NOUVELLES DU SIGNET

BULLETIN DU MINISTÈRE DES AFFAIRES ÉTRANGÈRES ET DU COMMERCE INTERNATIONAL SUR LA TECHNOLOGIE DE L'INFORMATION

# OÙ VOUS TROUVIEZ-VOUS AU MOMENT DE LA RÉBELLION?

Par Paul S. Dunseath
Directeur
Direction des opérations (STO)

Ceux d'entre nous qui sont dans le paysage depuis assez longtemps se rappelleront peut-être que lorsque les ordinateurs ont fait leur apparition dans les bureaux, ils servaient d'appareils de « traitement par lots ». Nichés dans des caissons vitrés dans les entrailles des édifices, ils étaient surveillés par une confrérie assurant leur contrôle et leur programmation. Les « travaux » dont on les alimentait se présentaient sous forme de liasses de cartes perforées, et le client recevait ses résultats imprimés un ou deux jours plus tard. Le personnel de la salle des ordinateurs veillait à ce que l'ordre de priorité des travaux soit respecté et à ce que les ordinateurs ne dépassent jamais leurs capacités. Les systèmes étaient fiables et, pour leur époque, relativement rapides.

Cette situation a changé pour toujours avec la mise au point des systèmes fonctionnant « en temps réel ». Exploités tout d'abord par l'industrie des réservations de billets d'avion, ils se sont répandus et sont maintenant omniprésents. Ce type de systèmes, parmi lesquels figurent les guichets automatiques et le SIGNET, fonctionnent dans un cadre régi par la demande, ce qui signifie qu'il est impossible de prévoir leur charge de travail à un moment précis. Cette caractéristique est d'ailleurs à l'origine d'un phénomène courant, dont les utilisateurs des serveurs LMX02 et LMX12 à l'Administration centrale ont malheureusement fait l'expérience au début du mois d'avril : les systèmes en temps réel continuent de fonctionner de façon égale, malgré l'augmentation de la charge de travail, jusqu'à « la » goutte d'eau qui fait déborder le vase et qui provoque soudainement une instabilité complète du système. L'atteinte du point de rupture peut résulter de la combinaison d'un certain nombre de facteurs comme le nombre d'utilisateurs, le type de travaux que le système a à exécuter et l'intensité de l'exploitation de la mémoire et des répertoires communs.

Les concepteurs des systèmes en temps réel ont peu de moyens à leur disposition pour éviter que ce phénomène ne survienne en situation réelle. L'un de ces moyens consiste à effectuer une simulation, au moyen d'un modèle mathématique du système, avant la construction de ce dernier. Malheureusement, cette méthode exige du temps, de l'argent et l'accès à des données valides recueillies en situation réelle. L'équipe du SIGNET n'avait accès à rien de tout cela avec comme conséquence, lorsque le système atteint ses limites, et comme un certain nombre d'utilisateurs ont eu l'occasion d'en faire la douloureuse expérience, un effondrement retentissant du système.

Quels mesures avons-nous mises en place pour éviter que ce genre d'incident ne se reproduise? La Direction des opérations a entrepris d'analyser de façon détaillée la façon dont les serveurs sont exploités, afin de repérer les endroits où il faudra prévoir des ressources supplémentaires. Là où les serveurs font l'objet de l'exploitation la plus intense, on envisage une redistribution des utilisateurs entre les serveurs. Nous avons aussi entrepris des démarches auprès de la direction de l'entreprise qui fabrique les serveurs - Olivetti - afin de mettre en place un plan d'intervention visant à stabiliser le système.

À titre de partenaires dans cette entreprise qu'est le SIGNET, nous avons tous un rôle à jouer; un coup d'oeil, même rapide, au contenu des répertoires communs révèle que bon nombre d'employés utilisent ces derniers comme s'il s'agissait de leurs répertoires personnels, et que ces répertoires communs contiennent bon nombre de documents, dont certains sont très longs et d'autres périmés, qui ne présentent pratiquement ou carrément aucun intérêt pour quiconque, à l'exception de la personne qui les a remisés à cet endroit. Ce genre d'exploitation ne respecte pas, bien sûr, les objectifs énoncés lors de la création de ces répertoires communs. Elle complique la navigation dans les répertoires en plus de priver les autres utilisateurs de l'accès à cette ressource commune. La Direction des opérations a entrepris d'examiner de façon détaillée le contenu de tous les répertoires communs à l'Administration centrale, et de classer tous les documents auxquels personne n'a demandé l'accès au cours des douze derniers mois. Elle supprimera par la même occasion des répertoires communs tout fichier exécutable (c'est-à-dire portant l'extension .EXE) non autorisé. En tant qu'utilisateurs, nous pouvons contribuer à ce nettoyage en passant périodiquement tous nos fichiers en revue afin de supprimer ceux qui ne présentent plus d'utilité. Ceci est particulièrement important dans le cas des personnes qui s'apprêtent à partir en affectation; pour vous guider dans cette tâche, songez que les noms de fichiers qui n'évoquent rien pour vous n'évoqueront sans doute rien non plus pour la personne qui vous succédera!

