Amendements au Règlement relatif à l'utilisation des ressources informatiques et de télécommunications

Le SPUQO propose plusieurs types d'amendements au règlement. Les buts poursuivis sont les suivants:

1- Permettre l'atteinte des objectifs du règlement en ciblant les enjeux pertinents et en évitant les formulations à portée invasive.
2- Compléter le règlement par l'ajout de définitions et de modalités.
3- Poser le principe de : « 3° l'équivalence fonctionnelle des documents et leur valeur juridique, quels que soient les supports des documents, ainsi que l'interchangeabilité des supports et des technologies qui les portent ;», principe reconnu dans la *Loi concernant le cadre juridique des technologies de l'information*, art.1, 3e par. (Éditeur officiel du Québec). Il en découle que la direction n'a pas plus le droit d'ouvrir un courriel qu'une lettre cachetée et mise dans le courrier interne de l'UQO pour envoi.
4- Reconnaître que l'UQO est déjà protégée d'un éventuel usage illégal de ses ressources informatiques par la *Loi concernant le cadre juridique des technologies de l'information,* aux articles 22 et 36. En effet, l'UQO, pour la plupart des documents et informations présents ou circulant via les ressources informatiques et communicationnelles de l'Université, agit à titre d'hébergeur et de transporteur d'informations, un peu comme une entreprise de télécommunications ou un *Icloud*. À ce titre, 1- la responsabilité de la direction de l'UQO est limitée et 2- elle ne peut accéder aux données ni fouiller dans les documents et échanges d'information comme bon lui semble : elle « peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite …» .
    a.

> *Art.22*. Le prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci.
>
> Cependant, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité.
>
> De même, le prestataire qui agit à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche, n'est pas responsable des activités accomplies au moyen de ces services. Toutefois, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les services qu'il fournit servent à la réalisation d'une activité à caractère illicite et s'il ne cesse promptement de fournir ses services aux personnes qu'il sait être engagées dans cette activité.

2001, c. 32, a. 22.

b.
art. 36 : Le prestataire de services qui agit à titre d'intermédiaire pour fournir les services d'un réseau de communication exclusivement pour la transmission de documents technologiques sur ce réseau n'est pas responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission et pendant le temps nécessaire pour en assurer l'efficacité.

Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui :

1° en étant à l'origine de la transmission du document ;

2° en sélectionnant ou en modifiant l'information du document ;

3° en sélectionnant la personne qui transmet le document, qui le reçoit ou qui y a accès ;

4° en conservant le document plus longtemps que nécessaire pour sa transmission.

2001, c. 32, a. 36.

5- Rendre le règlement plus équitable en tenant compte des droits et des devoirs des diverses parties intéressées. Plus particulièrement, des ajouts significatifs sont apportés afin de tenir compte du principe de responsabilité des organisations et des institutions eu égard à la protection des données, de la formation du personnel, etc. Ce principe est prévu dans la *Loi sur la protection des renseignements personnels et les documents électroniques*, dans d'autres législations nationales et dans des accords cadres internationaux (voir la note no 1 pour la source). Le Commissariat Canadien à la protection de la vie privée en fait un principe tellement important qu'il demande au Gouvernement fédéral d'indiquer dans la Loi que les « organisations ont l'obligation de démontrer, sur demande, … qu'elles prennent leurs responsabilités et d'assujettir à l'examen de la Cour fédérale certaines dispositions relatives à la responsabilité » (Voir note no 1, p. 19).
6- Répondre aux exigences éthiques de la recherche. Vu le caractère particulier de la recherche universitaire, et l'engagement de confidentialité des données de recherches pris par les professeurs-chercheurs nous avons adapté en conséquence la protection des données confidentielles. Plus particulièrement, selon l'article 5.1 de l'énoncé de politique des trois conseils (Éthique de la recherche avec les êtres humains) : « les établissements doivent aider les chercheurs à tenir leurs engagements de confidentialité ». Un établissement qui viole ses obligations aux termes de la politique s'expose à devenir inadmissible à recevoir des fonds de recherche des organismes subventionnaires.
7- Reconnaître que plusieurs des données produites par les divers membres de la communauté universitaire, dont les professeurs, chargés de cours et étudiants, leur appartiennent en propre, ne sont pas la propriété de l'Université, même si produites à l'occasion du travail ou des études à l'UQO et en utilisant les divers supports informatiques et électroniques mis à leur disposition par l'Université. Et reconnaître les

obligations de l'Université de ne pas tenter d'accéder par quelque moyen que ce soit à ces données. Respecter la propriété intellectuelle telle que prévue notamment à l'article 12 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* de même que l'article 23.03 de la convention collective des professeur.es; 25.05 de la convention collective des chargé.es de cours ainsi que la *Politique et règles en matière de gestion de la propriété intellectuelle* de l'UQO. http://uqo.ca/sites/default/files/fichiers-uqo/propriete-intellectuelle.pdf

8- Empêcher l'utilisation par l'Université d'information contenue dans les documents électroniques ou empêcher à l'Université de donner un accès à ces documents sans le consentement explicite du propriétaire de ces données. L'Université n'a pas le pouvoir d'autoriser une tierce personne (physique ou morale) à accéder ou utiliser l'information contenue dans les documents électronique sans le consentement explicite du propriétaire de ces données.
9- Assurer de manière efficace la sécurité des données qui sont hébergées dans les installations informatiques de l'Université tels que les renseignements personnels, les données de recherches confidentielles, boites de courriels, etc. Ceci permettra à la communauté universitaire d'éviter d'une part, la perte de confiance dans la gestion des technologies informatiques et données électroniques de l'UQO, et d'autre part, d'éventuelles poursuites civiles de plus en plus coûteuses contre les organisations et institutions pour les manquements à ces obligations.
10- Élaborer des politiques précises de contrôle d'accès aux ressources informatiques permettant d'assurer la sécurité des données. Des politiques de haut niveau peuvent être élaborées par le comité aviseur. L'Université aura alors pour tâche de proposer des règles organisationnelles et des installations technologiques pour opérationnaliser ces politiques.
11- Les risques de perte de réputation de l'Institution et de la communauté universitaire mettent à mal l'idée même d'Université : la relation de confiance entre le personnel et les étudiant.es, et plus particulièrement, la relation pédagogique, est mise en jeu de même que la possibilité de mener à bien de nouvelles recherches. Une des bases essentielle de la recherche dans plusieurs disciplines repose sur la confiance qu'ont les répondant.es que les données de la recherche demeureront anonymes et confidentielles.
12- Établir des pratiques saines pour la gestion des technologies de l'information. En particulier, il faut prendre très au sérieux la sécurité de l'information en allouant des budgets spécifiques pour la formation du personnel et l'acquisition des meilleures technologies de protection. De plus, il faut traiter en toute transparence toute violation des ressources informatiques gérées par l'Université et rendre obligatoire le signalement de ces violations à la communauté universitaire. Plusieurs gouvernements en Occident imposent désormais ces pratiques de divulgation tant aux Commissaires à la protection de la vie privée, qu'aux utilisateurs et employés qui en sont victimes.[1]
13- Poser des balises à l'exercice des pouvoirs énormes confiés au seul Responsable en tenant compte des droits et libertés en jeu.
14- Ajouter des règles au sujet du fonctionnement du service des STI. Les risques les plus dommageables, même si leur occurrence est faible, sont souvent le fait des

