

Charte de bon usage de l'informatique et du réseau Osiris

Les équipements informatiques de l'Université de Strasbourg et des autres institutions partenaires à la gestion du réseau *Osiris* sont dédiés à l'enseignement, la recherche et l'administration. La plupart de ces équipements sont reliés au réseau *Osiris*, et par cet intermédiaire, au réseau Internet. Tout utilisateur de ces équipements appartient donc à une vaste communauté, ce qui implique de sa part le respect de certaines règles de sécurité et de bonne conduite, l'imprudence, la négligence ou la malveillance d'un utilisateur pouvant avoir des conséquences graves pour la communauté. La présente charte définit les droits et les devoirs de chacun et représente un engagement mutuel entre l'utilisateur et la communauté universitaire.

Les différents acteurs

Du point de vue informatique, il faut distinguer trois catégories d'acteurs dans la communauté universitaire :

1. les utilisateurs : étudiants, enseignants, chercheurs, personnels, utilisant les systèmes informatiques mis à leur disposition ;
2. les administrateurs systèmes, responsables techniquement du bon fonctionnement des outils informatiques (systèmes, réseaux et applications) ;
3. les responsables fonctionnels : le chef d'établissement, les directeurs de composantes, les responsables administratifs, les directeurs de laboratoire ou de service, les enseignants encadrant des étudiants dans le cadre d'activités faisant appel à des ressources informatiques.

Chacun a des droits et des devoirs identiques, auxquels s'ajoutent des droits et devoirs spécifiques pour les administrateurs systèmes et pour les responsables fonctionnels.

En outre, chaque établissement connecté à *Osiris* désigne un RSSI (Responsable de la Sécurité des Systèmes d'Information), dont la mission est de coordonner les actions en matière de sécurité informatique, et qui doit être l'interlocuteur privilégié de tous les acteurs.

Les droits de tous

Chacun a droit à :

1. l'information relative aux ressources et aux services communs offerts par l'établissement, la composante ou le laboratoire ;
2. l'information lui permettant d'utiliser au mieux les moyens mis à sa disposition ;
3. l'information sur la sécurité du système qu'il utilise.

Les devoirs de chacun

1. chacun doit respecter la propriété intellectuelle et commerciale conformément à la législation en vigueur ;
2. chacun a le devoir de respecter les règles de sécurité applicables au système qu'il utilise ; ces règles consistent en la présente charte complétée par des annexes régulièrement actualisées, ainsi qu'éventuellement, les règles spécifiques liées à un environnement de travail particulier (laboratoire, salle de ressources pour étudiants) ; ces règles sont tenues à la disposition de chaque utilisateur par le responsable fonctionnel ou l'administrateur système ;
3. chacun s'engage à ne pas prendre connaissance d'informations appartenant à autrui sans son accord, à ne pas communiquer à un tiers de telles informations, ou des informations non publiques auxquelles il peut accéder, mais dont il n'est pas propriétaire ;
4. chacun doit s'identifier clairement, nul n'a le droit d'usurper l'identité d'autrui ou d'agir de façon anonyme ; nul ne peut céder ses droits d'accès à autrui ;
5. chacun doit s'efforcer de parvenir à son but par le moyen le plus économe en ressources communes (espace disque, impressions, occupation des postes de travail, transferts réseau, occupation de serveurs distants...) ;
6. chacun doit contribuer à l'amélioration du fonctionnement et de la sécurité des outils informatiques, en respectant les règles et conseils de sécurité, en signalant immédiatement aux responsables toute anomalie constatée, en sensibilisant ses collègues aux problèmes dont il a connaissance ;
7. chacun doit veiller à utiliser les moyens mis à sa disposition dans un cadre professionnel, ce qui exclut l'utilisation dans un but commercial. Un usage raisonnable dans le cadre des nécessités de la vie courante et familiale est toléré, à condition que l'utilisation n'affecte pas les performances du système et du réseau ;
8. nul ne peut modifier un équipement, tant du point de vue matériel que logiciel système, sans l'accord du responsable système.

Droits et devoirs spécifiques des administrateurs systèmes

Les administrateurs doivent veiller à assurer le fonctionnement normal et la sécurité des outils informatiques. Ils sont conduits par leur fonction même à avoir accès à l'ensemble des informations relatives aux utilisateurs, y compris celles

qui sont enregistrées sur le poste de travail.

Dans le cadre de ses missions, tout administrateur système a le droit :

1. d'être informé des implications légales de son travail, y compris des risques qu'il encourt dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible ;
2. d'utiliser des fichiers de journalisation et d'accéder aux informations privées à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations.

Dans le cadre de ses missions, tout administrateur système a le devoir :

1. de porter à la connaissance des utilisateurs les informations et les traitements auxquels il a accès de par sa fonction ;
2. de veiller à la déclaration des traitements automatisés d'informations nominatives, conformément à la réglementation en vigueur ;
3. d'informer les utilisateurs et de les sensibiliser aux problèmes de sécurité informatique inhérents au système, de leur faire connaître les règles de sécurité à respecter, aidé par le correspondant sécurité du réseau ;
4. de respecter les règles de confidentialité, en limitant l'accès à l'information confidentielle au minimum nécessaire et en respectant une stricte discrétion professionnelle sur ce point ;
5. d'agir dans le sens d'une meilleure sécurité, dans l'intérêt de l'établissement et des utilisateurs ;
6. en cas d'incident sécurité, d'informer immédiatement son responsable fonctionnel et de coopérer pour la résolution de l'incident avec le RSSI de l'établissement ainsi que, le cas échéant, avec les responsables de la sécurité des organismes concernés.

Droits et devoirs spécifiques des responsables fonctionnels

Les responsables fonctionnels de systèmes informatiques ont le droit :

1. de suspendre l'accès aux ressources informatiques et au réseau en cas de problème affectant le bon fonctionnement du système ;
2. de prendre toute mesure conservatoire, et d'en informer le RSSI de l'établissement, en cas de non respect de la charte de la part d'un utilisateur.

Les responsables fonctionnels de systèmes informatiques ont le devoir :

1. d'informer tous les acteurs, de diffuser la présente charte par tout moyen approprié ;
2. de communiquer, au correspondant sécurité du réseau, le nom des responsables système de toutes les machines placées sous leur autorité et à la Direction Informatique le nom d'un responsable réseau ;
3. de soutenir de leur autorité les administrateurs système dans leur travail de mise en application de cette charte.
4. de saisir l'autorité hiérarchique et le RSSI des manquements graves résultant du non respect de cette charte, le chef d'établissement pouvant déclencher des procédures disciplinaires ou pénales.

Sanctions encourues en cas de non respect

Le non respect des règles définies dans cette charte peut entraîner des sanctions de nature :

1. disciplinaire :
 - les responsables fonctionnels ont pleine autorité pour prendre les mesures conservatoires nécessaires en cas de manquement à la présente charte et interdire aux utilisateurs fautifs l'accès aux moyens informatiques et au réseau,
 - ces utilisateurs fautifs peuvent être déférés devant la commission de discipline compétente ;

2. pénale :

L'utilisation de moyens informatiques et de communication électronique est soumis au droit commun, comme le code de la propriété intellectuelle, ou le code pénal, et à quelques textes spécifiques, comme la loi dite « Informatique et Libertés », ou la loi relative à la fraude informatique (loi dite « Godfrain »).

La présente charte, ainsi que ses annexes s'applique à l'ensemble des utilisateurs des ressources informatiques de l'établissement.