POLITIQUE DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

VERSION 1

Créée le 24 août 2012 (v1), par Christian Lambert

Table des matières

1 INTRODUCTION

Le Conseil des écoles fransaskoises (CÉF) s'est donné pour mission de ″préparer l'élève du XXIe siècle à sa réussite scolaire, identitaire et culturelle″. Pour ce faire, le CÉF a déployé une infrastructure informatique (TI) utilisée autant par les élèves que par les professeurs ainsi que par le personnel d'encadrement et de soutien.

La sécurité des informations conservées et traitées par les infrastructures TI est au cœur des préoccupations du Conseil. Pour souligner de façon tangible l'importance d'agir avec le souci de la protection des renseignements personnels sous sa responsabilité, le CÉF se dote d'une politique de sécurité TI.

Ce document énonce cette politique et y associe des règles afin de s'assurer au quotidien du respect de la règlementation. Ce document s'adresse donc à tous les acteurs dont la tâche est d'accéder et d'utiliser les données du CÉF.

2 ÉNONCÉ DE POLITIQUE DE SÉCURITÉ

L'énoncé de politique se décline en plusieurs éléments, chacun ciblant une action de l'utilisateur. Une fois l'élément énoncé, des règles sont édictées afin de cibler les précautions à prendre lors de l'action. Parfois, pour souligner fles comportements fautifs, certains sont ajoutés sous la rubrique ″Ne pas faire″.

2.1 VERROUILLAGE DES ORDINATEURS

S'il est laissé sans surveillance et sans protection, votre ordinateur peut être utilisé ou volé par d'autres utilisateurs mettant ainsi en péril de précieux renseignements, tels des mots de passe, des courriels confidentiels et des documents.

Voilà pourquoi *chaque utilisateur doit* :

- Protéger les actifs informationnels contre la perte, les dommages, une utilisation malveillante, le vol, le retrait et le gaspillage.
- Verrouiller son ordinateur lorsqu'il s'absente de son bureau ou poste de travail.
- Protéger son ordinateur portatif à l'aide d'un dispositif de sécurité adéquat, tel un câble de sécurité.
- Ranger son ordinateur portatif en lieu sûr après les heures de travail.

Ne pas faire :

- Régler son économiseur d'écran de façon à ce qu'il ne soit jamais déclenché automatiquement.
- Laisser son ordinateur portatif non verrouillé et sans surveillance.

2.2 UTILISATION ET PROTECTION DU MOT DE PASSE

Les mots de passe constituent un aspect important de la sécurité des ordinateurs. Ils sont le principal élément de protection de l'information sauvegardée dans le poste de travail et dans les systèmes du CÉF. Les mots de passe doivent être uniques et difficiles à deviner.

Un mot de passe mal choisi pourrait compromettre l'ensemble du réseau du CÉF. Ainsi, tous les utilisateurs (employés, fournisseurs, élèves, visiteurs et autres tiers qui utilisent les systèmes d'information, les réseaux et les actifs informationnels ou qui y ont accès) ont la responsabilité de choisir avec soin et de protéger leur mot de passe.

Chaque utilisateur est donc :

- Entièrement responsable de l'utilisation de son code d'utilisateur et du mot de passe associé.
- Responsable de choisir avec précaution son mot de passe en suivant les instructions à cet effet (généralement disponibles dans la fenêtre d'authentification).
- Passible de se voir retirer son droit d'accès après 3 tentatives infructueuses.

- Responsable de garder son mot de passe confidentiel et de se conformer aux règles établies pour la sélection et l'utilisation du mot de passe.
- Responsable d'informer le centre de soutien aux utilisateurs s'il croit ou a des raisons de croire que la confidentialité de son mot de passe a été compromise.

Ne pas faire :

- Divulguer son mot de passe à des collègues de travail.
- Inscrire son mot de passe sur un papillon adhésif et le coller bien en vue sur son bureau.

2.3 RANGEMENT DU BUREAU

L'information constitue un actif important pour une organisation et doit être adéquatement protégée. Elle peut, entre autres, être imprimée, inscrite sur un morceau de papier ou envoyée électroniquement. Quelle que soit sa forme, chaque utilisateur est responsable de la protéger.

Par conséquent, *chaque utilisateur doit* :

- Éviter de fournir à une personne ou organisation des renseignements qui pourraient avoir des répercussions sur le CÉF, son image et les biens qu'il possède ou utilise.
- Garder sous clé les renseignements de nature confidentielle ou hautement confidentielle en tout temps.
- Rester à proximité de l'imprimante, lorsqu'il imprime des documents renfermant des renseignements d'affaires de nature confidentielle ou hautement confidentielle, ou du télécopieur lorsqu'il envoie ou reçoit de tels documents.
- Garder en lieu sûr de tels renseignements lorsque son bureau est sans surveillance.

Ne pas faire :

- Quitter le travail à la fin de la journée sans enlever de vos bureau, imprimante et télécopieur les documents contenant des renseignements de nature confidentielle ou hautement confidentielle.