Quel est l'aspect positif de tout cela? Eh bien, le fait que le SIGNET - qui achemine actuellement plus de 60 000 messages par jour - a été victime de son propre succès. L'équipe de soutien du SIGNET est résolue à faire en sorte que les quelques nids de poule qui entravent la conduite sur l'autoroute de l'information du Ministère soient rapidement réparés, afin que le SIGNET puisse continuer de croître et de satisfaire à vos attentes et à vos exigences.

# *PREMIERS PAS* AVEC ICONDESK 4.4*

**Acceptation des Messages**

Vos nouveaux messages sont **automatiquement** acceptés chaque fois que vous ouvrez une session ICONDESK. Ces messages sont copiés dans la Boîte de réception, à partir de laquelle vous pouvez les déplacez vers des dossiers spécifiques. Vous pouvez aussi accepter vos nouveaux messages périodiquement pendant votre session ICONDESK.

Pour accepter des messages pendant la session ICONDESK:
Dans la fenêtre Boîte aux lettres ICONDESK 4.4:

1. Sélectionnez l'option **MESSAGE, ACCEPTER** de la barre de menus.

2. La fenêtre Vue: Acceptés est affichée, OU

La boîte **AUCUN MESSAGE EN ATTENTE** apparaît.

**Consultation des Messages**

**Pour consulter un message unique:**
Ouvrez n'importe quel dossier ou la fenêtre Vue: Acceptés.

1. Cliquez deux fois sur le message désiré OU
   Cliquez sur le message désiré, puis sélectionnez l'option **FICHIER, CONSULTER.**

2. Lisez votre message. (Cliquez sue le bouton **DÉTAILS** pour afficher la liste complète des destinataires.)

3. **FERMEZ** la fenêtre du message actif en utilisant la Case du menu système.

4. Sortez de la fenêtre de Consultation en utilisant la Case du menu système.

**Pour consulter plusieurs messages:**

1. Ouvrez n'importe quel dossier ou la fenêtre Vue: Acceptés.

2. Sélectionnez tous les messages que vous désirez consulter en utilisant les conventions Windows (*Ctrl+Clic*, *Maj+Clic*).

3. Cliquez sur le bouton **CONSULT**. OU sélectionnez l'option **FICHIER, CONSULTER.**
   (Le premier message apparait dans une fenêtre et les autres apparaissent sous forme d'icônes au bas de la fenêtre Consultation.)

4. Lisez le premier message, puis cliquez sur le bouton **SUIVANT.**
   (Le message suivant apparâit dans la fenêtre et le message précédent devient une icône au bas de l'écran en autant que l'option OPTIONS, une fenêtre soit cochée.)

5. Lorsque tous les messages sont lus, sélectionnez l'option **FICHIER, SORTIR.**

*de **Initiation à ICONDESK, Version 4.4, Guide d'apprentissage**, p. 37-39.

«De nos jours, les biens les plus précieux que possède une entreprise sont incorporels. C'est la matière grise qui est primée, pas les appareils, ni les logiciels.» - Alvin Toffler

# COMMENT MODIFIER LE GABARIT INTERNET POUR L'ADAPTER À LA VERSION 4.4 D'ICONDESK

Le numéro du 18 avril dernier des Nouvelles du SIGNET contenait un article précisant les modalités à suivre pour échanger des messages par l'intermédiaire d'Internet (voir, en page 3 du numéro susmentionné, l'article intitulé « Comment échanger des messages électroniques par l'intermédiaire d'Internet »). La conclusion de cet article mentionnait que d'autres instructions suivraient pour décrire comment interroger et modifier le gabarit Internet fourni dans le Répertoire d'adresses. La Direction du soutien informatique et des opérations vous recommande la marche à suivre présentée ci-après :

1. Accédez à votre compte ICONDESK

2. Dans la fenêtre Boîte aux lettres, sélectionnez l'option N.Msg (ou l'icone correspondante) afin d'afficher la fenêtre Composer un message. Cliquez ensuite sur le bouton Adresses pour afficher la fenêtre correspondante.

