



Politique sur l'usage approprié des technologies – 5.BP.6

Première publication : Le 1^{er} juin 2000
Dernière révision : 1^{er} décembre 2013

1. Introduction

Le YMCA du Grand Toronto offre à ses utilisateurs¹ l'accès à des ressources informatiques, à ses systèmes de messagerie électronique, de productivité au bureau, à ses systèmes administratifs et opérationnels, et un accès Internet dans le cadre de l'exécution de leurs tâches et des responsabilités propres à leur poste.

Cet accès vise à accroître la productivité et ne peut être utilisé pour des activités autres que celles du YMCA. Internet pourrait permettre à des utilisateurs non autorisés de visualiser les renseignements du YMCA ou d'y accéder. Les connexions doivent donc être sécurisées, contrôlées et surveillées. Tout accès d'un non-employé à des ressources ou aux systèmes informatiques du YMCA sans l'autorisation préalable du service des TI est interdit.

Pour favoriser la responsabilisation des utilisateurs, les lignes directrices suivantes ont été établies. On y trouve les principes généraux d'utilisation des supports et services électroniques. Toute exception à cette politique doit être approuvée par le vice-président principal des technologies de l'information (TI).

2. Procédures

Les utilisateurs doivent respecter les procédures ci-dessous lors de l'utilisation de ressources, appareils et systèmes informatiques, de soutien et de services électroniques.

2.1 Usage approprié

Les ordinateurs, le soutien et les services électroniques fournis par le YMCA du Grand Toronto sont principalement destinés à des fins opérationnelles pour aider les utilisateurs à accomplir leur travail. Ils doivent donc être utilisés pour de telles activités. L'utilisation personnelle limitée, occasionnelle et raisonnable est compréhensible et acceptable tant qu'elle :

- a) utilise une quantité raisonnable de ressources;
- b) d'empêche pas l'exécution des tâches et aux responsabilités de l'employé;
- c) ne nuit pas à une activité commerciale;
- d) ne présente pas de risque pour la sécurité et l'intégrité des données.

Les documents et fichiers personnels stockés dans les ressources fournies par l'Association demeurent l'entière responsabilité de l'employé en vertu du paragraphe **2.12 Propriété du YMCA** (ci-dessous). Tous les renseignements tirés d'Internet doivent être considérés comme douteux, jusqu'à ce qu'ils soient

¹ Dans le présent document, utilisateurs s'entend des employés qui utilisent les systèmes informatiques du YMCA du Grand Toronto.

confirmés par d'autres renseignements issus d'une autre source. Il n'y a pas de procédure de contrôle de la qualité dans Internet, et une somme considérable de ces renseignements n'y est pas à jour ou inexacte. Les utilisateurs doivent faire preuve de responsabilité et ne pas abuser de ce privilège. En vertu de la nouvelle politique sur les communications électroniques pour l'envoi de messages électroniques au nom du YMCA, le personnel et les bénévoles (le cas échéant) doivent appliquer les procédures de la *Politique sur les communications électroniques 5.BP.7*, qui précise les exigences de la *Loi canadienne anti-pourriel*.

2.2 Protection de la vie privée

Le YMCA du Grand Toronto ne peut pas garantir le caractère privé des communications électroniques. Les utilisateurs doivent savoir que les communications électroniques peuvent, selon la technologie, être transmises, interceptées, imprimées et stockées par d'autres personnes. En outre, d'autres personnes peuvent accéder à des communications électroniques conformément à cette procédure. Tous les utilisateurs du courrier électronique doivent respecter notre protocole relatif au courrier électronique, notamment en ce qui concerne les envois massifs ou de groupe, disponible dans les *Pratiques de gestion du YMCA*.

Les **appareils mobiles** (ordinateurs portatifs, clés USB, BlackBerry, etc.) peuvent être volés ou perdus. Pour protéger la confidentialité de leurs données, les employés doivent s'adresser à leur gestionnaire ou s'adresser au service de soutien des TI pour discuter des alternatives au stockage de renseignements personnels ou sensibles. Tous les appareils contenant des renseignements sensibles ou personnels doivent être sécurisés à l'aide d'un mot de passe. Pour en savoir plus sur la protection de la vie privée, consulter la *Politique de protection des renseignements personnels (3.BP.2)* et à la *Politique sur les appareils mobiles 5.S.6*.

2.3 Conservation

Les utilisateurs doivent sauvegarder toutes les communications électroniques nécessaires à la bonne marche des activités et pour respecter les exigences réglementaires et légales. Les utilisateurs doivent supprimer régulièrement les messages inutiles pour leurs activités (y compris dans les dossiers « éléments envoyés » et « éléments supprimés » dans Outlook). Les messages peuvent être archivés en utilisant la fonction d'archivage d'Outlook. Les superviseurs ont plus de renseignements sur les Lignes directrices de conservation des dossiers dans les *Pratiques de gestion du YMCA*.

