

POLITIQUE SUR LES INSTALLATIONS INFORMATIQUES

Date d'entrée en vigueur: 8 mars 1999

Origine: Vice-rectorat aux services

Remplace/amende: VRS-30/1^{er} octobre 1997

Numéro de référence: VPS-30

N.B.: Le genre masculin est utilisé comme générique à seule fin d'alléger le texte.

PORTÉE

La présente politique s'applique à tous les membres de l'Université ainsi qu'à toute personne autorisée à utiliser les installations informatiques de l'Université Concordia.

DÉFINITION

Dans le cadre de la politique, on entend par :

Installations informatiques de Concordia (IIC) : tout ordinateur, réseau, périphérique, système d'exploitation, logiciel ou toute combinaison de ces éléments appartenant à l'Université, sous sa garde ou sous sa responsabilité. Le matériel et les logiciels achetés au moyen des fonds de recherche administrés par l'Université appartiennent à l'Université sauf indications contraires clairement stipulées dans la subvention ou le contrat de recherche en question.

PRÉAMBULE

Les IIC sont mises à la disposition des étudiants, des membres du corps professoral, du personnel, des diplômés et autres utilisateurs pour faciliter l'apprentissage, l'enseignement et la recherche ainsi que l'administration qui soutient ces buts. Il incombe à tout utilisateur de s'abstenir de gaspiller les ressources, de nuire au travail d'autrui et d'enfreindre les politiques ou lois applicables.

POLITIQUE

Généralités

1. Le Service de technologie de l'information et de l'enseignement (IITS) joue le rôle de fournisseur central de services de technologies de l'information et des communications alors que l'infrastructure générale consiste en un environnement informatique réparti et partagé. Les responsables de réseaux, collectivement appelés « administrateurs des

POLITIQUE SUR LES INSTALLATIONS INFORMATIQUES

Page 2 de 7

systèmes informatiques de Concordia (ASIC) », assurent la gestion distribuée. IITS convoquera régulièrement des réunions d'information et de coordination avec les ASIC.

2. Afin de protéger les installations contre les accidents, les pannes ou les actes de malveillance, l'Université se réserve le droit de limiter, de restreindre ou de supprimer l'accès de tout utilisateur à ces installations ou de tout hôte ou appareil au réseau et d'inspecter, de copier, de retirer ou de modifier les données, les fichiers ou les ressources du système. Les ASIC agissent au nom de l'Université dans une telle éventualité.
3. L'Université n'offre aucune garantie expresse ou implicite en ce qui concerne les ressources et les installations informatiques offertes ou leur convenance à un but particulier. La fonction des ASIC est de servir un vaste bassin d'utilisateurs dans la communauté universitaire, mais on ne peut s'attendre à ce qu'ils répondent à chacun des besoins spécialisés.

Bon usage

4. L'accès aux IIC a pour but la poursuite de la mission pédagogique et l'exécution des fonctions administratives de l'Université, et non la poursuite des gains commerciaux ou de publicité gratuite sauf dans le cas des départements/services universitaires ou des sous-traitants qui respectent les paramètres définis dans le cadre de leur mission. De même, la publicité indirecte (comme sur internet) n'est autorisée que dans les limites de ces paramètres. Ainsi, il est interdit de vendre de l'espace publicitaire sur la toile (pages web) de l'Université, sauf si une politique interne l'autorise.
5. L'accès aux IIC ne peut être utilisé pour les envois de masse non sollicités, notamment les lettres et publicités en chaîne, sauf par les départements/services de l'Université et les sous-traitants qui agissent dans le cadre de leurs missions définies par l'Université. Les courriels de masse non sollicités doivent être utilisés avec modération et seulement par les canaux de distribution approuvés par IITS.
6. Le nom de l'utilisateur et le mot de passe sont réservés à l'usage exclusif de la personne à qui ils sont destinés. Le partage des noms utilisateurs et mots de passe parmi les personnes autorisées (par ex., utilisation d'un compte collectif) est fortement déconseillé et interdit dans toutes autres circonstances. Toute responsabilité incombe uniquement à la personne officiellement porteuse du nom utilisateur.

