Dispositions relatives à la sécurité des technologies de l'information

Conception : Paul Athaide

Date de conception : 1er décembre 2010

Révision : Paul Athaide

Date de révision : 27 janvier 2011

Version 1.1

Table des matières

1. Dispositions de la politique

Le présent document expose en détail les dispositions relatives à la sécurité des technologies de l'information, lesquelles viennent compléter les modalités de la *Politique relative à la sécurité des technologies de l'information*, approuvée par le conseil d'administration national de la Société canadienne de la sclérose en plaques (ou « Société de la SP ») le 4 mars 2011.

Ces dispositions ont été approuvées par l'équipe de la haute direction le 4 mars 2011.

Résumé de la politique applicable en matière de sécurité des TI

- La confidentialité de l'ensemble des données doit être assurée au moyen de mesures discrétionnaires et obligatoires en matière de contrôle de l'accès aux données.
- L'accès à Internet et à d'autres services externes est limité au personnel autorisé.
- Aucune donnée confidentielle ne doit être stockée sur un ordinateur portatif, car la perte ou le vol d'un tel appareil compromettrait la confidentialité des données.
- Seuls les logiciels autorisés et brevetés peuvent être installés sur les systèmes, et leur installation ne peut être effectuée que par le personnel du Service des TI.
- Il est interdit d'utiliser des logiciels non autorisés. Tout logiciel n'ayant fait l'objet d'aucune autorisation sera immédiatement supprimé, et ce, quel que soit le poste de travail où il aura été trouvé.
- Les mots de passe des utilisateurs doivent comprendre au moins huit caractères alphanumériques et être changés tous les 120 jours. Un mot de passe ne peut être choisi plus d'une fois par le même utilisateur.
- Seul le personnel du Service des TI peut modifier la configuration des postes de travail.
- La sécurité matérielle de l'équipement informatique doit être assurée conformément aux lignes directrices reconnues en matière de prévention des pertes et des vols.

2. Protection contre les virus

- Le Service des TI doit mettre à la disposition des utilisateurs un programme antivirus à jour en vue de la détection et de la suppression d'éventuels virus.

- Les serveurs de fichiers doivent être protégés au moyen de logiciels antivirus dont la mise à jour est assurée continuellement.
- Les postes de travail doivent être protégés au moyen de logiciels antivirus dont la mise à jour est assurée continuellement.
- Tous les systèmes (soit les postes de travail et les serveurs) doivent être montés à partir de copies maîtresses originales non modifiées des systèmes d'exploitation dont la protection contre l'écriture a toujours été activée. Seules des copies maîtresses originales doivent être utilisées jusqu'à ce que les systèmes aient été analysés par le logiciel antivirus.
- Les fournisseurs doivent exécuter leurs logiciels de démonstration sur leur propre équipement et non sur les systèmes de la Société de la SP. Aucun fournisseur n'est autorisé à se connecter aux réseaux de la Société de la SP.
- Pour permettre la récupération de données dans l'éventualité d'une infection des systèmes par un virus, des sauvegardes de sécurité doivent être effectuées à intervalles réguliers et contrôlées par le Service des TI.
- Les utilisateurs doivent être informés de tout incident impliquant un virus.
- Les employés de la Société de la SP ont à répondre de tout manquement de leur part aux dispositions adoptées par l'organisme en matière de protection antivirus.
- Advenant l'infection d'un poste de travail par un virus, l'utilisateur concerné doit en informer immédiatement le Service des TI. Le personnel des TI analysera alors le poste de travail infecté ainsi que les unités amovibles et les autres postes de travail auxquels le virus pourrait s'être propagé, puis il procédera à l'élimination du virus en question.
- Le Service des TI effectuera ensuite des investigations, en collaboration avec l'employé concerné, afin de déterminer la cause et les circonstances de l'infection de son poste de travail.

