SRMTI - PR - 1 - 2015

Procédure d'utilisation des ressources informatiques

OBJECTIF : Venir en appui à la réalisation de la mission de la CSRS par l'établissement d'un code de conduite et de mécanismes d'application encadrant l'utilisation de ses ressources informatiques.

ORIGINE : Politique sur l'utilisation des ressources informatiques (CSRS-POL-2014-02)

UNITÉ RESPONSABLE : Service des ressources matérielles et des technologies de l'information

Cette procédure a été autorisée par le soussigné et entre en vigueur ce jour même.

M. André Lamarche
Directeur général

Date

Procédure d'utilisation des ressources informatiques

1. Définitions des termes

Dans cette procédure, à moins que le contexte n'impose un sens différent, les expressions et les termes suivants signifient :

Audit : Opération d'inspection ou de vérification d'une activité ou d'un processus pour confirmer, ou infirmer que l'activité ou le processus soit effectué selon un standard accepté ou selon la meilleure pratique reconnue.

CSRS : Commission scolaire de la Région-de-Sherbrooke. À moins que le contexte n'impose un sens différent, le terme « CSRS » désigne implicitement toutes les instances de la CSRS : écoles, centres et services.

Invité(e) : Individus, associations ou organisations utilisant les ressources informatiques de la CSRS et n'étant pas assujettis à un lien d'emploi ou à un lien d'étude avec la CSRS. Autrement dit, ce terme désigne toute autre personne utilisant les ressources informatiques de la CSRS, qui n'est pas élève, employé(e) ou commissaire.

Médias sociaux : Média numérique basé sur les technologies du Web 2.0, qui vise à faciliter la création et le partage de contenu généré par les utilisateurs, la collaboration et l'interaction sociale. Les médias sociaux utilisent l'intelligence collective dans un esprit de collaboration en ligne. Ils permettent aux internautes de créer ensemble du contenu, de l'organiser, de le modifier et de le commenter. Les technologies utilisées sont, entre autres, les blogues, les wikis ...

Ressources informatiques : Équipements informatiques, équipements de réseautique, équipements de télécommunication, systèmes d'information, logiciels, banques de données, systèmes de courrier électronique et systèmes téléphoniques. À moins que le contexte n'impose un sens différent, le terme « Ressources informatiques » désigne implicitement « Ressources informatiques de la CSRS ».

Unités administratives : École, centre ou service de la CSRS.

Usager : Employé(e), élève, commissaire ou invité(e) qui utilisent une ressource informatique de la CSRS.

2. Code de conduite

Les usagers des ressources informatiques de la CSRS doivent respecter le Code de conduite présenté à l'annexe 1 sur l'utilisation et la gestion des ressources informatiques de la CSRS.

En plus du Code de conduite de la CSRS, une unité administrative peut adopter un code de conduite local auquel ses usagers devront également se souscrire. Cependant, les codes de conduite locaux ne peuvent pas être moins restrictifs en diminuant ou en éliminant des responsabilités et restrictions du Code de conduite de la CSRS.

3. Les mécanismes d'application

3.1. Utilisation autorisée des ressources informatiques

Toutes les ressources informatiques localisées dans les différentes unités administratives, ainsi que toutes les informations qui y sont enregistrées, sont la propriété de la CSRS. Les ressources informatiques sont des biens

achetés avec des deniers publics et ils doivent être consacrés et réservés à la réalisation de la mission de l'organisation, et ce, dans le respect des principes énoncés dans la politique d'utilisation des ressources informatiques.

Seules les personnes dûment autorisées peuvent utiliser les ressources informatiques de la CSRS. Tout accès ou tentative d'accès non autorisé à ces ressources constitue une violation à la présente procédure et peut faire l'objet de sanctions de la part de la CSRS tel que la révocation du droit d'accès aux ressources informatiques.

Les ressources informatiques sont des outils réguliers de travail ou d'apprentissage et ils doivent être dédiés et réservés à cet effet. Toute autre utilisation de ces ressources est interdite. Cependant, la CSRS reconnaît que, occasionnellement et particulièrement en dehors des heures normales de travail, les employés peuvent faire un « usage limité » (c'est-à-dire, une brève période d'utilisation) de certaines ressources informatiques aux fins de leur vie privée, qu'il s'agisse de messages téléphoniques ou de traitements informatiques. Un tel « usage limité » ne doit générer aucun coût direct d'utilisation. L'utilisation à des fins personnelles des ressources informatiques de la CSRS est un privilège et non un droit. Ce privilège peut être limité et même révoqué, en tout temps, à tout usager qui ne se conforme pas à la procédure ou au code de conduite de la CSRS sur l'utilisation des ressources informatiques. Toute limitation ou révocation d'utilisation des ressources informatiques sera faite selon une démarche administrative appropriée et respectueuse.