POLITIQUE SUR LES INSTALLATIONS INFORMATIQUES

Page 3 de 7

7. L'Université doit s'assurer qu'elle peut repérer toute utilisation du réseau à partir de son organisation interne afin de retrouver l'auteur. Par conséquent, la provenance de tout courriel ou message d'un groupe de nouvelles (ou tout autre communication électronique) doit être exacte et clairement indiquée. Par exemple, la rubrique de l'expéditeur doit contenir une adresse valide correspondant au compte informatique de l'expéditeur.
8. Il est interdit d'utiliser une partie des IIC sans l'autorisation de l'administrateur du système concerné.
9. Les utilisateurs ne doivent pas essayer d'accéder sans autorisation aux ressources informatiques de l'Université, que ce soit à l'intérieur ou à l'extérieur de l'Université.
10. Les réseaux et systèmes externes ont normalement leur propre réglementation et lignes de conduite que les utilisateurs sont tenus de respecter lorsqu'ils y accèdent.
11. Les utilisateurs ne doivent pas se servir des IIC pour obtenir ou échanger des logiciels, des informations ou autre matériel informatique protégés par des droits d'auteur quand une telle action porte atteinte aux droits d'auteur.
12. Les utilisateurs ne doivent pas se servir des IIC dans un but non autorisé ou illicite tel que, entre autres : la destruction ou l'altération de données appartenant à autrui, l'entrave à un accès légitime, la rupture des communications au sein des IIC, la tentative de découvrir ou de modifier les mots de passe ou de déjouer les systèmes de sécurité des IIC ou de toutes autres installations informatiques.
13. Les utilisateurs ne doivent pas profiter des IIC pour envoyer des messages obscènes, vulgaires ou de harcèlement par courrier électronique ou par tout autre moyen. L'Université a prévu des politiques pour sanctionner ces actes de malveillance et elles seront appliquées, s'il y a lieu.

Accès aux ordinateurs

14. IITS accorde à certains groupes de l'Université le privilège d'un accès libre et limité à des éléments particuliers des IIC par les systèmes publics qu'il met à leur disposition. Voici la liste de la plupart des groupes admissibles :

POLITIQUE SUR LES INSTALLATIONS INFORMATIQUES

Page 4 de 7

- a. étudiants des trois cycles, à temps plein et à temps partiel ;
 - b. membres du corps professoral à temps plein et à temps partiel ; professeurs associés et chercheurs boursiers post-doctoraux ;
 - c. personnel administratif et de soutien à temps plein ; personnel administratif et de soutien à temps partiel détenant des postes à contrat ;
 - d. personnel visé par une convention collective.
15. À part les groupes énumérés en 14, des arrangements spéciaux sont possibles, à la discrétion du directeur du Service des technologies de l'information et de l'enseignement.
16. Les personnes suivantes n'ont pas automatiquement accès aux IIC :
- a. Les étudiants de l'Éducation permanente;
 - b. les employés occasionnels;
 - c. les collaborateurs des chercheurs de Concordia.
17. En raison des limitations de ressources, les différents groupes reçoivent des services différents mais en général, l'accessibilité au réseau est équivalente. Les utilisateurs ont le droit de se servir du matériel d'accès public, d'exploiter des programmes sur des ordinateurs désignés, d'utiliser les services de réseau et d'emmagasiner des fichiers.
18. Sur les systèmes publics, les étudiants conservent leur nom utilisateur tant qu'ils sont inscrits et que le compte lui-même est actif. Après une certaine période d'inactivité, définie dans les consignes d'exploitation du Service TIE (*IITS Operational Procedures*), les comptes étudiants sont supprimés.
19. Le nom utilisateur attribué aux étudiants des cycles supérieurs demeure actif tant qu'ils sont inscrits ou que leur professeur superviseur autorise leurs activités.

POLITIQUE SUR LES INSTALLATIONS INFORMATIQUES

Page 5 de 7

20. Les membres du corps professoral et le personnel administratif et de soutien peuvent conserver leur nom utilisateur tant qu'ils sont au service de l'Université. Tous les ans, ils seront avisés du nom utilisateur dont ils sont responsables. S'ils n'ont plus besoin d'avoir accès aux IIC, ils doivent en informer le Service TIE ou leur administrateur de réseau.
21. Si un administrateur de réseau soupçonne qu'un utilisateur abuse du privilège d'accès aux ordinateurs décrit dans la présente politique, dans d'autres politiques de l'Université ou dans toute loi internationale, fédérale ou provinciale, cet utilisateur peut se voir temporairement retirer ce privilège, dans l'attente d'une enquête plus poussée.
22. Il existe des procédures de traitement des actes de malveillance informatique. Elles sont énoncées dans le *IITS Operational Procedures*. La sanction en cas d'abus de privilèges peut inclure la perte de ces privilèges.
23. Les cas de malveillance informatique peuvent aussi constituer un motif de recours en vertu du Code des droits et des obligations, du Code de conduite (pédagogique), des conventions collectives, d'autres politiques de l'Université, ou des lois fédérales ou provinciales.

