POLITIQUE

TITRE : CONTROLE DE L'UTILISATION D'INTERNET, DU RTSS, DU COURRIER ELECTRONIQUE ET DES RESEAUX INFORMATIQUES DU CHSLD/GESTION DES ANTI-VIRUS	**N° DF-POL-007**
ORIGINE : SERVICE DES RESSOURCES FINANCIÈRES ET TECHNIQUES	
DESTINATAIRE(S) : DIRECTION GÉNÉRALE, CHEFS DE SERVICE, TOUT LE PERSONNEL	
APPROUVÉE PAR : _____ NADINE COMEAU, DIRECTRICE GÉNÉRALE	APPROUVÉE LE : 28 MARS 2006 RÉVISÉE LE : SEPTEMBRE 2009, MARS 2013, MARS 2017, MARS 2018, MARS 2021

Énoncé

Le CHSLD doit mettre en place les mécanismes nécessaires au contrôle de l'utilisation d'Internet, du RTSS, du courrier électronique et des réseaux informatiques du CHSLD de la Côte Boisée.

Objectifs

-Présenter les principes généraux et les règles qui régissent l'utilisation adéquate et sécuritaire de l'Internet, du RTSS, du courrier électronique et des réseaux informatiques de l'établissement.
-Présenter les types d'incidents informatiques les plus fréquents.
-Énoncer la procédure de gestion des antivirus.

PROCÉDURE

Principes généraux

- Le CHSLD de la Côte Boisée utilise des logiciels permettant de contrôler et d'enregistrer toute utilisation d'Internet faite à partir de ses réseaux informatiques.
- Le responsable de sécurité informatique de l'établissement se réserve le droit d'enregistrer, peu importe l'utilisateur, toute page World Wide Web (www) visitée, tout «chat» ou «newsgroups» ou courrier électronique.
- Le CHSLD de la Côte Boisée analyse et évalue, en tout temps, l'usage qui est fait d'Internet, de ses réseaux informatiques et du RTSS. L'analyse peut également être faite par le CISSS ou installation d'un proxy internet.

** La politique « Gestion et utilisation des codes et des privilèges d'accès informatique » indique des règles de conduite complémentaires à celles présentées aux points 2.2 et 2.3.

Règles concernant l'utilisation de l'Internet, du RTSS et des réseaux informatiques de l'établissement