2.4 Utilisation interdite

Les supports électroniques, notamment les courriels, Internet et l'intranet, ne peuvent être utilisés pour visualiser, transmettre, récupérer ou stocker sciemment une communication :

- a) discriminatoire ou considérée comme étant un harcèlement;
- b) dérogoire à l'encontre d'une personne ou d'un groupe;
- c) obscène, sexuellement explicite ou pornographique;
- d) diffamatoire ou menaçante.

Aucun utilisateur ne doit utiliser les supports électroniques (courriels, Internet, intranet...) à des fins :

- e) qui constitueraient une violation de toute licence régissant l'utilisation de logiciels;
- f) qui constitueraient une violation des lois sur le droit d'auteur;
- g) illégales;
- h) de nature commerciale ou, pour une personne, pour un gain financier;
- i) contraires à la politique et aux procédures du YMCA du Grand Toronto.

2.5 Étiquette d'Internet

Tous les utilisateurs doivent respecter les règles généralement acceptées de l'étiquette d'Internet. Ces règles sont les suivantes, sans toutefois s'y limiter :

- a) Faire preuve de courtoisie et éviter les propos grossiers dans ses messages.
- b) Utiliser un langage approprié; éviter d'injurier, d'utiliser de termes vulgaires ou tout autre langage inapproprié; ne pas s'engager dans des activités illégales.
- c) Ne pas utiliser de supports ou de services électroniques pouvant provoquer la congestion du réseau ou nuire de façon importante à la capacité des autres personnes à accéder au système et à l'utiliser (p. ex. écoute de musique, de vidéos ou autres depuis votre ordinateur).

2.6 Participation à des forums en ligne

Les utilisateurs doivent se rappeler que tous les messages ou renseignements envoyés à partir des installations fournies par le YMCA à une ou plusieurs personnes par réseau électronique (p. ex. listes d'envoi, sites de réseaux sociaux, forums et autres services en ligne) sont des énoncés identifiables et attribuables au YMCA du Grand Toronto et doivent être traités comme tel. L'utilisation de forums en ligne est autorisée lorsque la participation à un forum peut être importante pour le rendement du travail d'un employé.

Les utilisateurs peuvent indiquer leur affiliation au YMCA du Grand Toronto dans les sites de réseaux sociaux, discussions, séances de clavardage et autres canaux de communication dans Internet. Cela peut être fait en ajoutant explicitement certains mots, ou implicitement, par exemple dans une adresse électronique. Lorsque les utilisateurs donnent une affiliation, ils doivent aussi clairement indiquer que les opinions formulées sont les leurs, et pas nécessairement celles du YMCA du Grand Toronto.

Les opinions et points de vue que j'exprime sur les réseaux sociaux sont personnels et ne reflètent pas nécessairement l'opinion et la politique du YMCA du Grand Toronto.

2.7 Sécurité

La sécurité des ressources informatiques du YMCA est une priorité de premier plan. Les utilisateurs doivent mettre en pratique les étapes suivantes en matière de sécurité :

- a) Ne pas télécharger de logiciels sur un disque dur utilisé à l'Association ni sur des clés USB qui seront utilisées sur les systèmes du YMCA.
- b) Seul le service de soutien aux utilisateurs des TI ou les personnes qu'il délègue peuvent installer des logiciels sur les ordinateurs du YMCA. Les privilèges d'administration en ce sens sont limités.
- c) Ne pas laisser d'autres employés utiliser son nom d'utilisateur ou son mot de passe. Ne pas utiliser le nom d'utilisateur et le mot de passe d'autres personnes.
- d) Tout problème de sécurité doit être signalé immédiatement au premier vice-président, TI (ou à son délégué). À moins d'autorisation explicite par le premier vice-président des TI, les utilisateurs ne peuvent :
 - surveiller ou intercepter les fichiers ou communications électroniques d'autres utilisateurs ou de tierces parties;
 - pirater ou obtenir l'accès aux systèmes ou comptes auxquels ils n'ont pas accès normalement;
 - enfreindre, tester ou surveiller les mesures de sécurité d'un ordinateur ou d'un réseau.

2.8 Sauvegarde

Le service des TI est responsable des procédures de sauvegarde sur les serveurs du YMCA du Grand Toronto. Ils sont responsables, notamment, du calendrier des copies de sauvegarde régulières, du stockage hors site des supports et des essais périodiques de la capacité de restauration conformément aux procédures du *Plan de reprise après sinistre du YMCA*.

Chaque utilisateur doit faire une copie de sauvegarde des données stockées sur le disque dur de son poste de travail (ordinateur de bureau ou portable). Tout support de sauvegarde doit être entreposé à un endroit sécurisé et protégé par mot de passe.

2.9 Prévention des virus

Un logiciel antivirus est installé sur les serveurs, les postes de travail et les ordinateurs portatifs. Le service des TI et l'utilisateur sont chargés d'effectuer les mises à jour régulières des fichiers de données, la mise à jour des virus, etc.

Tous les comportements inhabituels du système, tels que des fichiers manquants, pannes fréquentes, messages mal acheminés et autres doivent être signalés immédiatement au service des TI, car ils peuvent avoir été provoqués par un virus informatique ou des problèmes de sécurité du même type.