3. Sécurité du centre de données

Le Service des TI doit mettre à la disposition des utilisateurs un centre de données sécurisé qui héberge la majorité des serveurs et de l'équipement réseau nécessaires aux infrastructures de la Société de la SP, et ce, afin d'optimiser la sécurité et la disponibilité des systèmes et des données. Le centre de données doit présenter la configuration minimale suivante :

Sécurité matérielle

- Sécurité matérielle du site assurée en tout temps.
- Surveillance par caméras et patrouilles à l'intérieur et à l'extérieur des installations.
- Identification par cartes biométriques requise pour permettre l'accès à l'étage où se trouve le centre de données.
- Bâtis hermétiques dotés de cadenas à combinaison.

- Accès réservé au personnel clé du Service des TI et aux fournisseurs avec qui la Société de la SP a conclu une entente en vue de la gestion des infrastructures.

Sécurité du milieu

- Système d'alimentation sans coupure avec bloc d'alimentation de secours double.
- Système d'extinction sous air à étapes multiples.
- Connectivité Internet en amont multiple.
- Système de climatisation multiple.
- Sol surélevé.

4. Sécurité du poste de travail de l'utilisateur

Les bureaux de la Société de la SP doivent offrir un milieu de travail sécuritaire, conformément aux spécifications suivantes :

Sécurité matérielle

- Systèmes d'alarme dont il faut chaque année changer le code et réviser la liste des personnes qui y ont accès.
- Salle des serveurs verrouillée et à accès restreint.
- Tous les petits appareils électroniques, tels les ordinateurs portatifs, les miniportatifs et les projecteurs, doivent être solidement fixés aux meubles à l'aide de câbles de sûreté.

Sécurité du milieu

- Parasurtenseurs à installer sur les postes de travail si cela est nécessaire.
- Système d'alimentation sans coupure pour les serveurs et autre équipement réseau.
- Système CVCA (chauffage, ventilation, climatisation et aération) propre à la salle des serveurs si le système en place ne permet pas de maintenir une température constante de 20 °C à 22 °C et un taux d'humidité relative de 40 % à 60 %.

5. Contrôle d'accès

- Les utilisateurs ne doivent détenir que les droits d'accès aux systèmes dont ils ont besoin pour accomplir leurs tâches. Les droits qui leur sont accordés doivent se limiter en tout temps au minimum requis.
- Les utilisateurs souhaitant avoir accès à certains systèmes doivent en faire la demande par écrit en utilisant les formulaires appropriés fournis par le Service des TI.
- Les utilisateurs sont tenus de remplir et de signer chaque année le formulaire relatif aux conditions d'utilisation des technologies de l'information. Le défaut de se conformer à cette exigence entraînera la suspension de tous les accès aux réseaux de l'organisme.
- Les utilisateurs doivent également remplir et signer chaque année un formulaire relatif à l'accès aux réseaux. Le défaut de se conformer à cette exigence entraînera la suspension de tous les accès aux réseaux de l'organisme.
- Dans la mesure du possible, personne ne doit détenir de droits permettant l'accès à l'ensemble des réseaux de l'organisme. Le Service des TI gère les mots de passe donnant accès aux réseaux et aux serveurs, et les mots de passe des postes de travail sont attribués aux utilisateurs par l'administrateur de systèmes rattaché à leur service.

  Les administrateurs de systèmes ont pour responsabilités de maintenir l'intégrité des données du service dont font partie les utilisateurs et de définir les droits d'accès de ces derniers.
- L'accès aux réseaux, aux serveurs et aux systèmes nécessite l'attribution d'un nom d'utilisateur, d'un mot de passe et, selon le cas, d'un jeton RSA.
- Les utilisateurs ne doivent pas communiquer leur nom d'utilisateur ni leur mot de passe.
- Les utilisateurs ne doivent écrire nulle part leur nom d'utilisateur ni leur mot de passe.
- Le nom d'utilisateur est constitué de l'initiale du premier prénom de l'utilisateur, suivie du nom de famille de ce dernier.
- Chaque mot de passe ne peut être choisi qu'une seule fois et doit être changé à intervalles de 120 jours.
- Chaque mot de passe doit être conforme aux exigences du système d'exploitation Windows en ce qui concerne sa complexité :
    - Le nom d'utilisateur ne peut être compris dans le mot de passe.
    - Un mot de passe doit comporter des caractères choisis parmi au moins trois des cinq catégories suivantes :
        - lettres majuscules;
        - lettres minuscules;
        - chiffres;
        - caractères non alphanumériques;