- L'affichage de tout document ou tout graphique sexuellement explicite, haineux, raciste et socialement inacceptable est interdit. De plus, de tels documents ne doivent pas être archivés, enregistrés, distribués ou édités via le réseau du CHSLD de la Côte Boisée.
- Les actifs informationnels et de télécommunication, les outils Internet et le RTSS qui sont accessibles via les réseaux informatiques de l'établissement ne doivent pas être en violation des lois et réglementations en vigueur au Canada ou dans tout autre pays. L'usage d'Internet, du RTSS, des réseaux informatiques et des actifs informationnels et de télécommunication de l'établissement, pour des activités illégales, entraîne des mesures disciplinaires. De plus, l'établissement s'engage à coopérer face à toute requête provenant des forces de l'ordre ou à la demande de tout autre organisme mandaté à cet effet.
- Tout logiciel ou document téléchargé via Internet ou le RTSS vers les réseaux informatiques de l'établissement devient la propriété de celui-ci. Ils doivent être utilisés en accord avec leurs licences et copyright.
- Aucun utilisateur ne peut utiliser les facilités d'accès à Internet ou le RTSS pour télécharger ou distribuer des données ou des logiciels piratés.
- Aucun utilisateur ne peut utiliser les facilités d'accès à Internet pour propager quelque virus que ce soit, sur les réseaux informatiques de l'établissement.
- Aucun utilisateur ne peut utiliser les facilités d'accès à Internet ou au RTSS ou tout autre moyen, pour rendre inutilisable ou surcharger quelques ordinateurs ou réseaux que ce soit, ou encore pour contourner tout système mis en place pour protéger la vie privée ou la sécurité des autres utilisateurs.
- Aucun utilisateur des réseaux informatiques de l'établissement ne peut utiliser un modem sur son poste de travail sans l'approbation du responsable de sécurité informatique de l'établissement.
- Tout utilisateur utilisant les facilités d'accès à Internet doit s'identifier clairement et entièrement quand il participe à des «chats» et à des «newsgroups» ou quand il ouvre un compte sur des systèmes externes.
- Seuls les utilisateurs dûment autorisés à intervenir, au nom du CHSLD de la Côte Boisée, aux médias ou à des assemblées publiques peuvent participer à de tels groupes reliés à leur travail et en rapport avec leurs fonctions, mais ils le font en leur nom propre en tant qu'individu. Lors d'une telle participation, si un membre du personnel est identifié au CHSLD de la Côte Boisée, il doit s'abstenir de tout commentaire ou endossement non autorisé.
- L'établissement conserve la propriété et les droits d'auteur de tout matériel transmis à des forums, «newsgroups», «chats» ou page du World Wide Web (www) par les membres de son personnel, pendant leur travail.
- L'utilisation des facilités d'accès à Internet de l'établissement, pour commettre des infractions telles qu'un usage abusif des actifs informationnels et de télécommunication, du harcèlement sexuel, la tenue d'un discours public non autorisé et le détournement ou le vol de la propriété intellectuelle est également interdit.
- Les utilisateurs doivent planifier toutes opérations de téléchargements intensifs telles que les transferts de documents de grande taille, de documents vidéo ou sonores ou d'envois massifs de courrier électronique en dehors des heures de travail, soit avant 8 h 30, entre 12 h et 13 h ou après 17 h.
- Tout document téléchargé doit être vérifié contre les virus avant son exécution. L'utilisateur est responsable du contenu desdits documents. L'établissement exige l'emploi de logiciels antivirus sur ses ordinateurs entrant en communication avec ses réseaux informatiques.

- Aucun utilisateur ne doit divulguer, en tout ou en partie, la structure des réseaux informatiques de l'établissement. De plus, les utilisateurs doivent s'assurer que leur utilisation des réseaux informatiques n'altère pas la structure de ceux-ci.

Règles concernant l'utilisation du courrier électronique

- Le gestionnaire de système qui administre un système de courrier électronique doit fixer des règles concernant les délais de conservation des messages. Les copies des messages, notamment celles que peut garder en mémoire le fournisseur de services Internet, sont soumises aux mêmes dispositions. Dans les organismes publics, les délais de conservation doivent être consignés dans un calendrier approuvé par les Archives nationales.
- Le CHSLD de la Côte Boisée attribue un droit d'accès aux boîtes de courrier à l'administrateur Outlook et au responsable de sécurité informatique de l'établissement. Ces droits sont effectifs, pour l'administrateur Outlook, seulement pour la réexpédition de messages qui ne sont pas arrivés à destination. Le responsable de sécurité informatique de l'établissement peut faire la surveillance du contenu des messages et la détection de fraude pour fins d'enquête.
- Puisqu'il est question de l'utilisation du courrier électronique en milieu de travail, l'établissement s'accorde un droit de surveillance des boîtes postales.
- En l'absence de mesures de sécurité, la confidentialité du courrier électronique peut être précaire et les précautions élémentaires suivantes doivent être appliquées :

  - L'accès aux boîtes de courrier est restreint et protégé par un mot de passe.
  - L'utilisateur devra modifier son mot de passe selon les politiques en vigueur, au changement de personnel. Le mot de passe doit être composé de chiffres et de lettres et contenir au moins 8 caractères.
  - À chaque boîte postale correspond un mot de passe géré par la personne autorisée à y accéder.
  - Dans le cas d'une boîte commune, seuls les membres du personnel autorisés à y accéder doivent connaître le mot de passe.
  - Le système doit posséder un mécanisme de gestion des mots de passe selon le profil de l'utilisateur.
  - Le mot de passe n'est pas affiché lorsqu'il est saisi par l'usager.
  - L'usage du courrier électronique doit être limité aux messages et aux fichiers qui ont rapport au travail.
  - L'usage du courrier électronique est interdit pour fins syndicales.
  - La modification d'un message avant sa retransmission à un autre destinataire est interdite.
  - Comme précaution supplémentaire, pour assurer la confidentialité des messages et fichiers expédiés par courrier électronique, l'encodage ou le cryptage est recommandé.