3.2. Modification autorisée des ressources informatiques

Afin de s'assurer de l'intégrité des ressources informatiques, les usagers ne doivent pas modifier ou détruire les données, les logiciels, les progiciels, la documentation, les systèmes d'information et les équipements informatiques de la CSRS sans avoir obtenu l'autorisation appropriée.

Afin de préserver l'intégrité des ressources informatiques, de faciliter le support et la maintenance, le SRMTI se réserve le droit d'installer des dispositifs de gestion et de sécurité sur celles-ci. Selon les utilisations et le type des appareils, des progiciels peuvent être utilisés pour empêcher que le système d'exploitation, les applications et les données ne soient altérés par l'usager.

Afin de s'assurer de la performance et de la sécurité du réseau de la CSRS, les usagers ne doivent pas altérer le réseau informatique (installer, déplacer, configurer ou modifier de quelconque façon de l'équipement réseau) sans l'autorisation de la direction des SRMTI. Advenant le cas où de l'équipement aurait été branché sur le réseau sans autorisation, le SRMTI se réserve le droit de désinstaller cet équipement sans préavis.

3.3. Internet

Dans un contexte de partage équitable des ressources, tous les usagers doivent faire une utilisation raisonnable et responsable d'Internet. À moins qu'un contexte éducatif ou administratif le justifie, il est interdit de faire une utilisation d'Internet demandant l'envoi ou la réception de beaucoup de données (ex. : écouter la radio en ligne, écouter des vidéos en ligne, écouter de la musique en ligne, jouer à des jeux en ligne, etc.). Dans les écoles et les centres, les élèves doivent suivre la procédure d'autorisation en vigueur pour l'accès à Internet.

La CSRS peut exercer son droit de surveillance et de contrôle de l'utilisation que ses usagers font de l'outil Internet. Les usagers sont informés qu'il peut y avoir, lorsqu'ils naviguent sur Internet, un contrôle et une compilation des sites visités. Des données d'accès à Internet, notamment aux pages WEB, ainsi que l'heure, la durée, les services et les protocoles utilisés sont électroniquement enregistrés. Au besoin et suivant une

procédure stricte relativement à la confidentialité, ces données sont disponibles pour une analyse détaillée des accès à Internet pour un ou plusieurs usagers.

Dans l'éventualité d'une utilisation malveillante d'Internet par un usager de la CSRS, des démarches appropriées et respectueuses d'intervention et d'aide technique, si nécessaire, seront faites auprès de la personne prise en défaut afin de corriger la situation. En cas de récidive, la CSRS se réserve le droit d'appliquer les sanctions appropriées.

3.4. Communication électronique

Pour toute communication électronique envoyée avec les ressources informatiques de la CSRS, tout usager doit s'identifier à titre de signataire et préciser, s'il y a lieu, à quel titre il s'exprime. Les communications par courrier électronique doivent respecter les mêmes règles de confidentialité et de respect que tout autre type de communication.

L'envoi de courriels à des groupes, notamment des groupes de parents, doit être fait de manière sécuritaire. Pour envoyer un message sans que les noms et adresses courriels des destinataires soient visibles à tous ceux qui recevront le courriel, vous devez utiliser la case « Cci ». Ainsi, la confidentialité des courriels des parents sera respectée et nous éviterons des fuites de renseignements personnels.

La CSRS peut exercer son droit de surveillance et de contrôle de l'utilisation que ses usagers font de l'outil courrier électronique, tout en leur donnant une expectative raisonnable quant à leur vie privée. Dans l'éventualité d'une utilisation malveillante du courrier électronique par un usager de la CSRS, des démarches appropriées et respectueuses d'intervention et d'aide technique si nécessaire seront faites auprès de la personne prise en défaut afin de corriger la situation. En cas de récidive, la CSRS se réserve le droit d'appliquer les sanctions appropriées.

Lorsqu'un employé quitte la CSRS, cette dernière se réserve le droit de conserver l'adresse électronique de l'employé pendant un délai raisonnable suivant son départ afin de s'assurer que les communications importantes continuent, à court terme, d'être transmises à l'organisme.