    - caractères Unicode excluant les lettres en majuscule et en minuscule (tels %, $, ?, etc.).
- La détection d'intrus doit être mise en œuvre dans la mesure du possible. Un compte d'utilisateur sera bloqué après cinq tentatives infructueuses d'ouverture de session.
- Le Service des ressources humaines doit informer l'équipe des TI de toute cessation d'emploi au sein de l'organisme. Le Service des TI supprimera alors tous les droits d'accès qui avaient été accordés à l'employé ayant cessé de travailler pour l'organisme. Le compte courriel demeurera actif pendant 45 jours après le départ de l'employé, et les fichiers de ce dernier resteront en ligne et accessibles au superviseur concerné durant la même période. Une fois celle-ci écoulée, le compte courriel et les fichiers de l'utilisateur seront supprimés.
- Les mots de passe des responsables des réseaux et des serveurs, tout comme ceux des responsables des systèmes, seront conservés en un lieu sûr (ex. : coffre-fort résistant au feu placé dans l'un des bureaux du Service des finances) dans l'éventualité d'une catastrophe ou de toute autre situation d'urgence.
- Des procédures de vérification doivent être mises en place pour tous les systèmes afin que soit assuré un suivi des tentatives d'ouverture de session ayant abouti ou pas et des changements apportés à l'ensemble de ces systèmes.
- Il convient d'avoir recours le moins souvent possible aux noms d'utilisateur des administrateurs Windows.
- Les mots de passe par défaut de tout équipement réseau ou de tout système d'applications (par ex. : SQL Server) doivent être changés au moment de l'installation.
- Sur les systèmes UNIX et Linux, les droits d'accès à rlogin, FTP, Telnet et ssh seront accordés exclusivement au personnel des TI.
- Les systèmes de fichiers doivent présenter un niveau de sécurité optimal. Dans la mesure du possible, les utilisateurs devraient se voir attribuer des droits d'accès permettant uniquement de lire des fichiers, et les fichiers devraient être accessibles en mode lecture seulement de sorte que tout risque de suppression accidentelle soit écarté.
- Les fournisseurs ne doivent pas avoir accès aux réseaux de production (réseaux d'ordinateurs donnant accès à l'un ou à plusieurs des serveurs), sauf dans des cas où il leur faut travailler sur une application en particulier. Dans pareilles circonstances, un fournisseur pourra accéder aux réseaux à condition d'avoir signé l'entente de non-divulgation prévue à cet effet. Cette exigence s'applique aussi aux fournisseurs qui bénéficient d'un accès à distance leur permettant de travailler sur les systèmes de production (comme Opal ou *mercure*).
- L'accès à Internet peut être accordé aux fournisseurs à condition que ceux-ci aient signé l'entente relative à l'utilisation des réseaux de la Société de la SP par ses partenaires d'affaires.

6. Sécurité des réseaux locaux (LAN)

Concentrateurs et commutateurs

- L'équipement propre aux réseaux locaux, les concentrateurs, les ponts, les répéteurs, les routeurs et les commutateurs doivent tous être installés dans des pièces sécurisées et réservées à ce type d'équipement. Celles-ci doivent être verrouillées en tout temps, et seul le personnel du Service des TI doit y avoir accès. Les autres employés et les fournisseurs ayant besoin d'y accéder devront en aviser le Service des TI au préalable de sorte que celui-ci puisse prendre les mesures de surveillance qui s'imposent dans pareil cas.

Postes de travail

- Les utilisateurs doivent fermer leur session lorsqu'ils quittent leur poste de travail, quelle que soit la durée de leur absence. Il est également possible de verrouiller un poste de travail équipé du système d'exploitation Windows.
- Les postes de travail se verrouillent automatiquement après 30 minutes d'inactivité.