- S'il ne peut assurer l'encodage ou le cryptage d'un document à caractère confidentiel, l'utilisateur devra employer un autre moyen sécuritaire de communication pour acheminer ledit document ou obtenir l'autorisation de son supérieur immédiat.
- Tout utilisateur qui désire préserver le caractère confidentiel ou privé du contenu des courriers électroniques qu'il transmet doit utiliser des programmes ou autres techniques de cryptage ou d'encodage sur le poste dont il se sert pour transmettre son courrier électronique. Par ailleurs, il doit également être conscient que les courriers électroniques qu'il envoie peuvent, à son insu, être redirigés, imprimés, sauvegardés ou affichés sur des médias ou des systèmes informatiques de tiers.

- Tout utilisateur se doit de respecter les conventions d'accès et d'usage des réseaux internes et externes, et correctement identifier sa correspondance électronique.
- Il est interdit d'utiliser le courrier électronique pour véhiculer des messages ou des propos obscènes, haineux, racistes, diffamatoires, harcelants ou pour commettre tout autre acte réprimé par la Loi ou par les politiques et procédures de l'établissement.

Types d'incidents et directives à suivre[1]

Types d'incidents

- **Un virus informatique ?**

➢ Un antiprogramme dont l'exécution est déclenchée lorsque l'objet auquel il a été rattaché clandestinement est activé, qui se recopie au sein d'autres programmes ou sur des tours de moyen de propagation, et qui produit les actions malveillantes pour lesquelles il a été conçu. Un virus informatique peut comporter une *bombe logique ou un cheval de Troie*.

- **Une bombe logique (« logic bomb »)?**

➢ Un antiprogramme à déclenchement différé, qui ne se reproduit pas, activé soit à une date déterminée par son concepteur, soit lorsqu'une condition particulière se trouve vérifiée, ou un ensemble de conditions réunies, et qui, dès lors, produit l'action malveillante pour laquelle zones systèmes lui servant à leur il a été conçu.

- **Un cheval de Troie (« Trojan horse »)?**

➢ Un antiprogramme qui, introduit dans une séquence d'instructions normales, prend l'apparence d'un programme valide contenant en réalité une fonction illicite cachée, grâce à laquelle les mécanismes de sécurité du système informatique sont contournés, ce qui permet la pénétration par effraction dans des fichiers pour les consulter, les modifier ou les détruire. Le cheval de Troie peut passer inaperçu pendant des mois, puisqu'il se dissimule sous l'apparence d'un logiciel inoffensif, par exemple un jeu ou un petit utilitaire.

- **Un ver informatique (« Ransom ware ») ?**

➢ Antiprogramme autonome et parasite, capable de se reproduire par lui-même, en perpétuel déplacement dans la mémoire d'ordinateur qu'il surcharge et mine progressivement, en consommant, jusqu'à la paralysie, les ressources du système informatique. Le *ver et le virus* sont tous deux capables de se reproduire, mais à la différence du virus, le ver n'a pas besoin d'un programme hôte pour le faire. Il est totalement autonome. Les vers informatiques peuvent s'attaquer à une station de travail (ver de station de travail) ou à d'autres systèmes informatiques, habituellement par les réseaux (ver de réseau).

- **Un canular (« hoax ») se définit ainsi …**

➢ Un canular est un faux virus, présenté comme étant très dangereux ou encore délirant, généralement véhiculé par courrier électronique. Par exemple, un courriel contenant un canular peut menacer de détruire, s'il est lu, toutes les données d'un disque dur.

[1] Tiré de *Souris,* Centre hospitalier Pierre-Le Gardeur

- **Une chaîne de lettre**

Se distinguent par trois (3) éléments :

- comprend un appât pour attirer votre attention (ex. : « aidez-nous »);
- une menace qui avise contre de terribles dangers pouvant survenir si la chaîne n'est pas maintenue;
- une requête qui demande de transférer le message à d'autres personnes.