3.5. Médias sociaux

À la CSRS, l'utilisation pédagogique des médias sociaux est encouragée dans la mesure où les différents intervenants s'assurent de respecter l'encadrement légal de chaque outil et s'engagent à promouvoir le savoir-vivre en ligne. Par la nature publique des médias sociaux, il est attendu des différents usagers de la CSRS, lorsqu'ils communiquent ou amorcent des projets par ces médias électroniques, qu'ils respectent les mêmes règles de confidentialité et de respect qu'avec tout autre type de médias. Les usagers sont responsables des informations qu'ils publient sur les médias sociaux.

L'accès aux médias sociaux par les ressources informatiques de la CSRS constitue un privilège. Dans l'éventualité d'une utilisation inappropriée des médias sociaux par un usager de la CSRS, des démarches appropriées et respectueuses d'intervention et d'aide technique si nécessaire seront faites auprès de la personne prise en défaut afin de corriger la situation. En cas de récidive, la CSRS se réserve le droit d'appliquer les sanctions appropriées.

Afin de protéger ses usagers face à des phénomènes tels que le cyberharcèlement, la cyberintimidation, le vol d'informations personnelles ou l'accès à des contenus inappropriés, la CSRS se réserve le droit d'offrir un accès restreint aux principaux médias sociaux selon les types d'usagers.

Les usagers ne doivent pas publier des informations personnelles, confidentielles, restreintes ou diffamatoires à propos de la CSRS ou des autres usagers. Les usagers ne doivent pas publier ou distribuer du matériel protégé par la loi sur les droits d'auteur sans les autorisations des propriétaires. Les usagers ne doivent pas utiliser le nom, le logo ou l'image de la CSRS pour promouvoir un produit, une cause ou une opinion dans les médias sociaux sans avoir l'autorisation du Service des communications de la CSRS.

La CSRS est présente sur les principaux médias sociaux. Le Service des communications est responsable des publications via ceux-ci. Les unités administratives désirant avoir une présence dans les médias sociaux doivent en faire la demande auprès du Service des communications de la CSRS. Le Service des communications se réserve le droit de refuser ou d'accepter chaque demande.

3.6. Utilisation des ordinateurs, équipements ou logiciels personnels

L'utilisation d'un équipement informatique personnel à la CSRS est autorisée. Cette utilisation est un privilège et non un droit. Lorsque les usagers sont connectés au réseau de la CSRS avec leurs équipements personnels, ils s'engagent à respecter la politique d'utilisation des ressources informatiques et les procédures qui en découlent.

Afin de s'assurer de la performance et de la sécurité du réseau de la CSRS, les usagers s'engagent à ne pas connecter leur équipement informatique personnel au réseau filaire dans la CSRS. Par conséquent, l'accès au réseau et à Internet doit seulement être fait en utilisant le réseau sans fil (Wi-Fi).

À moins d'entente particulière, la CSRS n'assume aucune responsabilité de la perte, du vol ou du bris des appareils personnels apportés à la CSRS. De plus, la CSRS n'assume aucune responsabilité de tout coût engendré par l'utilisation des appareils personnels apportés à la CSRS par les usagers.

3.7. Sécurité de l'information

Les mesures de sécurité doivent être proportionnelles à la valeur de l'information à protéger. Elles doivent être établies en fonction des risques, de leur probabilité d'occurrence et de leurs conséquences.

Toute unité administrative assumant la gestion ou la mise à jour d'un système d'information institutionnel, par exemple le système de rémunération, doit désigner un gestionnaire responsable du système. Cette personne doit, entre autres, être responsable de la confidentialité du système.

Tout système d'information institutionnel doit être protégé, au minimum, par un processus d'accès nécessitant un mécanisme d'identification et d'authentification de l'usager. L'accès au système doit être limité aux personnes autorisées seulement, en fonction de la nature de l'information et des applications utilisées. Tout gestionnaire de système d'information institutionnel doit mettre en place, avec l'aide du SRMTI, des mesures adéquates de contrôle et de sécurité afin d'assurer la protection et le bon fonctionnement du système.