3. Dans la fenêtre Adresses, cliquez sur le bouton Interrogation pour afficher la fenêtre Interrogation adresse.

4. Dans la première boîte de dialogue intitulée Nom utilisateur, tapez -internet*

5. Cliquez sur le bouton OK. La fenêtre Adresses s'affichera à nouveau. L'adresse **-GABARIT INTERNET** devrait maintenant y figurer.

6. Cliquez alors deux fois sur l'entrée -GABARIT INTERNET, commandant ainsi son insertion dans la zone Destin., où elle devrait s'afficher comme suit : À : **-GABARIT INTERNET.**

7. Dans cette même zone , cliquez deux fois sur À : -GABARIT INTERNET. Ceci commandera l'affichage de la fenêtre Adresse X-400.

   Vous observerez, dans la première zone de cette fenêtre, l'indication **par défaut** suivante :
   Nom de forme libre : -GABARIT INTERNET; la deuxième zone affichera ce qui suit :
   X.400 Complète : $rfc-822*smithj(a)qucis,queensca.ca$$gc+internet$$govmt.canada$ca

   Il vous faut maintenant modifier le contenu de ces deux zones.

8. Dans le champ Nom de forme libre, modifiez -GABARIT INTERNET en fonction du nom de forme libre de la personne à qui vous comptez envoyer ce message. À titre d'exemple, si l'adresse Internet de Jonathan Seagull était la suivante : seagullj@ac.dal.ca, son nom de forme libre se présenterait comme suit : SEAGULL Jonathan

9. Dans le champ X.400 Complète, modifiez alors la partie de l'adresse suivante qui est indiquée en caractères gras :
   **$rfc-822*smithj(a)qucis,queensca.ca$$gc+internet$$govmt.canada$ca**

   pour qu'elle corresponde à l'adresse Internet , de la façon suivante :
   $rfc-822*seagullj(a)ac.dal,ca$$gc+internet$$govmt.canada$ca

   [Veuillez noter que le (a) qui figure dans l'adresse X.400 est l'équivalent ICONDESK du symbole internet @.]

   * À cette étape, si vous désirez créer un alias pour l'adresse internet que vous venez de modifier :

1. Rappelez la fenêtre Créer alias au moyen de l'option Alias.

2. Dans le champ « Nom alias », taper le nom de l'alias correspondant à votre adresse Internet.

3. Cliquez sur OK. Ceci entraînera l'affichage de la fenêtre Adresse X-400.

4. Dans cette fenêtre, cliquez sur OK pour finir de modifier votre adresse Internet.

   Répétez ces modalités pour chacune des adresses Internet contenues dans votre message.

5. Assurez-vous que toutes vos adresses Internet figurent bien dans le champ Destin.

6. Cliquez sur OK, ce qui vous ramènera à la fenêtre Composer un message. Terminez alors la rédaction votre message.

# 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.

SIGNET NEWS

INFORMATION TECHNOLOGY NEWSLETTER OF THE DEPARTMENT OF FOREIGN AFFAIRS AND INTERNATIONAL TRADE



# WHERE WERE YOU WHEN THE *FIT* HIT THE *LAN*?

by Paul S. Dunseath
Director, Operations Division
(STO)

Those of us who are sufficiently long in the tooth may recall that when computer systems first became widely accepted in the workplace they were known as "batch processors". They lived in a glass-walled room in the bowels of a building and were tended by a coterie of accolytes who controlled and scheduled them. "Jobs" were submitted in the form of a stack of punched cards, and the resulting "printout" was delivered to the user one or two days later. The computer room staff were able to ensure that work was priorized and that the computers were never overloaded. The systems were reliable and, for their day, relatively rapid.

That situation changed forever with the development of "real-time systems". First used in the airline reservation industry, these systems have spread and are now ubiquitous. A "real-time system", of which both your bank's automated teller network and SIGNET are examples, is characterized by a demand-driven environment in which the load on the system cannot be accurately predicted. These systems exhibit a common phenomenon, which users of LMX02 and LMX12 in Headquarters unfortunately experienced in early April: performance remains relatively unchanged as the load increases, until "the final straw" - a complex combination of number of users, workload mix, and use of memory and shared drives - at which point the performance abruptly becomes massively unstable.

Designers of real-time systems have limited tools at their disposal to avoid this from happening in a "live" situation. One is to simulate the system as a mathematical model before it is built, but this requires time, money, and access to valid "real world" data with which to load the simulation model. None of these were available to the SIGNET design team. As a number of users are painfully aware, the result is that when the system inevitably "hits the wall" in an operational environment, the resulting crash is public.