- **Ingénierie sociale**

- Le piratage par ingénierie sociale est un ensemble de techniques et tactiques utilisées dans le but de persuader des personnes à fournir des informations confidentielles (ou stratégiques) ou à faire exécuter des actions, sans que ces personnes réalisent le véritable objectif de la demande;
- Ces techniques, de plus en plus populaires, exploitent donc des vulnérabilités humaines par l'entremise d'appâts, de tromperies, de manipulations, de faux liens de confiance, permettant ainsi à des utilisateurs malveillants de tromper la vigilance des gens pour accéder à des systèmes ou ouvrir des brèches de sécurité.

Voici quelques exemples d'ingénierie sociale :

- une personne, téléphonant de l'établissement, s'est fait passer pour le technicien en informatique de l'organisation (avec nom à l'appui). Il a mentionné à l'utilisateur qu'un nouveau serveur sera installé ce week-end et lui demande donc son mot de passe pour le réinitialiser à la même valeur, pour le lundi matin…;

Directives à suivre

- Tout utilisateur doit être vigilant et doit aviser immédiatement par courriel l'adjointe de direction qui fera le suivi au responsable de la sécurité informatique ou le technicien en informatique de tout incident identifié.
- Ne jamais divulguer son mot de passe ou autres informations confidentielles ou stratégiques à quiconque.
- Ne pas laisser traîner ou jeter du papier qui contient des informations confidentielles ou stratégiques.
- Sur réception d'un courriel d'une personne demandant de le retransmettre à des amis, **détruisez le courriel**, car c'est peut-être une chaîne de lettres, un antiprogramme caché dans une pièce jointe ou tout simplement un canular, et sa redistribution ne ferait qu'engorger le réseau.
- En plus, dans le cas d'un antiprogramme (ce qui est peu probable, car nous avons des logiciels antivirus, mais …), il pourrait affecter tous les ordinateurs du CHSLD. De surcroît, vous prêtez votre nom et la réputation de notre établissement au message, le faisant paraître authentique même s'il n'en est rien. **Détruisez donc le courriel.**
- Autrement dit, il est interdit de faire usage du courrier électronique pour participer à une chaîne de lettres, pour effectuer de la publicité ou de la vente pyramidale ou encore pour faire des envois massifs de messages sans autorisation.

Gestion des antivirus

Anti-virus utilisé

- Le CHSLD de la Côte Boisée utilise Office Scan de Trend Micro pour la détection des virus informatiques et logiciels malveillants.

Mise à jour

- Gérée par le CISSS de Lanaudière.
- Chaque ordinateur Windows 10 possède Office Scan qui est installé de façon à ce qu'un seul administrateur puisse modifier les informations et la configuration. Office Scan est configuré de façon à détecter tout virus sur les postes informatiques à midi de chaque jour de la semaine.
- La mise à jour de l'antivirus du serveur est effectuée quotidiennement via le serveur Lanaudière.
- Les postes informatiques de l'établissement vont automatiquement mettre leur antivirus à jour à partir de la console de gestion sur le serveur.

Vérification

- Advenant une infection, le CISSS de Lanaudière nous avise. Nous avons accès à la console pour vérification et analyse ponctuelle.
- À partir de la console, il est possible de planifier la détection des virus ou des logiciels malveillants sur les postes de travail et les procédures à suivre à la suite de la détection (quels postes de travail et quels fichiers ont été affectés par un virus).
- Pour une escalade en cas d'infection, vous référez à la politique intitulée « Politique sur la gestion des crises et incidents informatiques ».

Interventions

- Lorsqu'un virus est détecté lors d'une vérification, le technicien en informatique voit à le supprimer ou à le mettre en quarantaine immédiatement.

RÉVISION

La présente procédure sera révisée minimalement aux quatre (4) ans.

ENTRÉE EN VIGUEUR

La présente procédure entre en vigueur le jour de son adoption par la direction générale.