La classification des informations est essentielle, car elle identifie le niveau de sécurité qu'il faut attribuer aux informations concernées en fonction de leur importance. Elle permet à la CSRS d'établir une base servant à la

protection contre la perte, l'usage abusif et la divulgation non autorisée. Une information peut être catégorisée sous trois grandes classes :

a) Publique : cette information peut être distribuée sans restriction à l'intérieur comme à l'extérieur de la CSRS. Elle est généralement informative. Sa divulgation ne risque pas de causer des dommages aux individus ou à la CSRS.

b) Privée : cette information est strictement d'usage interne. Les employés ou les commissaires peuvent s'en servir pour effectuer leur travail. Il pourrait y avoir des impacts indirects si les informations de cette classe étaient dévoilées au public.

c) Confidentielle : les renseignements nominatifs et les renseignements consignés au dossier des élèves et des employés, quel qu'en soit le support, ont un caractère confidentiel. Elle nécessite le plus haut niveau de sécurité. Leur divulgation pourrait causer des dommages importants à la CSRS.

L'information contenue dans les ressources informatiques de la CSRS est confidentielle si elle a le caractère d'un renseignement nominatif ou d'un renseignement que la CSRS peut ou doit protéger en vertu d'une loi, d'un règlement, d'un contrat ou d'une entente de confidentialité. Personne ne doit, à des fins autres que pour la réalisation de la mission de la CSRS, divulguer une information considérée comme confidentielle.

Les usagers des ressources informatiques doivent assumer la responsabilité de la précision, de la sécurité, de l'intégralité de l'information et des traitements effectués sur les équipements qu'ils utilisent. Ils doivent protéger la confidentialité des renseignements qu'ils peuvent détenir, soit dans le cadre de leurs fonctions à titre d'employés, soit dans le cadre d'une entente formelle avec la CSRS à titre de client ou fournisseur, soit privément à titre personnel, et, s'il y a lieu, en protéger l'accès par un mot de passe.

3.8. Surveillance et contrôle

La CSRS peut exercer son droit de surveillance et de contrôle de l'utilisation que les usagers font des ressources informatiques.

La protection des ressources informatiques organisationnelles (c'est-à-dire, les ressources dans les salles des serveurs) et de leur contenu relève du SRMTI. À cet effet, ce dernier doit instaurer des mesures adéquates et continues de contrôle et de sécurité pour protéger les installations institutionnelles mises sous sa responsabilité.

La protection des ressources informatiques locales (c'est-à-dire, dans les unités administratives) et de leur contenu incombe aux unités administratives qui en sont les utilisatrices. À cet effet, ces unités doivent respecter les standards techniques établis par le SRMTI relativement aux équipements et à leur configuration respective qui sont implantés dans les unités.

Des vérifications ou audits sont normalement effectués sur l'initiative de la direction des SRMTI ou à la suite de demandes qui lui sont formulées par l'autorité d'une unité administrative en collaboration avec le Service des ressources humaines qui a des raisons sérieuses et suffisantes de croire qu'un usager utilise les ressources informatiques et de télécommunication en contravention à la présente politique, au code de conduite, aux lois ou aux règlements de la CSRS.

3.9. Droits d'auteur

Les reproductions de logiciels, de progiciels, de pages WEB ou d'objets numérisés ne sont autorisées qu'à des fins de copies de sécurité ou selon la norme de la licence d'utilisation qui les régit.

Personne ne doit effectuer ou participer à la reproduction de logiciels, de progiciels, de pages WEB, d'objets numérisés ou de leur documentation, sans le consentement du propriétaire du droit d'auteur. De plus, personne ne doit utiliser de reproductions illicites de ce type de matériel sur les ressources informatiques de la CSRS ou sur tout autre équipement ne lui appartenant pas, mais utilisé dans ses locaux.

Toutes les pages WEB ou logiciels développés par les employés et les élèves dans le cadre formel de travail ou d'étude (exemple, une page WEB développée par un élève d'une école ou d'un centre et déposée officiellement sur le site WEB de l'école, du centre ou de la CSRS) sont la propriété de la CSRS qui doit elle-même respecter, s'il y a lieu, les droits d'auteur des développeurs.

Annexe 1

Code de conduite sur l'utilisation et la gestion des ressources informatiques de la CSRS

Le présent code de conduite doit être respecté par toute personne qui utilise ou qui gère des ressources informatiques de la CSRS, tel que défini dans la Politique sur l'utilisation des ressources informatiques.