What is being done to minimize these occurrences? Operations Division is carefully analyzing server performance to identify where additional resources are required. In the case of the most heavily used facilities, this will likely result in some users being moved to another server. In addition, the manufacturer of the servers - Olivetti - is being called in at a senior level to agree on an action plan to stabilize the system.

As partners in SIGNET, we all have a role to play as well; even a casual scan of the shared drives will reveal that many people seem to be using them as an extension of their own personal filing space. Examples abound of documents, some quite lengthy and others no longer relevant, which are of limited or no interest except to the person who placed them there. This, of course, is not the purpose of the shared drives. Not only does it make them difficult to navigate, but also deprives others of the use of part of a shared resource. Operations Division is in the process of undertaking a detailed review of the contents of all shared drives in Headquarters and archiving any documents which have not been accessed in the past twelve months. In addition, any unauthorized executable files (those with an extension .exe) will be deleted. As users, we can assist by periodically reviewing all of our files and deleting those which are no longer of importance. This is particularly relevant before a posting; as a rule of thumb, if you can't remember what a cryptic filename means, chances are your successor won't know either!

*The good news in all this is that SIGNET - which currently carries over 60,000 messages each day - is, if anything, a victim of its own success.*

The good news in all this is that SIGNET - which currently carries over 60,000 messages each day - is, if anything, a victim of its own success. The SIGNET support people are committed to ensuring that the few potholes on the Department's Information Superhighway are paved over as quickly as possible, and that SIGNET continues to grow to meet your expectations and demands.

# ICONDESK 4.4 *BASICS**

**Accepting Messages**

Messages will be accepted **automatically** every time Mail is opened. These are also copied to the Inbox and can be moved to specific folders. You can also periodically request to accept new mail during your ICONDESK session.

**To accept messages during your ICONDESK session:**
From the Mail Manager window

1. Select ACCEPT from the Menu Bar.
2. The Accepted window will be displayed OR

   A message indicating that there are **NO MESSAGES TO ACCEPT** will appear.

**Browsing Messages**

**To browse a single message**

From any of the folders or from the Accepted window:

1. Double-click on the message you want to read OR
   Click on the message, select **FILE** from the Menu Bar and click on the **BROWSE** option.
2. Scroll through your message. (Click **DETAILS** to consult the complete list of recipients.)
3. **CLOSE** the Message window using the Control Menu Box.
4. Exit the Browse window using the Control Menu Box.

**To browse multiple messages**

1. Open any of the folders or the accepted window
2. Select all of the messages to be read using standard Windows' conventions *(Ctrl + Click, Shift + Click)*.
3. Click on the **BROWSE** button on the Tool Bar OR
   Select **FILE** from the Menu Bar and click on **BROWSE**.

[Note: the first message is displayed in the Message window and the subsequent messages are iconified at the bottom of the Browse window.]

4. Read your first message, then click on **NEXT** on the Tool Bar.
5. After all messages are read, **EXIT** the Browse window.

*from **Introduction to ICONDESK, Version 4.4, Learning Guide**, pp. 37-39.

In today's world, "the most important (possessions of) a business are intangible. The real value is what's inside your head - not the machine's, not the software." - Alvin Toffler

# HOW TO MODIFY INTERNET TEMPLATE FOR ICONDESK 4.4

In the April 18 issue of *SIGNET News*, we provided you with a set of instructions on how to exchange e-mail with the Internet (see "How to Exchange E-Mail with the Internet," p. 3). At the conclusion of the article, we said we would give you instructions on how to query and modify the Internet template available in the Directory Service. Informatics Support and Operations (STOS) advises that this is how you do it:

1. Logon to your individual ICONDESK mail account.

2. From the Mail Manager window, select Message / New (or the New icon) to display the Compose Message window. Click on the command button Addresses to display the Addresses window.

3. Click on the command button Query to display the Address Query window.

4. In the first field box "user name:" type in -internet*

5. Click on the command button OK. The Addresses window will display again. The address **-INTERNET TEMPLATE** should appear in the field box Addresses.

6. Double click on the entry -INTERNET TEMPLATE. This entry should appear in the field box Recipients as **TO: -INTERNET TEMPLATE.**

7. In the field box Recipients, double click on the entry TO: -INTERNET TEMPLATE. This will display the X.400 addresses window.

   The default in the first field box is Free Form Name: -INTERNET TEMPLATE; the default in the second field box is Full X400: $rfc-822*smithj(a)qucis.queensca.ca$$gc+internet$$govmt.canada$ca

   Both of these entries need to be modified.