2.4 SAUVEGARDE DES DONNÉES

L'information est l'un des actifs les plus importants d'une organisation. La perte d'actifs informationnels pourrait avoir de graves répercussions sur l'organisation et ses activités d'affaires.

Dans cette perspective, *chaque utilisateur doit* :

- S'assurer que les données soient sauvegardées régulièrement lorsqu'elles ne sont pas conservées sur un serveur réseau.
- Entreposer les supports de sauvegarde dans un environnement approprié afin de protéger leur intégrité et d'en limiter l'accès.
- S'assurer que l'information sauvegardée peut être accessible à partir des supports de sauvegarde.

2.5 IDENTIFICATION ET COMMUNICATION DES INCIDENTS

Le processus de gestion des incidents liés à la sécurité a pour but de mieux protéger les actifs informationnels du CÉF. Le fait de communiquer immédiatement les incidents liés à la sécurité dès qu'ils se produisent contribue à limiter les répercussions et l'ampleur des dommages.

Dès qu'un incident est constaté, *chaque utilisateur doit* signaler tout incident lié à la sécurité de l'information qui pourrait avoir des répercussions sur la sécurité des systèmes d'information, notamment :

- Un virus;
- L'état d'incapacité d'un système ou d'une application;
- L'accès non autorisé aux systèmes d'information;
- L'accès physique non autorisé au centre de données ou à la salle dans laquelle se trouvent les serveurs et équipements de télécommunication;
- Une violation en matière de confidentialité ou d'intégrité;
- Toute utilisation inappropriée des systèmes d'information;
- Tout autre geste susceptible d'avoir une incidence négative sur les systèmes d'information du CÉF;
- Un accès offert qui n'est plus requis;
- Les droits d'accès d'un utilisateur qui ne sont pas légitimes.

Ne pas faire :

- Garder le silence et ne pas signaler une utilisation inappropriée des systèmes d'information dont l'utilisateur est témoin.

2.6 COMPORTEMENT SÉCURITAIRE

L'entraide entre collègues est un comportement naturel. Sans lignes directrices, ce comportement risque toutefois d'entraîner, au sein d'une organisation, un incident lié à la sécurité pouvant lui causer un préjudice.

Une technique appelée ″ingénierie sociale″ est utilisée pour solliciter auprès des gens des renseignements confidentiels en se basant sur le comportement humain. Le ″hameçonnage″ est une catégorie particulière d'ingénierie sociale qui utilise les courriels pour convaincre des gens de fournir des renseignements personnels. Ces renseignements personnels sont ensuite utilisés à des fins frauduleuses.

Méfiez-vous des courriels vous demandant de fournir des renseignements personnels. Les entreprises dignes de confiance ne demandent jamais de renseignements importants au moyen d'un simple message courriel.

Dans cette perspective, *chaque utilisateur doit* :

- Ne jamais fournir à une personne ou organisation des informations sur le CÉF ou sa clientèle, à moins d'être dûment mandaté pour ce faire.
- Ne jamais révéler des renseignements personnels par courriel.
- Aviser votre supérieur si une personne inconnue ou non autorisée demande des renseignements de nature confidentielle sur le CÉF ou sa clientèle.
- Communiquer tout incident lié à la sécurité de l'information qui pourrait avoir des répercussions sur la sécurité des systèmes d'information.

Ne pas faire :

- Garder le silence et ne pas signaler un incident.
- Donner des renseignements sur le CÉF ou sa clientèle à des amis ou des tiers.
- Donner des renseignements personnels à des sources inconnues.

2.7 LES TIERS

Les tiers (membres élus du Conseil, agents contractuels, fournisseurs de services ou experts-conseils) doivent se conformer à la politique globale et aux directives en matière de sécurité des TI du CÉF, selon le service offert et la responsabilité qui en découle.

Tout accès à un système d'information du CÉF doit faire l'objet d'une autorisation formelle et d'un contrôle.

Dans la démarche de conformité des ententes avec des tiers, chaque employé du CÉF impliqué doit :

- S'assurer que toute acceptation d'un service fourni par un tiers aux fins du traitement, de la communication et de la sauvegarde de l'information concernant le CÉF doit être étayée dans une entente conclue entre le CÉF et le tiers.
- S'assurer que toutes les modifications apportées aux ententes conclues avec des tiers soient contrôlées et approuvées par le palier de direction approprié, selon le type de service concerné.
- S'assurer que les tiers se conforment à la politique globale et aux directives en matière de sécurité des TI du CÉF, selon la nature du service fourni par le tiers.
- Établir au besoin les exigences précises en matière de sécurité des TI pour les tiers, selon le service fourni et les actifs informationnels concernés.
- S'assurer que tout accès aux systèmes d'information du CÉF soit approuvé par le palier de direction approprié.
- S'assurer que toute demande de connexion externe soit approuvée par l'agent de la sécurité de l'information du CÉF et réponde à un besoin d'affaires.
- S'assurer que toute demande de déménagement dans les locaux d'un tiers d'un équipement dont le CÉF est propriétaire doit être approuvé par le palier de direction approprié.

Ne pas faire :

- Lors d'une situation d'urgence, créer une connexion externe sans autorisation.