Si vous croyez qu'un virus a infecté votre système, avisez immédiatement le service de soutien des TI. Il est interdit de désactiver votre antivirus sur votre ordinateur.

2.10 Mots de passe

Les mots de passe sont les points d'entrée à nos ressources technologiques. Protéger l'accès à nos ressources est essentiel pour assurer la sécurité de nos systèmes. Nous devons faire preuve de diligence pour conserver l'accès à nos ressources et les protéger des menaces internes et externes pour notre organisation.

Les mots de passe pour tous les systèmes doivent respecter les règles suivantes :

- a) ils ne doivent pas être prononcés, écrits, envoyés par courriel ou partagés²;
- b) Ils ne doivent pas être partagés pour « couvrir » une personne absente du bureau;
- c) ils ne doivent pas être formés de votre nom, adresse, date de naissance, nom d'utilisateur, surnom ou tout autre terme facile à deviner par une personne qui vous connaît;
- d) on ne doit pas les afficher ou les cacher dans son espace de travail.

2.11 Mots de passe administratifs

Les mots de passe administratifs sont modifiés régulièrement et ont un accès limité. Il s'agit des mots de passe pour les routeurs, interrupteurs, liens WAN, pare-feu, serveurs, connexions Internet/intranet, comptes des systèmes d'exploitation ou toute autre ressource technologique.

Les mots de passe administratifs ne doivent pas être communiqués à des personnes en dehors du groupe des TI sans la permission du premier vice-président, TI.

2.12 Propriété du YMCA

Les systèmes de communications électroniques, les messages générés ou gérés par ces systèmes ainsi que les fichiers électroniques des employés, notamment les copies de sauvegarde, sont la propriété du YMCA du Grand Toronto, et ne sont pas la propriété des utilisateurs des services de communication électronique. Tout le matériel, notamment les ordinateurs de bureau, ordinateurs portatifs, imprimantes,

² Ne s'applique pas lorsque la TI attribue un mot de passe à un utilisateur, ou lorsqu'elle doit dépanner et résoudre un problème.

téléphones cellulaires ou BlackBerry achetés par le YMCA du Grand Toronto sont la propriété du YMCA. À la fin de son emploi, l'utilisateur doit remettre tous les appareils au YMCA.

2.13 Surveillance

Le YMCA du Grand Toronto se réserve le droit, à sa discrétion, de surveiller ou d'examiner les fichiers électroniques, répertoires, messages et tout contenu auquel un employé a accédé dans Internet afin de s'assurer que ses supports et services électroniques sont utilisés conformément à cette procédure et à la loi. L'examen de ce contenu aura lieu uniquement sur approbation du vice-président de l'employé et du premier vice-président, TI.

Les utilisateurs du YMCA du Grand Toronto doivent s'attendre à ce qu'aucune protection de leur vie privée ne soit assurée lorsqu'ils utilisent des ordinateurs loués par le YMCA ou dont le YMCA est propriétaire. Les renseignements transmis ou stockés dans ces équipements pourraient faire l'objet d'une surveillance.

2.14 Divulgence occasionnelle

Les employés des TI peuvent devoir examiner le contenu des communications d'un employé durant la procédure résolution des problèmes. Les employés des TI ne peuvent divulguer un tel contenu, à moins qu'il soit réputé assujéti à la section « utilisation interdite » du présent document. Le cas échéant, les employés des TI doivent aviser le vice-président, TI.

Les employés des TI ne peuvent examiner le contenu des communications d'un employé par simple curiosité ou à la demande de personnes qui n'ont pas eu recours à la chaîne d'approbation habituelle.

2.15 Violations

L'utilisation des systèmes et ressources informatiques du YMCA est un privilège et non un droit.

L'utilisation inappropriée, notamment la violation des règles et politiques de l'organisme, peut entraîner la fin de ces privilèges et l'imposition de mesures disciplinaires pouvant aller jusqu'au renvoi. Le vice-président de l'employé et le premier vice-président des TI établiront de telles mesures en consultation avec le service des ressources humaines.

3. Procédures/politiques connexes et documents de référence du YMCA

- **Politique relative à la protection de renseignements personnels (3.BP.2)** – Définit les attentes du YMCA en ce qui concerne les pratiques de gestion des renseignements, notamment la protection et la sécurité des données, des appareils électroniques et mobiles.
- **Politique relative aux communications électroniques (5.BP.7)**
- **Politique sur les appareils mobiles (5.S.6)** – Précise ce qu'est une utilisation appropriée des appareils mobiles afin d'en assurer un usage sécuritaire et rentable par les employés et le contrôle des coûts.
- **Plan de reprise après sinistre du YMCA** – Il fait partie de la planification de la poursuite des activités du YMCA et assure la reprise des procédures et des programmes essentiels plus sensibles au temps le plus rapidement possible à la suite d'une perturbation.

4. Personnes-ressources et autres ressources

Pour en savoir plus sur cette politique, les employés peuvent s'adresser au directeur général, vice-président ou premier vice-président, ou s'adresser au vice-président principal des technologies de l'information.

[Cette page est intentionnellement laissée en blanc]