[1] Voir le document : Commissariat à la protection de la vie privée du Canada. 2013. *Arguments* Le Commissariat fédéral à la protection de la vie privée a publié un guide de bonnes pratiques en la matière : *Un programme de gestion de la protection de la vie privée. La clé de la responsabilité*. 2012. http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_f.pdf

professionnels spécialistes du risque en question. Par exemple, les comptables chez Enron, à l'UQAM et à HEC, les spécialistes des STI comme l'informaticien de la GRC arrêté il y a quelques mois qui est accusé d'avoir piraté (créer une panne de leurs sites pour plus d'une journée) les sites informatiques du ministère de l'éducation et du PLQ lors du conflit étudiant du printemps 2012 (http://fr.canoe.ca/infos/societe/archives/2012/10/20121018-141708.html). De même pour le cas du spécialiste du renseignement américain, Snowden, lequel a réussi à outrepasser ses droits d'accès, et qui a révélé l'espionnage par le gouvernement américain de tous les cellulaires, et ordinateurs. (http://www.lapresse.ca/international/etats-unis/201306/12/01-4660411-snowden-washington-pirate-des-ordinateurs-chinois-depuis-des-annees.php)

15- Retirer du Règlement des règles, pratiques et normes déjà couverts par d'autres règlements et politiques de l'UQO. Par exemple, le fait que de l'intimidation soit exercée via un courriel plutôt que verbalement en face à face, ne change rien à l'application du Code de conduite. Celui-ci couvre déjà l'intimidation exercée par un moyen électronique. Sont maintenus les seuls actes répréhensibles non couverts par les règlements et politiques et liés directement aux technologies en question.

Deux articles d'intérêt

2) http://www.cautbulletin.ca/fr_article.asp?ArticleID=3584

RETOURNER IMPRIMER

Des criminologues recourent aux tribunaux pour protéger la confidentialité de leurs données

Chris Bruckert (à g.) et Colette Parent demandent à la Cour supérieure du Québec de confirmer le privilège de confidentialité.

Deux criminologues de l'Université d'Ottawa se tournent vers les tribunaux pour protéger la confidentialité des renseignements recueillis lors d'une recherche menée en 2007.

Colette Parent et Chris Bruckert demandent à la Cour supérieure du Québec de confirmer le privilège de confidentialité qui est au coeur même de leur pratique en criminologie. À l'origine de leur requête se trouve la volonté des services policiers d'avoir accès à l'enregistrement et à la transcription d'une entrevue que les deux professeures ont faite il y a cinq ans avec un travailleur du sexe montréalais, aujourd'hui accusé de meurtre.

C'est l'ACPPU qui finance l'instance, car l'Université d'Ottawa a refusé d'apporter son aide. Dans une lettre en date du 19 décembre 2012, le recteur de l'Université, Allan Rock, a déclaré à James Turk, directeur général de l'ACPPU, que l'Université d'Ottawa était certes responsable de protéger l'information qui lui était confiée, mais que cette responsabilité n'englobait pas le paiement de frais judiciaires si des chercheurs contestaient la saisie de dossiers de recherche dans le cadre d'une procédure au criminel.

Le Comité d'éthique de la recherche de l'Université d'Ottawa avait approuvé les travaux des criminologues à la condition que les chercheuses s'engagent auprès des participants à protéger leurs informations.

« Il est indispensable de garantir la confidentialité pour arriver à une compréhension de nombreux comportements humains », dit M. Turk. « Sans ces recherches, il est impossible de mettre en place des politiques sociales adéquates et de faire reculer les frontières de la connaissance humaine. »

Il fait un parallèle avec les journalistes d'enquête qui, pour faire des reportages sur des questions cruciales d'intérêt public, doivent parfois être en mesure de s'engager auprès de leurs informateurs à préserver leur anonymat.

« Contrairement à l'Université d'Ottawa qui a refusé de défendre les professeures Bruckert et Parent, les entreprises de presse se rangent du côté de leurs employés et n'hésitent pas à aller jusqu'à la Cour suprême s'il le faut », affirme M. Turk.

Au Canada, toute recherche auprès d'humains qui est financée par l'État doit être approuvée par des comités d'éthique de la recherche dûment constitués et être conforme à l'Énoncé de politique des trois Conseils : Éthique de la recherche avec des êtres humains établi par le gouvernement fédéral. On peut y lire ceci : « Il est essentiel de s'acquitter de ce devoir éthique de confidentialité pour maintenir tant le lien de confiance entre le chercheur et le participant que l'intégrité du projet de recherche. »

Cette politique précise également que « (r)ecueillir des renseignements en contrepartie d'une promesse de confidentialité confère aux chercheurs un devoir éthique qui est essentiel au maintien du respect des participants et à la préservation de l'intégrité du projet de recherche. Tout manquement à la confidentialité peut nuire au participant, à la relation de confiance entre le chercheur et le participant, à d'autres personnes ou à d'autres groupes, ou encore à la réputation du milieu de la recherche. La recherche portant sur des sujets de nature délicate (des activités illégales, par exemple) exige habituellement de solides promesses en matière de confidentialité pour qu'un rapport de confiance soit établi avec les participants. »

Les deux criminologues sont représentées par l'éminent avocat de Toronto, Peter Jacobsen, et par l'avocate montréalaise spécialisée en droit criminel, Nadine Touma. La Cour devrait se pencher sur la question en juin.

2) **http://www.caut.ca/fr/nouvelles/2013/04/23/rapport-d-un-comite-d-enquete-independant**

Rapport d'un comité d'enquête indépendant
(Ottawa, le 23 avril 2013) Une enquête indépendante sur la saisie des dossiers de recherche de deux ex-professeurs de l'Université d'Ottawa par l'Institut de recherche en santé mentale et l'Hôpital Royal Ottawa conclut que cette saisie était injustifiée, qu'elle soulevait des préoccupations en matière d'éthique de la recherche et qu'elle pouvait porter atteinte à la vie privée des sujets des recherches.

Le comité d'enquête a indiqué dans son rapport que « la saisie de dossiers de recherche est une mesure grave que seules des circonstances extrêmes peuvent justifier, lorsque toutes les options raisonnables ont été épuisées ».

En mars 2005, des employés de l'Hôpital Royal Ottawa et de l'Institut de recherche en santé mentale (IRSM) ont saisi, sans préavis, des documents de recherche, des dossiers cliniques, des fichiers informatiques et des documents personnels se rapportant aux travaux effectués par les professeurs Anne Duffy et Paul Grof. On a alors allégué que des personnes qui s'étaient portées volontaires pour participer aux études n'avaient pas signé les formulaires de consentement officiels. Le comité d'enquête souligne qu'« il est très improbable que les sujets de l'une ou l'autre des recherches effectuées par Anne Duffy n'aient pas donné officiellement leur consentement » et que « même si l'on avait constaté l'absence de formulaires de consentement dans les dossiers de recherche, il aurait suffi de simplement rectifier la situation ».

Selon le comité, la saisie des dossiers de recherche, soi-disant en raison de l'absence des formulaires obligatoires de consentement éclairé et dans l'optique du respect des normes d'éthique de la recherche, constituait un manquement à la responsabilité institutionnelle. Il

explique que, dans des études de ce genre, les formulaires ont pour but de protéger la vie privée des sujets et la confidentialité de l'information versée aux dossiers.