Câblage

- L'ensemble du câblage des réseaux doit faire l'objet d'une documentation détaillée.
- Toutes les prises pour transmission de données connectées aux réseaux mais non utilisées se trouvant dans des salles de réunion ou des locaux ouverts doivent être désactivées.
- Tous les câbles des réseaux doivent être vérifiés régulièrement, et les résultats de ces examens périodiques doivent être conservés aux fins de référence.
- Les utilisateurs doivent veiller à ne poser aucun objet sur un câble des réseaux.
- Dans la mesure du possible, il convient d'utiliser des schémas de câblage redondants.

Logiciels de contrôle

- L'utilisation d'analyseurs des réseaux locaux ou de logiciels permettant d'intercepter des paquets de données (technique appelée « reniflage de paquets ») est réservée au Service des TI.

Serveurs

- Tous les serveurs doivent se trouver dans des endroits fermés à clé.
- L'accès à la console système, aux disques de serveur et aux lecteurs de bandes magnétiques est réservé au personnel autorisé du Service des TI.

Sécurité des installations électriques

- Tous les serveurs doivent être équipés d'un système d'alimentation sans coupure pouvant moduler l'alimentation électrique au besoin.

- Tous les concentrateurs, ponts, répéteurs, routeurs et commutateurs, comme tout autre équipement réseau, doivent également être munis d'un système d'alimentation sans coupure.
- Tous les serveurs doivent être dotés d'un logiciel conçu pour procéder à la fermeture ordonnée des systèmes en cas de panne d'électricité complète.
- Tous les dispositifs d'alimentation sans coupure seront testés périodiquement.

7. Sécurité propre aux serveurs

- Le système d'exploitation sera mis à jour et recevra des correctifs régulièrement, soit à intervalles ne dépassant pas trois mois.
- Les serveurs doivent quotidiennement faire l'objet d'une vérification antivirus.
- Les serveurs doivent se trouver dans des locaux sécurisés et fermés à clé.
- Les mots de passe de gestion à distance doivent différer du mot de passe de l'administrateur.
- Les droits rattachés aux comptes d'administrateur sont réservés aux membres dûment formés du Service des TI.
- L'utilisation des comptes d'administrateur doit être limitée au strict nécessaire.
- L'accès des utilisateurs aux données et aux applications doit être limité au moyen de mesures de contrôle d'accès.
- Les fonctions de détection des intrus et de verrouillage doivent être activées.
- Le système de vérification des installations doit être activé.
- Les serveurs doivent être configurés de sorte qu'ils se verrouillent automatiquement après une période de trente minutes d'inactivité.

8. Sécurité des réseaux étendus

- Les réseaux locaux sans fil ne sont pas permis s'ils n'ont pas d'abord été approuvés par le Service des TI.
    - Les réseaux locaux sans fil autorisés doivent être dotés des systèmes de cryptage et d'authentification les plus sûrs.
    - Les utilisateurs ne peuvent, en aucune circonstance, installer leur propre équipement sans fil.
- L'accès à distance n'est autorisé que s'il se fait par Citrix ou au moyen d'un tunnel RPV (réseau privé virtuel).

- Tous les ponts, routeurs et passerelles doivent se trouver dans des locaux sécurisés et fermés à clé.
- Les protocoles inutiles seront retirés des routeurs.

9. Sécurité TCP/IP et Internet

- Les connexions permanentes à Internet nécessitent l'utilisation d'un pare-feu qui permettra de contrôler le trafic réseau.
- Les connexions permanentes à d'autres réseaux externes, notamment pour le traitement de l'information hors site, nécessitent l'utilisation d'un pare-feu qui permettra de contrôler le trafic réseau.
- La solution à privilégier en matière de pare-feu est celle qui consiste en l'utilisation d'un pare-feu à cartes réseaux multiples (un dispositif ayant plus d'une adresse TCP/IP).
- L'équipement réseau sera configuré de sorte que les sessions inactives se ferment automatiquement.
- L'accès à Internet à partir d'un poste de travail nécessite l'utilisation de l'analyseur de contenu Web de l'organisme.
- Tous les courriels entrants et sortants seront contrôlés par l'analyseur de contenu de courriel de l'organisme.