Confidentialité de l'information

24. Tout utilisateur est en droit de s'attendre raisonnablement au respect de la confidentialité de la part des autres utilisateurs.
25. L'information détenue sur les IIC par un utilisateur lui appartient en propre, sauf si celui-ci prend des mesures spécifiques pour mettre l'information à la disposition des autres utilisateurs.
26. La confidentialité des informations sur ordinateur dépend en grande partie du degré de protection dont les usagers eux-mêmes entourent leur nom utilisateur et mot de passe. Il leur appartient de veiller à la sécurité informatique et aux risques d'intrusion frauduleuse (comme les dommages causés par les programmes du Cheval de Troie ou par des virus). Conformément au paragraphe 6 de la présente politique, il incombe à l'utilisateur de ne pas révéler son mot de passe.

POLITIQUE SUR LES INSTALLATIONS INFORMATIQUES

Page 6 de 7

27. Il est interdit de parcourir les écrans des autres, de récupérer les fichiers que d'autres utilisateurs ont jetés à la poubelle, de voler de l'information sur support papier, ou d'accomplir tout autre acte de ce genre.
28. Toute violation, réelle ou soupçonnée, de la confidentialité doit être signalée à la section ou à l'ASIC concerné, à défaut de quoi cette omission pourra être interprétée comme un consentement tacite.
29. La confidentialité doit être respectée même après l'expiration du nom utilisateur.
30. Les utilisateurs doivent être informés que divers systèmes informatiques rendent certaines informations accessibles à d'autres. Le contenu des fichiers individuels n'est jamais du domaine public par défaut, mais certains éléments comme la dernière commande exécutée, l'heure d'entrée dans le système et le nom utilisateur sont souvent disponibles à d'autres utilisateurs.
31. Le contenu du message électronique est protégé par le principe de confidentialité de l'information, mais les utilisateurs doivent être conscients qu'en cours de livraison, il passe souvent par des systèmes informatiques qui ne sont pas forcément liés par la présente politique. C'est pourquoi il ne faut pas transmettre de documents délicats par courriel sans prendre des précautions particulières.
32. Afin de préserver l'intégrité des IIC contre les incidents, les pannes ou les fraudes, l'Université se réserve le droit d'inspecter, de copier, de retirer ou de modifier des données, des fichiers ou des ressources des systèmes relevant des IIC. En particulier, les représentants désignés du Service TIE, ou les ASIC désignés par leurs départements/services, ont l'autorité de retirer tout matériel des installations qu'ils dirigent s'ils jugent que ce matériel enfreint les politiques de l'Université ou les lois en vigueur ou est inapproprié par rapport à la vocation de l'installation. Ils pourraient par exemple mettre en oeuvre des méthodes automatiques de détection et de retrait de ce matériel, comme configurer les logiciels de messagerie électronique pour rejeter les polluriels (*spam*).
33. Toutefois, l'Université n'entreprend pas de vérifier systématiquement son parc informatique pour déceler ce genre de matériel, sachant qu'il a pu être placé par des gens de l'extérieur. Ainsi, elle décline toute responsabilité pour le matériel reçu par

POLITIQUE SUR LES INSTALLATIONS INFORMATIQUES

Page 7 de 7

l'intermédiaire de listes d'envoi électronique, groupes de nouvelles ou autres forum. Des transmissions valides risquent parfois d'être retirées par erreur à cause des mesures correctives automatiques. Dans ce cas, l'Université n'en sera pas tenue responsable.

34. L'Université se réserve le droit d'inspecter, de copier, de retirer ou de modifier des données, des fichiers ou des ressources des systèmes faisant partie des IIC afin d'aider toute enquête extérieure menée à la suite d'un délit informatique mettant en cause les IIC. S'il y a lieu, l'Université pourra divulguer de l'information avec les autorités compétentes.
35. Les utilisateurs doivent en outre reconnaître que les ASIC dûment autorisés ont l'obligation de prendre des mesures raisonnables appropriées pour assurer l'intégrité des IIC et le respect de la présente politique.

Diffusion sur l'Internet

36. Les pages web sont considérées soit comme « officielles », c'est-à-dire comme représentant un département, un service ou un programme d'enseignement de l'Université, soit comme « non officielles », c'est-à-dire comme source d'information informelle ou officieuse.
37. Toute page officielle doit se conformer aux lignes de conduite édictées dans le manuel d'utilisation intitulé *University Identification Standards Manual* (administré par le Service communications/marketing) ainsi qu'à la politique *Utilisation du nom Université Concordia et de tout signe distinctif y afférent* ([SG-4](#)).
38. Toute page officielle doit indiquer la date de la dernière mise à jour ainsi que l'adresse électronique de l'éditeur de la page.
39. Les éditeurs des pages officielles doivent veiller à leur révision et mise à jour régulières.
40. Au besoin, l'éditeur d'une page publiée à partir des IIC doit obtenir la permission voulue avant d'afficher des textes, des graphiques, des sons ou des films qui ne sont pas de sa création.
41. L'Université se réserve le droit de retirer toute page des IIC.