Les enquêteurs attribuent la saisie à des tensions constantes entre les deux professeurs et des responsables de diverses fonctions à l'IRSM, l'hôpital Royal Ottawa et l'Université d'Ottawa, et à une méprise entre le consentement éclairé qui vise à protéger la vie privée et la confidentialité des données et le consentement éclairé obtenu en reconnaissance des préjudices que pourrait causer la recherche. Ils font remarquer que lorsque le consentement éclairé a pour objet d'assurer que les chercheurs protègent la confidentialité de renseignements sensibles sur la santé, une saisie comme celle qui s'est produite semble aller à l'encontre même de la finalité du consentement éclairé.

Pour éviter qu'une telle situation se reproduise, le comité d'enquête recommande notamment de préciser la propriété des dossiers de recherche, en partant du principe que les dossiers sont la propriété des chercheurs et non des établissements; d'indiquer clairement, à la signature d'un formulaire de consentement éclairé dans le cadre d'un projet de recherche, si l'intention est de protéger le sujet contre des préjudices possibles, ou de protéger sa vie privée et la confidentialité de l'information communiquée aux chercheurs; de clarifier la responsabilité des établissements face aux mesures à prendre pour garantir que les chercheurs se conforment aux normes d'éthique de la recherche; et d'adopter des lignes directrices établissant explicitement que la saisie des dossiers de recherche est « un dernier recours, une action inéluctable quand le bien-être des sujets de recherche est en danger, et que ce danger est grave et immédiat ».

Le comité a été mandaté par l'Association canadienne des professeures et professeurs d'université, dont il était entièrement indépendant. Il était composé de Trudo Lemmens, LicJur, LL. M. (bioéthique), D.C.L, chaire Scholl en droit et politique de la santé et professeur agrégé des facultés de droit et de médecine à l'Université de Toronto (président); Thomas A. Ban, M.D., F.R.C.P.C., professeur émérite de psychiatrie à l'Université Vanderbilt; et Louis C. Charland, Ph. D., professeur aux départements de philosophie et de psychiatrie et à l'École des études en santé de l'Université Western.

Pour lire le rapport du comité, cliquer sur Report of the Independent Committee of Inquiry into the University of Ottawa, the Institute for Mental Health Research and the Royal Ottawa Hospital (en anglais seulement).
Toutes les nouvelles
- See more at: http://www.caut.ca/fr/nouvelles/2013/04/23/rapport-d-un-comite-d-enquete-independant#sthash.UhCAXjCS.dpuf

Université du Québec en Outaouais	Université du Québec en Outaouais
RÈGLEMENT RELATIF À L'UTILISATION DES RESSOURCES INFORMATIQUES ET DE TÉLÉCOMMUNICATION	**RÈGLEMENT RELATIF À L'UTILISATION DES RESSOURCES INFORMATIQUES ET DE TÉLÉCOMMUNICATION** Modifications SPUQO

1. Principes L'Université reconnaît, pour les membres de la communauté universitaire, le caractère essentiel de l'accès à des ressources informatiques et de télécommunication pour la réalisation des activités reliées à sa mission.	**1. Principes** L'Université reconnaît, pour les membres de la communauté universitaire, le caractère essentiel de l'accès à une infrastructure informatique et de télécommunication pour la réalisation des activités reliées à sa mission. **L'université reconnait que ce service, mis à la disposition de la communauté Universitaire, doit garantir les droits fondamentaux des utilisateurs qui sont protégés par les lois, les conventions collectives ou ententes collectives, le Code du travail, le code civil du Québec, la Charte des droits et libertés de la personne ainsi que les lois et règlements régissant l'Université.** **L'Université reconnaît notamment le droit à la vie privée des membres de la communauté universitaire.** **L'Université reconnaît le droit à la confidentialité des échanges entre les membres de la communauté universitaire et leurs syndicats et associations ainsi que de toutes les communications, documents, et informations syndicales et associatives, qu'elles soient sur support informatique, électronique ou autre. Elle reconnaît aussi le droit à la confidentialité des échanges entre des syndicats et associations avec des personnes ou organisations à l'extérieur de l'Université.**
En tant que propriétaire responsable d'une saine gestion des équipements et des ressources informatiques et de télécommunication, l'Université désire en assurer une utilisation conforme à ses règlements, politiques et à ses procédures ainsi qu'aux lois et règlements applicables.	En tant que propriétaire responsable d'une saine gestion des équipements et des ressources informatiques et de télécommunication, l'Université désire en assurer une utilisation conforme à ses règlements, politiques et à ses procédures ainsi qu'aux lois et règlements applicables. **En tant que propriétaire responsable d'une saine gestion des équipements et des ressources informatiques et de télécommunication, l'Université doit assurer la plus grande protection possible des équipements mis à la disposition de la communauté universitaire ou acquis à même les budgets de recherches des membres de la communauté universitaire, en autant que ceux-ci aient été acquis via le service des achats de l'UQO, ou pour les achats de moins de 1000$, aient été agréé par le service des technologies de l'information.** **En tant que propriétaire responsable d'une saine**

	gestion des équipements et des ressources informatiques et de télécommunication, l'Université doit assurer la protection des données et informations contenues ou transférés via les équipements et ressources informatiques et de télécommunications de l'Université. De plus, elle se doit de garantir la confidentialité absolue des données et des sources de recherche faisant l'objet d'obligations émanant d'organismes subventionnaires ou des commanditaires et des exigences de protection de la confidentialité exigées par le Comité d'éthique de la recherche et des certificats d'éthiques liés à ces recherches. Elle assure la confidentialité des ébauches de textes, travaux de recherche, contacts et collaborateurs de recherche. Elle doit aussi garantir la confidentialité des décisions des assemblées départementales, ce qui inclut la confidentialité des documents préparés, consultés ou échangés entre les membres de ces instances. **L'Université reconnaît le droit à la confidentialité des échanges électroniques et téléphoniques des actes professionnels et exigés par les Ordres professionnels.**
Le présent règlement (ci-après « le Règlement ») n'a pas pour effet de limiter les droits de gestion découlant du statut d'employeur et d'administrateur de l'Université, ni d'empêcher l'Université d'aviser les autorités compétentes de toute infraction régie par la Loi, non plus que d'empêcher quiconque de divulguer et d'informer toute autorité compétente, y compris l'Université, de toute violation d'une loi, ou d'un règlement, d'une politique, d'une procédure de l'Université.	Le présent règlement (ci-après « le Règlement ») n'a pas pour effet de limiter les droits de gestion découlant du statut d'employeur et d'administrateur de l'Université, ni d'empêcher l'Université d'aviser les autorités compétentes de toute infraction régie par la Loi, non plus que d'empêcher quiconque de divulguer et d'informer toute autorité compétente, y compris l'Université, de toute violation d'une loi, ou d'un règlement, d'une politique, d'une procédure de l'Université.
2. Objectifs Les objectifs sont : • d'établir un cadre régissant les conditions d'utilisation des ressources informatiques et de télécommunication; • de protéger ces ressources et les utilisateurs contre une utilisation non-conforme, abusive ou illégale qui pourrait en être faite.	**2. Objectifs** Les objectifs sont : • d'établir un cadre régissant les conditions d'utilisation des ressources informatiques et de télécommunication; • de protéger ces ressources et les utilisateurs contre une utilisation non-conforme, abusive ou illégale qui pourrait en être faite. • de protéger ces ressources et les utilisateurs contre les atteintes à la sécurité et à la confidentialité des communications, documents et données protégés par ce Règlement et les lois.

