

CHARTRE DE BON USAGE des utilisateurs des ressources informatiques liées au domaine "uha.fr" ou au réseau de campus de l'UHA.¹

La Charte est destinée à rappeler aux utilisateurs réguliers de toute machine ou de tout réseau local lié au domaine "univ-mulhouse" ou ses sous-domaines, ou réseau de campus de l'UHA, qu'ils doivent observer certaines règles. Cette charte ne préjuge pas des contraintes particulières éditées par le Centre de Ressources Informatiques de l'UHA (CRI) ou les installations spécifiques.

L'ensemble de ces moyens est désigné sous le terme de Ressources Informatiques de l'UHA (RI-UHA).

Tout utilisateur signe un document attestant qu'il a bien pris connaissance de cette charte. Aucun accès ne sera accordé sans cette signature, et tout contournement sera soumis aux instances Disciplinaires de l'UHA.

1. Domaine d'application.

Ces règles s'appliquent à tout utilisateur des moyens informatiques locaux, distants, directement ou en cascade, lié aux RI-UHA.

2. Conditions d'accès

Le droit d'accès à un système informatique est personnel et incessible. Il disparaît lorsque son titulaire quitte le cycle d'enseignement, le laboratoire, ou l'administration concernés. Cet accès est limité à des activités autorisées par les Responsables des enseignements, des UFR's, des Laboratoires, ou de l'administration (REULA).

3. Conditions de confidentialité

L'accès aux informations conservées sur le système informatique doit être limité aux fichiers personnels et publics. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, même si elles n'avaient pas été explicitement protégées. Cette règle s'applique également aux conversations privées, tel E-mail, dont l'utilisateur n'est pas destinataire. Si un utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant en avoir reçu l'autorisation.

4. Respect de la législation concernant les logiciels

Il est illicite d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit.

5. Utilisation de comptes

Lorsque l'utilisation d'un système informatique implique l'ouverture d'un compte nominatif, l'utilisateur ne doit pas se servir, pour y accéder, d'un autre compte que celui qui lui a été attribué par le REULA.

6. Préservation de l'intégrité des informations

L'utilisateur s'engage à ne pas modifier ou détruire d'autres fichiers que ceux qui lui appartiennent en propre, directement ou indirectement. En particulier, il est interdit de modifier le ou les fichiers contenant des informations comptables, d'identification, ou de configuration.

7. Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas perturber volontairement le système informatique, soit par des manipulations anormales du matériel, soit par l'introduction de logiciels parasites. Toute perturbation causée accidentellement doit être signalée immédiatement au responsable de tutelle ou du CRI.

Un travail risquant de violer cette règle ne pourra être accompli que sous le contrôle du responsable concerné, et dans le strict respect de règles qui auront alors été définies.

8. Responsabilité du responsable de tutelle

Le signataire de cette charte est tenu responsable pour toute détérioration d'information due à une utilisation qui ne serait pas conforme à l'engagement qu'il a signé. Le "REULA" ne fournit aucune garantie, implicite ou explicite, ni quant aux performances des Ressources Informatiques, ni quant à l'intégrité des données utilisateur (sauf cas spécifiés ponctuellement).

9. Utilisation de moyens périphériques

L'utilisation des moyens de production de documents (affichage, imprimantes, ...) est strictement limitée à l'usage prévu par les conditions d'accès autorisées (Administration, enseignement, recherche).

10. Accès aux locaux et conditions particulières

L'utilisateur devra se plier aux moyens et horaires de mise à disposition et/ou aux restrictions d'accès définis pour accéder aux systèmes informatiques. Des conditions particulières propres à l'établissement peuvent être fournies en complément, et leurs obligations s'imposent au signataire dans la mesure où elles ne sont pas contraires à celles du présent document.

11. Respect mutuel et bonne entente

L'utilisateur ne doit à aucun moment oublier qu'il vit et travaille au sein d'une communauté et s'interdit de gêner tout autre utilisateur du système informatique à l'aide d'outils électroniques.

Tout utilisateur enfreignant cette règle est passible de sanctions disciplinaires et/ou de poursuites pénales.

¹ Sont concernés également les établissements détachés (ENSCM, ...) et les UPR du CNRS (ICSI, ...)

12. Dispositions particulières

Les administrateurs des RI-UHA sont susceptibles d'être amenés à outrepasser les règles de cette charte pour des raisons techniques précises *motivées et journalisées*.

Le Conseil de Discipline de l'UHA se réserve le droit de décider si une action d'un utilisateur ou d'un REULA est contraire à l'esprit de cette charte.

Le signataire renonce, sauf contrat explicite contraire, à tout droit et revendication concernant les travaux et résultats effectués à l'UHA, enseignement ou recherche.

13. A savoir

Des mises à jours et directives peuvent se rajouter: il est impératif de consulter régulièrement [v. ci dessous]

Renseignements: consulter régulièrement les pages sécurité sur l'intranet (<http://www.uha.fr/INTRANET/>)

Remarques et anomalies: aux responsables concernés ou au Responsable Sécurité de l'UHA : RSSI@uha.fr

Guide de bon usage "étudiant"

-1 Tout travail sur une machine locale liée au domaine "uha.fr" ou ses sous-domaines, ou réseau de campus de l'UHA, doit être lié au suivi d'un responsable d'enseignement, d'un directeur de laboratoire ou d'un responsable administratif. Aucun autre travail n'est autorisé.

-2 Seul le niveau utilisateur est autorisé. Toute action risquant de nuire à l'intégrité du système et du réseau est interdite.

-3 Les informations (nom,...) concernant chaque utilisateur doivent être fournies aux gestionnaires des machines.

Chaque utilisateur possédant un compte personnel est responsable de son compte. Il doit s'assurer de la complexité et de la confidentialité de son mot de passe ; celui-ci ne doit jamais être communiqué à personne.

-4 Le partage d'un compte par plusieurs n'est pas autorisé.

En cas de problèmes ou dégradations éventuelles, le propriétaire du compte sera tenu pour responsable.

-5 La tentative d'intrusion d'un autre compte, ou du système, de la part d'un utilisateur peut entraîner la suppression de tous les droits d'usage des RI-UHA ou à des poursuites pénales.

-6 L'installation de logiciels ou utilitaires pouvant porter atteinte au fonctionnement des machines n'est pas autorisée.

Les gestionnaires des RI-UHA se réservent le droit d'intervenir, en pareil cas.

-7 l'UHA est le maître d'oeuvre du réseau informatique.

Toute machine connectée au réseau doit respecter les directives d'administration et de sécurité établies.