8. In the Free Form Name, modifiy the -INTERNET TEMPLATE to reflect the Free Form Name of the person to whom you are sending your message. For example, Jonathon Seagull has the Internet address seagullj@ac.dal.ca
   Free Form Name: SEAGULL Jonathon

9. In the X.400, modify this bolded part of the default:
   **$rfc-822*smithj(a)qucis.queensca.ca$$gc+internet$$govmt.canada$ca**

   to reflect the Internet address:
   $rfc-822*seagullj(a)ac.dal.ca$$gc+internet$$govmt.canada$ca

[Please note the (a) in the x.400 is the ICONDESK acceptable symbol for the Internet @ sign.]

* At this point, if you want to create an alias for the Internet address you have modified:

1. Click on the command button Create Alias to display the Create Alias window.

2. In the field box "Alias name", type in the **alias name** for your Internet address.

3. Click on the command button OK. This will display the X.400 Addresses window.

4. In the X.400 Addresses window, click on the command button OK to complete the modifications of your Internet address.

   Repeat these steps for each Internet address of your message.

5. Confirm that all of your Internet addresses have been added to the field box Recipients.

6. Click on the command button OK. This will return you to the Compose Message window. Complete the remainder of your message as required.

# IT SECURITY CORNER

SECUR IT

## 15 Practical Security "Tips" for SIGNET Users

SIGNET-D, the unclassified/designated version of SIGNET, is only authorized for processing, storing or communicating (transmitting) information that is UNCLASSIFIED or PROTECTED. Information which is designated PROTECTED-SENSITIVE or is classified CONFIDENTIAL or higher must NOT be processed on SIGNET-D, as the system does not provide adequate protection for this type of information.

Information transmitted by SIGNET-D is done in the clear; that is, the information is not encrypted. When information is sent from one site to another (e.g., mission to HQ), or is transmitted internally (e.g., workstation to printers), including e-mail, it is unprotected. Even when a SIGNET-D workstation appears to be in stand-alone mode, there are possible network connections; connections to printers, for example. With easily used and readily available programs, it is possible to capture and monitor information, user IDs and passwords on SIGNET-D.

**Employees are responsible for the security of information they handle and process on SIGNET.** To ensure that appropriate security procedures and precautions are observed, ISSC recommends:

1. Never process classified or PROTECTED-SENSITIVE information on SIGNET-D. Use a TEMPEST stand-alone workstation with a removable hard drive, a non-TEMPEST stand-alone workstation with a removable hard drive (HQ ONLY), SIGNET-C2, DUCS, or Secure FAX instead;

2. Be aware of the security limitations that exist with respect to the processing of critical non-sensitive and sensitive information on SIGNET-D;

3. Include the classification or designation on each message or document processed, stored or transmitted;

4. Label each diskette containing other than UNCLASSIFIED information with the highest designation or classification level of the data it contains. A diskette with PROTECTED-SENSITIVE or classified information should never be used on a SIGNET-D workstation;

5. Recognize that information stored on the hard drive of a SIGNET-D workstation can be directly accessed by individuals without a user ID and password;

6. Protect passwords and ensure that they are changed frequently;

7. Ensure that you logout of your workstation if leaving it unattended;

[A useful complimentary feature to this is the automatic password invocation that can be turned on in the Windows Screen Saver.]

8. Ensure that data files and applications are backed-up and stored separately from the workstation;

9. Verify that diskettes containing sensitive information are destroyed according to established procedures. The delete command does not remove the data, but only changes the file name by removing the first character in the file name. This data can easily be recovered by a knowledgable individual until overwritten by another file;

10. Refrain from and discourage "browsing" through files and programs for which specific access has not been authorized;

11. Ensure that only authorized software is installed on servers and workstations, as the use of unlicensed software (including shareware used beyond its demonstration period) is illegal;

12. Refrain from installing unauthorized modems or connections to other computers or networks;

13. Treat all diskettes from external sources (this includes your co-worker at the next desk and new preformatted diskettes from sealed packages) with caution, as they could potentially be infected by a malicious code. Scan the diskette for viruses before using in your workstation;

14. Ensure that your workstation is scanned regularly for virus infections; and

15. Report all security concerns and security incidents, such as suspected intrusion attempts or virus incidents, to ISSC.

*SIGNET Newsletter* is published fortnightly by the SIGNET Client Services Division (STC) and d
Canada and at missions abroad to all employees of the Department of Foreign Affairs and Intern

Units wishing to have a notice published in the *SIGNET Newsletter* should forward the text to STC wi
the director level. All readers are invited to send to the SIGNET Suggestion Box draft articles they wis