3. Champ d'application et responsabilité Le Règlement s'applique à tout utilisateur des ressources informatiques et de télécommunication appartenant à l'Université. Le vice-recteur à l'administration et aux ressources est l'autorité responsable (ci-après «le Responsable») du Règlement et peut instaurer des procédures et émettre des directives en application de celle-ci. **4. Définitions** **Réseau:** tout réseau de communication informatique, accessible par l'intermédiaire des ressources informatiques et de télécommunication contrôlées ou administrées par l'Université. **Ressources informatiques et de télécommunication:** notamment les serveurs informatiques, les ordinateurs et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception et de traitement de l'information et tout équipement de télécommunication y compris les appareils de téléphonie cellulaire, les logiciels, progiciels, didacticiels, banques de données et d'informations contrôlées et administrées par l'Université (textuelle, sonore, symbolique ou visuelle) placées dans un équipement ou sur un média informatique. Sont également inclus le système de courrier électronique et le système de messagerie vocale, qu'ils soient la propriété de l'Université ou qu'ils utilisent ou hébergent des actifs dont l'Université est propriétaire, locataire, fiduciaire ou dépositaire ainsi que les fichiers et les dossiers qui peuvent être contenus dans les ordinateurs de bureau ou portatifs.	• **3. Champ d'application et responsabilité** Le Règlement s'applique aux gestionnaires et aux utilisateurs des ressources informatiques et de télécommunication appartenant à l'Université. Le vice-recteur à l'administration et aux ressources est l'autorité responsable (ci-après «le Responsable») du Règlement et peut instaurer des procédures et émettre des directives en application de celle-ci, après un avis favorable quant aux procédures et directives du Comité aviseur des STI. Guy Bellemare 13-6-13 16:56 **Commentaire [3]:** Une autre politique devra être adoptée afin de créer ce comité aviseur et d'en définir le mandat **4. Définitions** **Réseau: Englobe tout support de communication de données, connectés aux ressources informatiques et de télécommunication contrôlées ou administrées par l'Université.** **Ressources informatiques et de télécommunication:** notamment les serveurs informatiques, les ordinateurs et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception et de traitement de l'information et tout équipement de télécommunication y compris les appareils de téléphonie cellulaire, les logiciels, progiciels, didacticiels, banques de données et d'informations contrôlées et administrées par l'Université (textuelle, sonore, symbolique ou visuelle) placées dans un équipement ou sur un média informatique. Sont également inclus le système de courrier électronique et le système de messagerie vocale, qu'ils soient la propriété de l'Université ou qu'ils utilisent ou hébergent des actifs dont l'Université est propriétaire, locataire, fiduciaire ou dépositaire ainsi que les fichiers et les dossiers qui peuvent être contenus dans les ordinateurs de bureau ou portatifs. **Sécurité informatique et des télécommunications** : La sécurité informatique regroupe l'ensemble des moyens juridiques, techniques et organisationnels nécessaires pour assurer la sécurité des systèmes informatiques. Elle permet, en particulier d'assurer la confidentialité, l'intégrité et la disponibilité des ressources informationnelles stockées sur support informatique ou transféré via les réseaux de télécommunication (Wikipedia).

Supérieur immédiat : désigne le cadre immédiatement supérieur à celui de l'utilisateur concerné, si ce dernier est employé de l'Université. Pour les fins de ce règlement, le vice-recteur à l'enseignement et à la recherche agit à titre de supérieur immédiat des professeurs. **Utilisateur:** toute personne, membre ou non de la communauté universitaire, qui utilise les ressources informatiques et de télécommunication de l'Université.	**Supérieur immédiat :** désigne le cadre immédiatement supérieur à celui de l'utilisateur concerné, si ce dernier est employé de l'Université. Pour les fins de ce règlement, le vice-recteur à l'enseignement et à la recherche agit à titre de supérieur immédiat des professeurs. **Utilisateur:** toute personne, membre ou non de la communauté universitaire, qui utilise les ressources informatiques et de télécommunication de l'Université.
5. Règles d'utilisation des ressources ***5.1 Dispositions générales*** L'utilisateur dispose des ressources informatiques et de télécommunication de l'Université pour la réalisation des activités reliées à la mission de celle-ci. L'utilisateur peut y avoir accès seulement dans les limites de l'autorisation qui lui est accordée et en conformité avec le Règlement. L'utilisateur est aussi tenu de se conformer aux normes institutionnelles et à toutes les directives et procédures en découlant. ***5.2 Utilisation personnelle*** L'utilisateur doit se servir des ressources informatiques et de télécommunication mises à sa disposition par l'Université à des fins professionnelles. Toutefois, l'Université reconnaît que l'employé peut utiliser, accessoirement, ces ressources à des fins personnelles dans la mesure où cette utilisation ne cause aucun préjudice à l'Université et qu'elle demeure dans les limites de ce qui est raisonnable. Ce privilège peut être révoqué, en tout temps, à tout utilisateur qui ne se conforme pas au Règlement. ***5.3 Conditions d'utilisation des ressources informatiques et de télécommunication*** Dans l'utilisation des ressources informatiques et de télécommunication, l'utilisateur ne doit pas poser ou tenter de poser un geste abusif ou illégal, contraire aux principes du Règlement comme par exemple : • utiliser un langage injurieux, malveillant, haineux ou discriminatoire; • harceler, menacer, diffamer, ou autrement porter préjudice à une autre personne;	**5. Règles d'utilisation des ressources** ***5.1 Dispositions générales*** L'utilisateur dispose des ressources informatiques et de télécommunication de l'Université pour la réalisation des activités reliées à la mission de celle-ci ainsi que pour ses communications syndicales et professionnelles. L'utilisateur peut y avoir accès en conformité avec le Règlement. L'utilisateur est aussi tenu de se conformer aux normes institutionnelles et à toutes les directives et procédures en découlant. ***5.2 Utilisation personnelle*** L'utilisateur doit se servir des ressources informatiques et de télécommunication mises à sa disposition par l'Université dans le respect des principes formulés à l'article 1. Toutefois, l'Université reconnaît que l'employé peut utiliser, accessoirement, ces ressources à des fins personnelles dans la mesure où cette utilisation est conforme aux lois et règlements en vigueur. ***5.3 Conditions d'utilisation des ressources informatiques et de télécommunication*** Dans l'utilisation des ressources informatiques et de télécommunication, l'utilisateur ne doit pas poser ou tenter de poser un geste abusif ou illégal, contraire aux principes du Règlement comme par exemple :

Louise Briand 13-9-20 12:38

Commentaire [4]: Lorsque des éléments de la colonne de gauche ne sont pas reproduits dans la colonne de droite, c'est parce qu'ils sont déjà couverts par d'autres politiques/règlements.