2.8 INTERNET ET COURRIER ÉLECTRONIQUE

Internet

L'Internet est devenu un outil de communication essentiel, mais malheureusement, un outil utilisé aussi pour des activités frauduleuses.

Dès que la connexion à Internet est établie, vous risquez d'infecter votre ordinateur de virus ou des logiciels malveillants, ou encore de révéler des renseignements personnels ou confidentiels.

Voici donc les règles encadrant l'utilisation d'Internet :

- L'accès à Internet est réservé aux besoins d'affaires du CÉF.
- L'utilisateur doit éviter d'accéder à des sites susceptibles de discréditer le CÉF de quelque manière que ce soit, notamment à des sites qui exploitent un contenu offensant. Il est également interdit d'imprimer, de demander, de télécharger ou de conserver des documents au contenu frauduleux, malveillant ou obscène.
- La direction peut limiter l'accès à l'Internet.

Ne pas faire :

- Visiter un site web au contenu offensant.

Courrier électronique

Les règles relatives à l'utilisation de la messagerie électronique sont les suivantes :

- N'utiliser le courrier électronique du CÉF que pour les affaires (administration et pédagogie).
- L'utilisation du courrier électronique ne doit en aucun cas nuire à l'exploitation du réseau informatique, ni à l'image du Conseil et le courrier électronique ne doit pas être utilisé pour des motifs immoraux ou illégaux.
- Les employés doivent faire preuve d'une grande prudence lorsqu'ils envoient des courriels è un réseau externe au moyen des systèmes du CÉF.
- Les utilisateurs ne doivent pas ouvrir les courriels provenant de sources inconnues et non fiables.
- Les utilisateurs ne doivent pas envoyer des pourriels, des chaînes de lettres, des blagues ou autres messages semblables, ni des messages dont le contenu peut être considéré comme offensant ou perturbateur incluant, mais sans s'y limiter, des messages ou images obscènes ou à connotation raciste, ethnique, sexuelle ou sexiste.
- Les utilisateurs ne doivent pas désactiver le logiciel anti-virus.

2.9 ORDINATEURS PORTATIFS ET ACCÈS À DISTANCE

La perte d'un ordinateur portatif peut causer un sérieux préjudice au CÉF. Les ordinateurs portatifs doivent toujours être gardés en lieu sûr et être utilisés de façon appropriée, afin de prévenir la compromission de renseignements confidentiels ou l'accès non autorisé au réseau du CÉF. Le

service des TI du CÉF a pris les mesures nécessaires pour faire face aux menaces auxquelles sont exposés les utilisateurs d'ordinateurs portatifs.

Il ne suffit que de quelques secondes à une personne pour voler un ordinateur portatif. Il est donc impératif de toujours observer les mesures de sécurité suivantes :

- Les ordinateurs portatifs ne doivent jamais être laissés sans surveillance s'ils ne sont pas verrouillés au moyen d'un câble de sécurité.
- Lorsque vous voyagez, assurez-vous de garder votre ordinateur portatif avec vous en tout temps, à l'aéroport ou dans tout autre lieu public.
- Dans l'avion, gardez-le avec vous, ne l'enregistrez pas avec vos bagages.
- Ne jamais laisser votre ordinateur portatif dans votre chambre d'hôtel, sauf si vous le remisez dans le coffret de sûreté ou si vous utilisez un câble de sécurité pour le verrouiller.
- Faites une sauvegarde de vos données avant de partir en voyage.
- Si votre ordinateur portatif est volé, signalez immédiatement ce vol à votre centre de soutien aux utilisateurs. Chaque minute compte lorsqu'il faut empêcher des intrus de compromettre l'intégrité du réseau du CÉF.
- L'employé ne doit pas désactiver les mesures de sécurité intégrées à son ordinateur portatif.
- L'utilisation d'économiseurs d'écran automatiques protégés par un mot de passe est obligatoire.
- L'utilisation d'un logiciel anti-virus local qui effectue une mise à jour automatique est obligatoire.
- Les utilisateurs ne sont pas autorisés à activer le partage de fichiers ou è partager des disques locaux.
- L'installation de logiciels sans l'approbation préalable de la direction des TI est interdite, afin de prévenir tout problème lié aux licences, au soutien ou à la compatibilité.
- Les renseignements confidentiels doivent être sauvegardés sur le réseau du CÉF.
- L'interface d'accès au réseau sans fil doit être désactivée lorsqu'elle n'est pas requise.
- L'accès à distance doit être offert en fonction des besoins d'accès, être approuvé et utilisé conformément aux besoins d'affaires ayant fait l'objet d'une autorisation.
- Tous les utilisateurs qui jouissent d'un accès à distance doivent se conformer aux règles et aux lignes de conduite du CÉF en matière de sécurité. Plus précisément, ils doivent :
    - Protéger leur ordinateur avec un mot de passe en tout temps;
    - Utiliser uniquement les logiciels approuvés par le CÉF pour accéder aux systèmes d'information du Conseil.

Ne pas faire :

- Partager votre ordinateur avec un ami.
- Installer un logiciel piraté, ou non autorisé par le Conseil.