Administration centrale d'ISTC.

	Ordinateurs utilisés (veuillez cocher)		
	Micro-ordinateur	Mini-ordinateur	Gros ordinateur
Utilisateur			
Gestionnaire des installations informatiques			
Gardien du système informatique			
Gestionnaire responsable d'une des trois catégories ci-dessus			

Nom _____ Numéro de téléphone _____

Veuillez ajouter vos commentaires au verso.

Observations supplémentaires

_____

_____

_____

_____

_____

_____

_____

_____

_____

	Veuillez préciser **O** - oui; **N** - non; **S/O** - sans objet			
Section du Guide	**Utile**	**Claire**	**Détails suffisants**	**Détails excessifs**
Responsabilités en matière de sécurité				
Sécurité du personnel				
Sécurité matérielle				
Sécurité de l'information				
Administration de la sécurité informatique				
Virus				
Contrôle de l'accès aux systèmes informatiques				
Maintenance du matériel et des logiciels				
Entretien des ordinateurs et des supports lisibles par machine				
Vérification de la conformité				
Copie de sauvegarde et procédures d'éventualité				
Droits d'auteur				

Veuillez expliquer vos observations au verso.