• diffuser des renseignements personnels concernant un autre utilisateur; • propager des virus informatiques; • accéder ou tenter d'accéder, sans les autorisations requises, aux différents systèmes d'information de l'Université; • usurper l'identité d'un utilisateur; • surcharger intentionnellement le réseau; • décrypter, décoder ou tenter de décrypter ou décoder des codes ou des clés d'accès, de fichiers ou de mots de passe; • consulter ou diffuser du matériel pornographique, obscène ou injurieux; • utiliser les ressources informatiques et de télécommunication à des fins commerciales (incluant la sollicitation et la publicité) sans une autorisation préalable du Responsable de l'application du Règlement; • lire, modifier ou détruire tout message, texte, donnée ou logiciel appartenant à un tiers sans son autorisation; • utiliser les ressources informatiques et de télécommunication à des fins autres que celles pour lesquelles elles sont rendues disponibles.	• propager des virus informatiques; • accéder ou tenter d'accéder, sans les autorisations requises, aux différents systèmes d'information de l'Université; • usurper l'identité d'un utilisateur; • surcharger intentionnellement le réseau; • décrypter, décoder ou tenter de décrypter ou décoder des codes ou des clés d'accès, de fichiers ou de mots de passe; • lire, modifier ou détruire tout message, texte, donnée ou logiciel appartenant à un tiers sans son autorisation; • utiliser les ressources informatiques et de télécommunication à des fins autres que celles pour lesquelles elles sont rendues disponibles. • Par ailleurs, l'Université reconnaît le droit aux utilisateurs d'être systématiquement informés de tout logiciel installé sur leurs ordinateurs et les effets possibles de ce logiciel sur la confidentialité des données qui y sont hébergées. En particulier, l'utilisateur doit être informé de tout logiciel installé, permettant de communiquer la trace de ses activités sur l'ordinateur ou ceux permettant de prendre le contrôle de l'ordinateur à distance.
Seul le Responsable peut autoriser une dérogation à l'une ou l'autre des interdictions précitées lorsque cette dérogation est requise dans le cadre des activités de l'Université. Exceptionnellement, cette même dérogation peut être consentie par le vice-recteur à l'enseignement et à la recherche lorsque l'interdiction visée concerne une activité d'enseignement ou de recherche. Dans un tel cas, ce dernier en avise le Responsable dans les plus brefs délais.	Seul le Comité aviseur des STI, sur avis du Responsable ou du VRER, lorsque l'interdiction visée concerne une activité d'enseignement ou de recherche, peut autoriser une dérogation à l'une ou l'autre des interdictions précitées lorsque cette dérogation est requise dans le cadre des activités de l'Université. Tout refus de déroger à la politique peut faire l'objet d'une demande de révision du ou de la personne requérante auprès du Comité. Si la décision du Comité est maintenue, cette personne peut déposer un grief à l'encontre de cette décision.
L'installation, le déplacement, la désinstallation ou l'utilisation d'un équipement personnel sur le réseau de l'Université doit être préalablement autorisé par le directeur du Service des technologies de l'information (ci-après le STI).	L'installation ou l'utilisation d'un équipement person sur le réseau de l'Université doit être préalablem autorisé par le directeur du Service des technologies l'information (ci-après le STI).

Guy Bellemare 13-6-19 15:46

Commentaire [5]: Cet article doit être retiré ou balisé, car, cela empêcherait, par exemple, un invité de brancher son ordinateur portable sur le réseau de l'UQO pour donner un séminaire. Il y a aussi des prof./CC qui utilisent leurs ordinateurs portables perso. pour enseigner et ils doivent se brancher sur le réseau de l'UQO pour accéder à Moodle.

6. Mot de passe et confidentialité ***6.1 Mot de passe*** Lorsque l'Université fournit un compte à un utilisateur, auquel est rattaché un mot de passe, ce dernier est tenu d'en conserver la confidentialité et d'en assurer une gestion conforme aux directives établies à cet effet par le STI. Lorsqu'un utilisateur oublie un mot de passe et qu'il ne peut le récupérer à partir des applications de gestion de compte fournies par l'Université, il doit en aviser le STI. Si l'utilisateur s'aperçoit qu'une tierce personne s'est approprié son mot de passe, il doit en aviser sans délai le STI. ***6.2 Confidentialité*** L'utilisateur doit respecter la confidentialité des communications avec les autres utilisateurs, lorsqu'il en est fait expressément mention. Il est également interdit de consulter ou de traiter de l'information disponible sur un poste de travail laissé temporairement sans surveillance sans l'autorisation de son utilisateur désigné. Dans le cas d'une absence du titulaire du poste de travail, l'accès à l'information contenue sur toute ressource informatique et/ou de télécommunication peut être demandé par le supérieur immédiat et doit être autorisé par le Responsable.	**6. Mot de passe et confidentialité** ***6.1 Mot de passe*** Lorsque l'Université fournit un compte à un utilisateur, auquel est rattaché un mot de passe, ce dernier est tenu d'en conserver la confidentialité et d'en assurer une gestion conforme aux directives établies à cet effet par le STI. Les gestionnaires du réseau et les responsables ne doivent, en aucun cas, avoir accès, aux mots de passe des utilisateurs, ni le communiquer à une tierce personne. Lorsqu'un utilisateur oublie un mot de passe et qu'il ne peut le récupérer à partir des applications de gestion de compte fournies par l'Université, il doit en aviser le STI. Si l'utilisateur s'aperçoit qu'une tierce personne s'est appropriée son mot de passe, il doit en aviser sans délai le STI. ***6.2 Confidentialité*** L'utilisateur doit respecter la confidentialité des communications avec les autres utilisateurs, lorsqu'il en est fait expressément mention. Il est également interdit de consulter ou de traiter l'information disponible sur un poste de travail lais temporairement sans surveillance sans l'autorisation son utilisateur désigné. Dans le cas d'une absence du titulaire du poste travail, l'accès à l'information contenue sur to ressource informatique et/ou de télécommunication faire l'objet d'une autorisation à distance du titulaire défaut de joindre le titulaire et d'une urgence grave (à définir), le Responsable doit demander au Com l'autorisation de permettre l'accès au contenu. aucun cas, cet accès ne peut concerner la confidentialité liée aux activités de recherche, professionnelles, personnelles et des assemblés départementales et syndicales. Cet accès au contenu, doit se faire en présence d'un avocat et d'un représentant syndical ou de l'association qui représente le titulaire. Lorsque, en vertu de l'absence prolongée de la personne (par exemple, en congé sabbatique ou autre congé prolongé), l'impossibilité d'accéder à l'information contenue dans un fichier ou équipement imposerait une contrainte excessive à l'établissement, l'université doit prendre les moyens nécessaires pour contacter cette personne afin d'obtenir son autorisation pour accéder au fichier visé. À défaut de pouvoir

Guy Bellemare 13-6-19 13:28

Commentaire [6]: Ce paragraphe doit être retiré car il n'est pas spécifique à l'utilisation des RIT. Par ailleurs, il y a beaucoup de cas particuliers ou la confidentialité d'une communication doit être brisée même si elle a été expressément demandée. La communication peut être en violation des règlements, doit être communiqué au syndicat, etc.

