SÉCURITÉ DE LA TECHNOLOGIE DE L'INFORMATION (TI)

La sécurité de la technologie de l'information (TI) sauvegarde les systèmes, les biens, les renseignements et les services ministériels contre des menaces délibérées ou accidentelles, en vue de garantir :

- la confidentialité des renseignements;
- l'intégrité des processus et des données;
- la disponibilité des données, des systèmes et des services.

La sécurité de la TI vise également le matériel informatique, les logiciels, les réseaux, le matériel de télécommunications et tout autre matériel interconnecté, ainsi que les endroits où se trouve ce matériel.

La TI comprend aussi tous les renseignements et données que vous créez dans le cadre de vos fonctions; les rapports officiels, les notes de service, les messages de courrier électronique, etc. sont des documents gouvernementaux et appartiennent à l'État.

Pourquoi la sécurité de la TI est-elle nécessaire?

Les employés d'AEC et de CICan doivent se protéger contre plusieurs menaces à la sécurité de la TI, notamment :

- des menaces *délibérées* y compris l'accès non autorisé à des données ministérielles, l'écoute électronique, l'inobservation des pratiques d'AEC et de CICan et les virus;
- des actions ou des événements *accidentels* y compris les erreurs des utilisateurs, l'ignorance des utilisateurs et la défaillance du matériel informatique.

Réseaux ministériels

Les réseaux ministériels suivants sont utilisés pour traiter l'information :

- SIGNET 3 (autrefois SIGNET 2000+)
- SIGNET 2000+ (autrefois SIGNET D)
- SIGNET C4.

SIGNET 2000+/SIGNET 3

Le SIGNET 2000+/SIGNET 3 est le principal réseau ministériel utilisé à l'Administration centrale et dans les missions. Il sert à traiter des renseignements non classifiés et des renseignements dont la protection n'est pas supérieure à Protégé A. Tous les employés ont accès à ce système, y compris les employés recrutés sur place, ainsi que quelques ministères, d'autres organismes et des gouvernements étrangers. Dans la plupart des missions, un administrateur de système recruté sur place est responsable du sytème SIGNET 2000+/SIGNET 3.
Note: Tout personnel doit, au minimum, tenir une cote de fiabilité avant avoir accès à SIGNET 2000+/SIGNET 3.