10. Évaluation du niveau de sécurité

- Le Service des TI fera appel à un consultant en sécurité informatique chaque année aux fins d'évaluation du niveau de sécurité du périmètre réseau.
- Le Service des TI fera appel à un consultant en sécurité informatique tous les deux ans aux fins d'évaluation du niveau de sécurité des réseaux internes.

11. Sécurité du système de messagerie vocale

La Société de la SP est sur le point d'adopter une solution de téléphonie sur Internet (VoIP) hébergée, dont il est question dans la présente section.

- Le service d'entretien et la gestion des mots de passe du système VoIP seront assurés par le fournisseur.

- Seul le Service des TI disposera d'un compte qui lui permettra uniquement d'effectuer des transferts, des ajouts et des modifications, et le mot de passe attribué à ce compte sera sécurisé.
- Les comptes de messagerie vocale et de portail Web seront accessibles par un mot de passe constitué d'au moins cinq chiffres.
- Les factures de téléphone feront l'objet d'un contrôle rigoureux de sorte que toute utilisation inappropriée du système téléphonique puisse être relevée.

12. Acquisition de matériel et de logiciels

- Les spécifications relatives aux ordinateurs de bureau, aux ordinateurs portatifs et aux miniportatifs sont établies par le Service des TI, et ce type d'équipement peut être commandé au moyen du bon de commande des TI accessible par *mercure*.
    - Toute commande effectuée à l'aide du bon de commande des TI est gérée suivant un processus automatisé et doit être approuvée par le superviseur de l'utilisateur ayant passé la commande ou par le chef ou directeur du service concerné.
    - Le Service des TI n'intervient pas dans le processus de commande, et les commandes approuvées sont transmises directement au fournisseur.
    - Les factures sont envoyées directement aux services ayant approuvé les commandes, lesquels doivent vérifier, enregistrer et approuver les factures. Note : Le défaut de régler une facture dans un délai raisonnable pourrait compromettre l'exécution des commandes ultérieures.
- Tout article technologique doit être approuvé au préalable par le Service des TI, qui s'assurera que l'article en question est compatible avec les systèmes et pourra être pris en charge.
- Dans le cas des commandes d'un montant supérieur à 10 000 $ envisagées pour l'acquisition de nouveaux serveurs ou d'un nouvel équipement en lien avec les infrastructures, le Service des TI doit obtenir trois soumissions afin de s'assurer que l'organisme puisse opter pour la meilleure offre possible.

13. Inventaire

- Le Service des TI doit tenir un inventaire complet de tous les serveurs et de l'équipement réseau de l'organisme.
- Les autres services de l'organisme doivent tenir un inventaire complet de tous leurs ordinateurs de bureau, ordinateurs portatifs et imprimantes.

14. Accès accordé aux tierces parties

Tout fournisseur ayant besoin d'accéder aux systèmes ou aux données de la Société de la SP est tenu de signer les documents suivants pour que l'accès nécessaire leur soit accordé :

- entente de non-divulgation;
- entente relative à l'utilisation des réseaux de la Société de la SP par ses partenaires d'affaires.

15. Conception et mise à niveau des logiciels

- La présente section s'applique à tous les logiciels tiers utilisés par les unités opérationnelles de la Société de la SP.
- Les processus standards du cycle de vie des logiciels, mentionnés ci-dessous, doivent faire l'objet d'un suivi continu en ce qui a trait aux systèmes actuels ou futurs :
    - planification de projet et étude de faisabilité;
    - analyse des systèmes, établissement des exigences;
    - conception des systèmes;
    - implantation;
    - intégration et mise à l'essai;
    - approbation, installation, déploiement;
    - entretien.