Guy Bellemare 13-5-30 09:03

Commentaire [7]: À qualifier autrement

	contacter cette personne, il faut en référer à l'article 8.3.
	Lors du remplacement des ordinateurs mis à la disposition des professeurs
7. Information	**7. Information**
7.1 Propriété intellectuelle	***7.1 Propriété intellectuelle***
L'utilisateur doit, en tout temps, respecter les droits de propriété intellectuelle et les droits d'utilisation des logiciels, des données ou des équipements utilisés.	L'utilisateur doit, en tout temps, respecter les droits de propriété intellectuelle et les droits d'utilisation des logiciels, des données ou des équipements utilisés.
La reproduction de logiciels n'est autorisée qu'à des fins de copies de sécurité ou selon les normes institutionnelles de la licence d'utilisation la régissant ou avec le consentement du titulaire du droit d'auteur.	La reproduction de logiciels n'est autorisée qu'à des fins de copies de sécurité ou selon les normes institutionnelles de la licence d'utilisation la régissant ou avec le consentement du titulaire du droit d'auteur.
	L'Université reconnait que les professeur.es, personnes chargé.es de cours et étudiant.es conservent la propriété intellectuelle de leurs écrits, y incluant la garde et le contrôle de tous les documents : ceux-ci incluent les communications, fichiers et dossiers personnels et professionnels stockés ou transférés sur un ou via le système ou le réseau informatique ou les comptes de messagerie électronique de l'établissement. En aucun moment, elle ne peut empêcher ces personnes d'accéder à leurs productions intellectuelles.
7.2 Protection de l'information et des renseignements personnels	***7.2 Protection de l'information et des renseignements personnels***
L'information contenue dans les systèmes informatiques est confidentielle si elle a le caractère d'un renseignement personnel ou d'un renseignement que l'Université peut ou doit protéger en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q. c. A-2.1).	L'information contenue dans les systèmes informatiques est confidentielle si elle a le caractère d'un renseignement personnel ou d'un renseignement que l'Université peut ou doit protéger en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q. c. A-2.1).
Dans les cas d'utilisation non conforme aux lois, au Règlement ou à toute réglementation en matière de sécurité, de même que dans les situations de force majeure, hors de son contrôle, l'Université ne peut assurer à l'utilisateur la confidentialité de ses informations et renseignements personnels.	L'Université s'engage à communiquer systématiquement à l'ensemble des utilisateurs toute violation accidentelle ou intentionnelle de la sécurité de ses systèmes et qui a ou aurait pu avoir comme conséquence une perte de confidentialité ou d'intégrité des données qui y sont hébergés.
L'utilisateur ayant besoin d'assurer une protection particulière de certaines informations hébergées sur les systèmes de l'Université, en vertu d'une subvention ou d'une entente avec une organisation externe, doit prendre les mesures nécessaires convenues préalablement avec	Lors du remplacement des ordinateurs mis à disposition du personnel, l'Université s'assure de la confidentialité de la destruction des données qui y sont stockées.

Guy Bellemare 13-5-30 09:06
Commentaire [1]: Rendu inutile par suite des amendements

le Service des technologies de l'information.	
8. Application du Règlement ***8.1 Contrôle et vérification***	**8. Application du Règlement** ***8.1 Contrôle et vérification***
Dans le cadre de ses activités de contrôle et de vérification, l'Université reconnaît son obligation de respecter la dignité, la liberté d'expression et la vie privée des utilisateurs.	Dans le cadre de ses activités de contrôle et de vérification, l'Université reconnaît son obligation de respecter la dignité, la liberté d'expression et la vie privée des utilisateurs.
Toutefois, le Responsable peut procéder à toutes les vérifications d'usage jugées nécessaires pour assurer le respect de ses dispositions, ainsi que des autres règlements, politiques, procédures et normes institutionnelles ou des lois et règlements provinciaux ou fédéraux.	Toutefois, le Responsable peut procéder à une demande de vérification auprès du Comité aviseur des STI. Tout autre utilisateur de la communauté universitaire peut formuler une demande de vérification auprès de ce Comité. Une fois autorisé, le responsable ou son représentant désigné peut accéder à un fichier d'un compte utilisateur enregistré sur le réseau ou à tout autre équipement identifié à l'article 4 sans la permission de l'utilisateur dans les circonstances suivantes : a- Lorsqu'une action immédiate s'impose pour protéger l'intégrité du réseau informatique, une preuve à cet effet pouvant être réclamée par le ou les utilisateurs visés par cette intervention par la suite; b- Dans le cadre d'une perquisition menée par les autorités policières agissant en vertu de l'ordonnance d'un tribunal compétent; Dans tous les autres cas, l'Université informe la personne et son association ou syndicat avant d'accéder au compte utilisateur, ou autre équipement visé à l'article 4, de cette personne. Lorsqu'une notification préalable n'est pas possible, l'Université informe sans délai l'association ou le syndicat et poursuit ses démarches pour que cette personne en soit avisée le plus rapidement possible. Tout accès à un fichier ou autre équipement visé à l'article 4 d'un utilisateur de la communauté universitaire par le Responsable ou son représentant est consigné dans un journal d'exploitation prévu à cet effet. Le nom de la personne ayant accédé au fichier du membre de la communauté universitaire ainsi que la date, l'heure et la raison de l'accès sont enregistrés dans le journal. Les membres de la communauté universitaire ont le droit de consulter toutes les entrées au journal qui ont trait à leur compte utilisateur, ou autre équipement visé à l'article 4.

Guy Bellemare 13-5-28 10:31

Commentaire [2]: Rendu inutile vu les modifications apportées au règlement. La protection est garantie a priori avec nos amendements et l'administration n'y a jamais accès.

	L'Université doit rendre public une fois l'an sur son site web le nombre de communications effectuées chaque trimestre à des autorités chargées de l'application des lois à l'insu de l'intéressé et sans son consentement, et sans mandat, afin de faire la lumière sur la fréquence à laquelle cette exception extraordinaire est invoquée et l'utilisation qui en est faite. Les défauts de la part de l'Université d'aviser et informer les individus ou la communauté universitaire sont passibles de sanctions administratives pécuniaires et de dommages-intérêts légaux. L'Université s'engage à vérifier le caractère valide des requêtes d'organismes externes d'accès à des informations confidentielles, à exiger que l'organisme en question obtienne une ordonnance de la cour en cas de doute et à contester toute demande insuffisamment appuyée.
Une vérification des renseignements personnels et privés d'un utilisateur ou de son utilisation des ressources informatiques et de télécommunication ne peut être effectuée sans le consentement de cet utilisateur, à moins que le Responsable n'ait des motifs raisonnables et probables de croire que cet utilisateur contrevient au Règlement ou abuse des ressources qui lui sont fournies. Le cas échéant, seul le Responsable peut en autoriser la vérification aux conditions qu'il détermine et peut entreprendre les démarches nécessaires pour corriger la situation.	Une vérification des renseignements personnels et privés d'un utilisateur ou de son utilisation des ressources informatiques et de télécommunication ne peut être effectuée sans le consentement de cet utilisateur, à moins que le Responsable n'ait des motifs raisonnables et probables de croire que cet utilisateur contrevient au Règlement ou abuse des ressources qui lui sont fournies. Le cas échéant, le Responsable réfère la situation au Comité aviseur STI qui en décide. Si l'utilisateur donne son consentement, la procédure de vérification est celle spécifiée dans ce règlement. L'Université doit signaler les atteintes à la protection des renseignements personnels et des données confidentielles spécifiées au paragraphe 6.2 au Comité et doit en aviser les personnes concernées afin que des mesures d'atténuation appropriées puissent être prises en temps opportun. Le registre annuel de ces atteintes doit être déposé publiquement au Conseil d'administration de l'UQO. **Le Comité aviseur des STI** Le mandat général de ce comité est défini dans le Règlement créant le Comité aviseur STI. Ce Comité dispose du mandat et des rôles suivants en matière de sécurité informatique et des télécommunications. Ce comité a pour mandat d'étudier la demande de vérification formulée par le Responsable ou par tout autre membre de la communauté universitaire. Il peut en autoriser la vérification aux conditions qu'il