1. Code de conduite des usagers

- Utiliser les ressources informatiques de manière efficace et licite;
- Utiliser seulement les codes d'accès et/ou les mots de passe pour lesquels il a obtenu une autorisation d'usage;
- Être responsable des activités résultant de l'usage de ses codes d'accès et/ou mots de passe;
- Prendre des mesures raisonnables afin de protéger ses codes d'accès, ses mots de passe ainsi que l'intégrité et la confidentialité des ressources informatiques utilisées;
- S'abstenir d'utiliser les ressources informatiques à des fins non autorisées ou illégales;
- S'assurer que l'usage personnel qu'il fait des ressources informatiques n'entrave pas la performance au travail des autres usagers;
- Minimiser l'espace disque qu'il utilise en évitant le stockage d'information désuète, redondante ou personnelle;
- Obtenir l'autorisation de son supérieur immédiat avant d'emprunter une ressource informatique;
- Ne pas, sans autorisation du propriétaire, accéder à, modifier, reproduire, détruire ou lire des informations, des programmes ou des logiciels;
- Ne pas brancher dans les prises réseau de l'équipement qui n'a pas été approuvé par le SRMTI;
- Ne pas installer, altérer ou réparer du câblage réseau sans l'approbation du SRMTI;
- Ne pas installer de l'équipement qui retransmet ou altère les signaux du réseau sans fil de la CSRS;
- Respecter les droits d'auteur des logiciels, des informations et de la documentation utilisés;
- Respecter le droit à la vie privée des autres usagers notamment en ce qui a trait à l'utilisation et à l'accès au contenu du courrier électronique, des boîtes vocales, de la téléphonie ou tout autre média de communication;
- Respecter les conventions d'accès et d'usage des réseaux internes et externes, et correctement identifier sa correspondance électronique;
- Collaborer avec les gestionnaires de réseau(x) ou de système(s) afin de faciliter l'identification et la correction de problèmes ou d'anomalies pouvant se présenter;
- Informer le responsable du réseau ou du système concerné de tout usage non autorisé de ses codes d'accès et /ou mots de passe;
- Éviter tout comportement nocif ou malveillant tel que les suivants, indiqués à titre d'exemple:
    - intrusion ou tentative d'intrusion non autorisée dans un ordinateur ou système informatique;
    - usage volontaire de programmes ou autres moyens qui endommagent les ressources informatiques ou leur contenu (ex. virus informatiques);

- usage de programmes, de logiciels ou autres moyens en vue d'intercepter, de collecter, de prendre connaissance, de décrypter ou de décoder de l'information (ex. code d'usager, clé d'accès, fichier ou mot de passe) véhiculée sur un réseau ou résidant sur un poste de travail;
- usage de subterfuges ou de moyens pour transmettre du courrier électronique de façon anonyme, pour usurper l'identité d'un usager ou en masquant son identité;
- utilisation du courrier électronique, de la messagerie vocale ou des médias sociaux 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 règlements de la CSRS;
- utilisation sans autorisation du code d'accès et/ou mot de passe d'un tiers;
- lecture, modification, destruction ou diffusion non autorisée d'informations, de programmes ou de logiciels appartenant à un tiers;
- interférence volontaire en vue de dégrader la performance d'un poste de travail, d'un système ou d'un réseau;
- 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 ou à des fins personnelles (« spamming »).

2. Code de conduite des gestionnaires

Toute personne responsable de la gestion des ressources, d'équipements, de systèmes ou réseaux informatiques a certaines obligations envers les usagers et l'infrastructure matérielle, logicielle et informationnelle sous sa responsabilité. Elle doit en particulier:

- S’assurer de l'application dans leur milieu de la politique et des procédures qui en découlent;
- Informer, responsabiliser et sensibiliser les usagers au respect de la politique et des procédures qui en découlent;
- Sensibiliser les usagers à l'utilisation saine et sécuritaire des ressources informatiques;
- Administrer les ressources informatiques de manière licite et efficace;
- Respecter le caractère confidentiel de l'information emmagasinée par les usagers lors de toute intervention de gestion;
- Prendre des mesures adéquates afin que les usagers puissent travailler dans un environnement garantissant la sécurité et la confidentialité des informations;
- Informer les usagers des conventions d'usage des logiciels et de protection des informations se trouvant dans les ressources sous sa responsabilité;
- Prévenir la modification, la corruption et la reproduction illicite des informations, des programmes et des logiciels (incluant la documentation) sous sa responsabilité;
- Informer la direction du SRMTI de tout manquement à la Politique de sécurité sur l'utilisation des technologies de l'information et des télécommunications et au présent Code de conduite et collaborer aux suites à donner.