16. Traitement des incidents et processus d'intervention

- En cas d'intrusion ou de toute autre violation de la sécurité, le Service des TI prendra des mesures immédiates visant à isoler le(s) système(s) atteint(s) et à informer les personnes concernées. Les utilisateurs ont pour responsabilité d'aviser sans délai le Service des TI de toute atteinte à la sécurité des systèmes, réelle ou suspectée. Chaque effraction ou violation donnera lieu à des investigations menées par le Service des TI.
- Le Service des TI pourrait faire appel à des fournisseurs tiers en vue d'obtenir une aide supplémentaire.
- La personne ou l'entité responsable de la prise en charge d'un système dont la sécurité a été atteinte doit dans tous les cas :
    - rapporter l'incident au chef des activités des TI et au vice-président des technologies de l'information ou à l'un d'eux;
    - bloquer l'intrusion ou empêcher la propagation de l'atteinte dans la mesure du possible;
    - remédier aux effets dommageables de l'incident;

- rétablir le service tel qu'il était avant l'incident;
- conserver des preuves de l'atteinte, le cas échéant;
- effectuer une analyse après l'incident pour en déterminer la cause;
- préparer une liste de recommandations pour éviter la survenue de tout autre incident de nature similaire;
- procéder à un suivi au cours des trois prochains mois.

- Il importe de ne pas apporter de modifications à un système ou à appareil ayant servi à une activité criminelle (ou qu'on soupçonne d'avoir été utilisé à des fins criminelles) jusqu'à ce que le vice-président des technologies de l'information indique que le système ou appareil en question peut être modifié.

Glossaire

Analyseur des réseaux locaux (LAN)	Dispositif capable de surveiller et d'analyser le trafic réseau. Ce type d'appareil est généralement utilisé pour contrôler le volume des échanges d'information sur les réseaux. Certains analyseurs sophistiqués peuvent décoder les paquets de données, permettant ainsi de savoir quelles données ont été transmises.
Authentifier	Identifier un utilisateur, un appareil ou toute autre entité en lien avec un système informatique, souvent en vue de permettre l'accès aux ressources de ce système.
Autorisation	Octroi de droits d'accès à un utilisateur, à un programme ou à un processus.
Concentrateur	Dispositif d'un réseau destiné à répéter des paquets de données au sein du réseau.
Contrôle d'accès	Processus consistant à limiter aux seuls programmes, processus et systèmes autorisés l'accès aux ressources de certains systèmes.
Contrôle d'accès discrétionnaire	Méthode consistant à limiter l'accès à certains systèmes selon l'identité et les besoins de l'utilisateur de même que les besoins du groupe dont il fait partie ou ceux du processus concerné.

Contrôle d'accès obligatoire	Méthode consistant à limiter l'accès à certains systèmes selon le caractère sensible de l'information contenue dans ces systèmes et selon le niveau d'autorisation accordé aux entités concernées en ce qui a trait à l'accès à de l'information sensible.
FTP	De l'anglais *file transfer protocol*. Protocole permettant le transfert de fichiers à l'aide d'un réseau TCP/IP.
Identification	Processus permettant à un système de reconnaître des entités, généralement au moyen de noms d'utilisateurs uniques lisibles par une machine.
Internet	Système de communication international constitué d'un réseau d'ordinateurs répartis dans le monde entier et reliés entre eux au moyen de connexions téléphoniques.
Messagerie vocale	Système permettant aux appelants de laisser des messages vocaux destinés aux membres du personnel.
Mot de passe	Chaîne de caractères confidentielle et protégée permettant de vérifier l'identité d'un utilisateur.
Nom d'utilisateur	Chaîne unique constituée de symboles ou de caractères permettant à un système d'identifier un utilisateur donné.
Ordinateur portatif	Ordinateur de petit format pouvant être facilement transporté.
Pare-feu	Dispositif ou logiciel conçu pour prévenir les accès et les flux de données non autorisés ou inappropriés entre différents réseaux.
Système d'alimentation sans coupure/unité d'alimentation permanente	Souvent désigné par le sigle UPS (de l'anglais *uninterruptable power supply*). Système doté de batteries et conçu pour protéger un équipement électrique contre les surtensions pouvant toucher le réseau de distribution d'électricité et pour fournir le courant nécessaire au fonctionnement de cet équipement en cas de panne d'électricité.
Telnet	Protocole permettant à un dispositif de se connecter à un hôte UNIX dans le cadre d'une session.
Virus	Logiciel programmé pour se multiplier et, dans la plupart des cas, corrompre les programmes et les données compris

dans les ordinateurs qu'il a infectés.