	détermine et doit approuver les démarches nécessaires que le Responsable ou un autre cadre si le Responsable est lui-même impliqué dans la demande de vérification, et approuve les mesures à entreprendre pour corriger la situation. Le Comité approuve toutes les vérifications d'usage légales jugées nécessaires pour assurer le respect de ses dispositions, ainsi que des autres règlements, politiques, procédures et normes institutionnelles ou des lois et règlements provinciaux ou fédéraux. Le comité élabore des politiques générales de sécurité informatique. Il fait le suivi de leurs mises en œuvre aussi bien au niveau technique qu'organisationnel, auprès du ou des services concernés et en informe, sur demande, le conseil d'administration. **Composition du Comité** : Le Comité se compose de 8 membres : deux représentant.es de la direction (VRAR ou son représentant et directeur/directrice des STI, un représentant de chaque groupe suivant : professeur.es, personnes chargées de cours, employé.es de soutien, professionnel.es, étudiant.es chercheur.es et étudiant.es. Ces représentants sont nommés par chacun des syndicats et par l'AGE-UQO. Le Comité peut s'adjoindre, au besoin, les services d'un expert conseil externe en matière de sécurité informatique et des télécommunications, sans droit de vote. Tous les membres du Comité ainsi que le responsable sont tenus à la confidentialité. **Procédure de vérification** : Lorsque la vérification implique l'accès à des données privées et confidentielles, que ces données soient l'objet ou non de la vérification, la vérification doit se faire en présence de la personne suspectée. Cette personne peut se faire accompagner d'un.e représentant.e de son association ou de son syndicat ou d'un.e avocat.e. La personne suspectée et son accompagnateur doivent identifier les fichiers et autres informations protégées par la confidentialité (données personnelles, de recherche, d'assemblées départementales, professionnelles, syndicales ou associatives). En cas de désaccord, la cause est référée aux tribunaux et la sauvegarde confidentielle de tous les éléments contestés doit être assurée. En cas d'urgence, le Responsable en réfère au Comité afin d'obtenir l'autorisation de demander une injonction à un juge. Le Responsable doit veiller à éviter toute surveillance ou contrôle abusif de même qu'à assurer la protection des données recueillies.
Lorsque la vérification implique l'accès à des données privées et confidentielles, que ces données soient l'objet ou non de la vérification, le Responsable doit veiller à éviter toute surveillance ou contrôle abusif de même qu'à assurer la protection des données recueillies.	

Guy Bellemare 13-6-19 15:55
Commentaire [8]: Faut trouver une formulation permettant de limiter les abus du huis-clos.

	Cette vérification doit se faire dans les meilleurs délais. Dans tous les cas, la personne visée doit regagner l'accès à ses données confidentielles et aux données et fichiers non suspectés dans un délai maximal de trois jours.
Lorsqu'une vérification des renseignements personnels et privés d'un utilisateur ou de son utilisation des ressources informatiques et de télécommunication a été effectuée et que l'ensemble du processus de vérification est complété, l'utilisateur doit être informé de la vérification qui a eu lieu, des motifs ayant justifiés celle-ci et des renseignements qui ont été consultés dans ce cadre.	Lorsqu'une vérification des renseignements d'un utilisateur ou de son utilisation des ressources informatiques et de télécommunication a été effectuée et que l'ensemble du processus de vérification est complété, l'utilisateur doit être informé de la vérification qui a eu lieu, des motifs ayant justifiés celle-ci et des renseignements qui ont été consultés dans ce cadre. Afin d'assurer le respect des Principes de ce règlement, des Lois et obligations de l'Université, toute démarche de vérification se fait dans le respect des Principes de ce règlement, des conventions collectives et des lois.
	La sécurité et la protection de la confidentialité au STI Afin d'assurer la rigueur des contrôles de sécurité, et la fiabilité des : équipements, logiciels, services des technologies de l'information, des données des divers utilisateurs des technologies de l'information de l'Université; des procédures de contrôles et d'audits techniques et organisationnels sont mis en place par l'Université. Ces procédures de contrôles et audits techniques et organisationnels sont soumis pour avis au Comité aviseur. À tous les trois ans, un audit externe des procédures de contrôles et d'audits techniques et organisationnels est réalisé et le rapport est soumis au Comité aviseur qui recommande au Responsable les mesures à mettre de l'avant ???
8.2 Procédure de dénonciation	***8.2 Procédure de dénonciation***
Toute personne qui a des motifs raisonnables et probables de croire qu'une utilisation non conforme au Règlement a été commise ou est en voie d'être commise doit, dès que possible, aviser le Responsable et lui fournir tous les renseignements et tous les documents disponibles et pertinents.	Toute personne qui a des motifs raisonnables et probables de croire qu'une utilisation non conforme au Règlement a été commise ou est en voie d'être commise doit, dès que possible, aviser le Responsable et lui fournir tous les renseignements et tous les documents disponibles et pertinents. Si la dénonciation vise le Responsable, celle-ci doit être faite auprès de sa/son supérieur.e immédiat.e. Celui-ci transmet la dénonciation au Comité.
Toute dénonciation est traitée de façon confidentielle.	Toute dénonciation est rapportée par le Responsable

	au Comité et est traitée de façon confidentielle.
8.3 Procédure d'intervention	***8.3 Procédure d'intervention***
A la suite d'une dénonciation, le Responsable, ou une personne qu'il mandate par écrit, peut faire enquête sur les incidents ou faits rapportés. Le Responsable, ou son mandataire, peut prendre tous les moyens nécessaires pour effectuer toutes les vérifications requises, incluant celui d'accéder aux données contenues dans les ressources informatiques et de télécommunication.	A la suite d'une dénonciation, le Responsable, ou une personne qu'il mandate par écrit, après autorisation du Comité, peut faire enquête sur les incidents ou faits rapportés. Le Responsable, ou son mandataire, peut prendre tous les moyens nécessaires légaux et conformes au Règlement pour effectuer toutes les vérifications requises, incluant celui d'accéder aux données contenues dans les ressources informatiques et de télécommunication.
Si une vérification révèle une utilisation non conforme au présent règlement et après avoir donné l'occasion à l'utilisateur concerné de se faire entendre, le Responsable prend toutes les mesures appropriées pour corriger la situation, incluant la possibilité de retirer l'usage des ressources informatiques et de télécommunication à l'utilisateur concerné, et celle d'interdire l'accès aux fichiers personnels et au courrier électronique. Dans un tel cas, le Responsable avisera l'utilisateur concerné ainsi que toute personne en autorité susceptible d'avoir à intervenir dans le dossier, selon les circonstances. Ces mesures ne peuvent avoir pour effet d'empêcher un professeur de l'Université d'avoir accès aux données de ses recherches.	Si une vérification révèle une utilisation non conforme au présent règlement et après avoir donné l'occasion à l'utilisateur concerné de se faire entendre, le Responsable propose au Comité toutes les mesures appropriées pour corriger la situation, incluant la possibilité de retirer l'usage des ressources informatiques et de télécommunication à l'utilisateur concerné et au courrier électronique. En cas d'urgence, il prend ces décisions sur le champ et les soumet par la suite dans les meilleurs délais au Comité, pour approbation. Dans un tel cas, le Responsable avise l'utilisateur concerné ainsi que toute personne en autorité susceptible d'avoir à intervenir dans le dossier, selon les circonstances. Ces mesures ne peuvent avoir pour effet d'empêcher un membre de la communauté universitaire de l'Université d'avoir accès aux données de ses recherches, liées à l'enseignement, et personnelles, ni à ses dossiers protégés par le secret professionnel, ni aux données et documents de son assemblée départementale, ni de communiquer privément avec son syndicat ou association.
L'application des mesures prévues au présent règlement n'exclut pas le recours aux autres dispositifs réglementaires qui pourraient s'appliquer à l'égard des faits reprochés.	L'application des mesures prévues au présent règlement n'exclut pas le recours aux autres dispositifs réglementaires qui pourraient s'appliquer à l'égard des faits reprochés.
Afin de préserver l'intégrité des ressources informatiques et de télécommunication, le Responsable peut, après avoir pris les moyens raisonnables pour aviser l'utilisateur, prendre les mesures suivantes :	Afin de préserver l'intégrité des ressources informatiques et de télécommunication, le Responsable peut, après consultation du Comité et après avoir pris les moyens raisonnables pour aviser l'utilisateur, prendre les mesures suivantes, dans le respect de l'article 8.1 :
• limiter temporairement les services offerts à un ou plusieurs utilisateurs; • interdire l'accès, retirer ou déplacer un équipement informatique ou de télécommunication;	• limiter temporairement les services offerts à un ou plusieurs utilisateurs; • interdire l'accès, retirer ou déplacer un équipement informatique ou de télécommunication;

Guy Bellemare 13-6-19 16:00
Supprimé: , et celle d'interdire l'accès aux fichiers personnels

Guy Bellemare 13-6-19 16:00
Commentaire [9]: Des chargés de cours, des étudiants, dont des employés de l'UQO étudiants peuvent aussi avoir des données de recherche ou des communications associatives dont la confidentialité doit être protégée.

• appliquer les différentes fonctions de diagnostic sur les équipements; • prendre toutes autres mesures requises afin de corriger la situation. Cependant, si la situation nécessite une intervention d'urgence, le Responsable peut prendre une de ces mesures avant d'aviser l'utilisateur.	• appliquer les différentes fonctions de diagnostic sur les équipements; • prendre toutes autres mesures requises afin de corriger la situation. Cependant, si la situation nécessite une intervention d'urgence, le Responsable doit demander une autorisation à un juge afin de pouvoir prendre une de ces mesures avant d'aviser l'utilisateur.
8.4 Sanctions	***8.4 Sanctions***
L'utilisateur qui contrevient aux dispositions du Règlement peut faire l'objet, en plus des sanctions prévues par les lois pertinentes, les règlements, les conventions collectives et les protocoles d'entente, ou de ce qui en tient lieu, de l'une ou de plusieurs des sanctions suivantes : • se voir imposer des règles d'utilisation spécifiques et être tenu de respecter une convention particulière d'utilisation selon des modalités définies par le Responsable; • perdre en partie ou en totalité son droit d'accès; • rembourser à l'Université toute somme que celle-ci serait appelée à débourser à la suite d'incidents ou d'actes préjudiciables qu'il a commis. •	L'utilisateur qui contrevient volontairement aux dispositions du Règlement peut faire l'objet d sanctions prévues par les lois pertinentes, règlements, les conventions collectives et protocoles d'entente, ou de ce qui en tient lieu, al que de l'une ou de plusieurs des sanctions suivantes • se voir imposer des règles d'utilisation spécifiques et être tenu de respecter une convention particulière d'utilisation selon des modalités définies par le Responsable et approuvées par le Comité; • perdre en partie ou en totalité son droit d'accès; • rembourser à l'Université toute somme que celle-ci serait appelée à débourser à la suite d'incidents ou d'actes préjudiciables qu'il a commis.
8.5 Décision finale et sans appel	***8.5 Décision finale***
Les décisions prises par le Responsable en application du Règlement sont finales et sans appel.	Les décisions prises par le Comité en application du Règlement sont finales. Tout membre de la communauté universitaire demeure libre d'en appeler en vertu de sa convention collective ou entente collective, et de ses droits qui lui sont conférés en vertu des lois et chartes.
9. Responsabilité de l'Université	**9. Responsabilité de l'Université**
L'Université n'offre aucune garantie de confidentialité des communications effectuées par l'intermédiaire de ses ressources informatiques et de télécommunication. L'utilisateur doit présumer que toute communication, personnelle ou non, qu'il crée, envoie, reçoit ou mémorise par l'intermédiaire des ressources informatiques et de télécommunication de l'Université peut être lue ou entendue par quelqu'un d'autre que le destinataire. L'Université ne peut être tenue responsable des pertes,	L'Université garantit la confidentialité des communications effectuées par l'intermédiaire de ses ressources informatiques et de télécommunication conformément aux principes identifiés à l'article 1. L'utilisateur doit présumer que toute communication, autre que celles visées par le paragraphe précédent, qu'il crée, envoie, reçoit ou mémorise par l'intermédiaire des ressources informatiques et de télécommunication de l'Université peut être lue ou entendue par quelqu'un d'autre que le destinataire. L'Université ne peut être tenue responsable des pertes,

Guy Bellemare 13-6-19 13:32
Commentaire [10]: On peut contrevenir de manière involontaire ou accidentelle et dans un tel cas, il ne devrait pas y avoir de sanctions.

dommages, manques à gagner ou inconvénients qui pourraient être occasionnés à un utilisateur à l'occasion ou en conséquence de l'utilisation des ressources informatiques et de télécommunication ou advenant le cas où elle devrait, pour quelque cause que ce soit, diminuer ses services ou les interrompre, quelle que soit la durée de telles diminutions ou interruptions.	dommages, manques à gagner ou inconvénients qui pourraient être occasionnés à un utilisateur à l'occasion ou en conséquence de l'utilisation des ressources informatiques et de télécommunication; à moins de négligence de la part de l'Université à assurer les plus hauts standards d'entretien et de protection des équipements et données; ou advenant le cas où elle devrait, après en avoir informé à l'avance les utilisateurs, pour quelque cause que ce soit, diminuer ses services ou les interrompre, quelle que soit la durée de telles diminutions ou interruptions, hormis les causes liées à une négligence de sa part à assurer les plus hauts standards d'entretien et de protection des équipements et données. L'Université s'engage à assurer la mise à jour constante de ses pratiques afin d'approcher les plus hauts standards de sécurité informatique et protection des données, que ce soit par ses procédures ou par design technique (*privacy by design*), tant pour les volets de sécurité que de gestion du cycle de vie des données ou en matière de transferts de données. (OCDE 2011, p. 31 et ss.) L'Université s'engage à gérer au mieux les risques et à assurer la reddition de compte par la production de rapports, d'audits, de formation et d'évaluation de la performance de son service des STI (OCDE 2011, p. 33) au Comité aviseur des STI.
Lorsqu'un utilisateur fait l'objet d'une dénonciation ou d'une sanction en vertu du Règlement, l'Université ne peut être tenue responsable des pertes d'information qui en découlent.	Lorsqu'un utilisateur fait l'objet d'une dénonciation ou d'une sanction en vertu du Règlement, l'Université ne peut être tenue responsable des pertes d'information qui en découlent à moins de négligence de sa part à protéger celles-ci au cours de sa procédure de vérification.
10. Entrée en vigueur Le Règlement entre en vigueur au moment de son adoption par le Conseil d'administration ou à une date ultérieure fixée par celui-ci et pourra être révisé au besoin. Le responsable fera rapport annuellement au conseil d'administration des sanctions imposées dans le cadre de l'application de ce règlement, le cas échéant.	**10. Entrée en vigueur** Le Règlement entre en vigueur au moment de son adoption par le Conseil d'administration ou à une date ultérieure fixée par celui-ci et pourra être révisé au besoin. Le responsable fera rapport régulièrement au Comité STI, et annuellement au conseil d'administration, des interventions, décisions, actions et des sanctions imposées dans le cadre de l'application de ce règlement, le cas échéant.