Computing and Network Services

Charter of good usage of data processing and networks within the International Space University

Table of Content

Charter of good usage of data processing and networks within the International Space University 2
Charte de bon usage de l'informatique et des réseaux à l'International Space University . 5

Document name: OSIRIS Charter.doc
Revision: 1.0

Last updated by: Joel Herrmann – IT Manager
On: September 1st, 2006

INTERNATIONAL SPACE UNIVERSITY
1, rue Jean-Dominique Cassini • Parc d'Innovation • 67400 Illkirch-Graffenstaden • FRANCE
Telephone +33 (0) 3 88 65 54 63 • Fax +33 (0) 3 88 65 54 47
n° SIRET 395 006 315 00026 • APE 803 Z
E-mail:cns@isunet.edu • www.isunet.edu

Charter of good usage of data processing and networks within the International Space University

The data processing equipment of the International Space University and other institutional partners with the management of the *Osiris* network is dedicated to teaching, research and administration. The major part of this equipment is connected to the *Osiris* network, and through it, to the Internet network. Thus, any user of this equipment belongs at a vast community, which implies that he complies with certain safety requirements and good behavior rules, as imprudence, negligence or the ill will of a user may have serious consequences on the community. The present charter defines the rights and the duties of each user and represents a mutual obligation between the user and ISU.

Various actors.

From the data processing perspective, it is necessary to distinguish two categories:

- users: students, teachers, researchers, personnel using the information processing systems at their disposal,
- the system and/or network administrators, in charge technically for the correct operation of the data processing tools,

Each one has rights and duties identical in spirit but different in practice.

Rights of all.

Each one is entitled to have:

- information relating to the resources and the common services offered by the University,
- information allowing him to use the means at its disposal as well as possible
- information on the safety of the system which he uses.

Obligations of each one.

- Each one has the obligation to comply with the safety requirements applicable to the system which he uses; these rules exist in the present charter illustrated by appendices regularly updated, and, possibly, specific rules related to a particular work environment (laboratory, room of resources for students); these rules are available to each user from the CNS manager or the system administrator.
- Each one must respect the intellectual and commercial property in accordance with the legislation in force.

- Each one is committed to not take note of information belonging to another person without his agreement, to not communicate to a third party such information or nonpublic information to which he has access but for which he has no ownership.

- Each one must identify himself clearly; no one is allowed to usurp the identity of others or to act in an anonymous way. No one can yield his rights to others.

- Each one must endeavor to arrive to his goal by the "cheapest" way of using common resources (disk space, prints, occupation of working stations, network transfers, …).

- Each one must contribute to the improvement of the operation and the safety of the data processing tools by complying with the rules and security advice, by immediately pointing out to the persons in charge any noted anomaly, by sensitizing his/her colleagues to the problems of which he is informed.

- Each one will use the equipment at his disposal for professional purposes and respect the function which is assigned to it, which excludes the use for personal matters, the use with a commercial aim, the abusive use of teaching equipment for research and vice versa. No one can modify any equipment or the hardware or software system without the agreement of the person in charge of the system.

Rights and specific obligations of the system and/or the network administrators

On many systems, the administrator technically has all rights, therefore he has important obligations, in particular not to misuse his rights. According to the penal code, the system administrator is personally responsible for the safety of the machine and/or the network of which he is in charge.

Any system administrator has the right:

- to be informed of the legal implications of its work, in particular of the risks which he runs if a user of the system of which he is in charge commits a reprehensible action,

- to access private information for diagnosis purposes and administration of the system, by scrupulously respecting the confidentiality of this information,

- to establish procedures for monitoring of all the tasks carried out on the machine in order to detect the violations or the attempts of violation of this charter, after authorization of the CNS manager and in relation with the safety correspondent for the network…

Each system administrator has the obligation:

- to inform the users of the extent of the rights he technically has by virtue ofhis function,

- to inform the users and to sensitize them to the problems of computer security inherent to the system, to make them aware of the safety requirements to be respected, helped by the safety correspondent of the network,

- to comply with the general rules of access to the network defined for the *Osiris* network,
- to comply with the rules of confidentiality, by limiting the access to confidential information to bare essentials and by respecting a "professional secrecy" on this point,
- to respect, if he is himself a user of the system, the rules he has to impose on the other users,
- to modify the system in the direction of better safety in the interest of the users,
- to immediately inform the CNS manager and the safety correspondent of the University of any attempt (successful or not) of intrusion on its system, or any dangerous behavior of a user,
- to cooperate with the safety correspondents of the OSIRIS network in the event of an attack affecting a machine he administers.

Sanctions incurred in the event of nonrespect

The noncompliance with the rules defined in this charter may lead to the following kinds of sanctions:

- disciplinary:
    - the CNS manager will have full authority to take the conservative measures required in the case of breach of the present charter and to prohibit the access to the data processing system and the network to the faulty users,
    - these faulty users may be referred to a disciplinary commission,
- penal:

The developments in the electronic and data processing technologies led the legislatureto define penal sanctions of a great severity in line with the risks that uncontrolled use of files or data processes may represent to individual freedom,. **This charter is integral part of ISU Internal rules. It is made available of all users and applies to all.**

Adopted by the ISU Board of Trustees of the International Space University on 25 august 2006

Charte de bon usage de l'informatique et des réseaux à l'International Space University

Les équipements informatiques de l'International Space University 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 l'ISU.

Les différents acteurs.

Du point de vue informatique, il faut distinguer deux catégories d'acteurs:

- les utilisateurs : étudiants, enseignants, chercheurs, personnels utilisant les systèmes informatiques mis à leur disposition,
- les administrateurs systèmes et/ou réseau, responsables techniquement du bon fonctionnement des outils informatiques,

Chacun a des droits et des devoirs identiques dans l'esprit mais différents dans la pratique.

Les droits de tous.

Chacun a droit à :

- l'information relative aux ressources et aux services communs offerts par l'Université,
- l'information lui permettant d'utiliser au mieux les moyens mis à sa disposition,
- l'information sur la sécurité du système qu'il utilise.

Les devoirs de chacun.

- Chacun a le devoir de respecter les règles de sécurité applicables au système qu'il utilise ; ces règles consistent en la présente charte illustrée 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 informatique ou l'administrateur système.

- Chacun doit respecter la propriété intellectuelle et commerciale conformément à la législation en vigueur.
- 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.
- 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 à autrui.
- Chacun doit s'efforcer de parvenir à son but par le moyen le moins « coûteux » en ressources communes (espace disque, impressions, occupation des postes de travail, transferts réseau, ...).
- 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.
- Chacun doit se limiter à un usage professionnel des équipements mis à sa disposition et respecter la fonction qui leur est assignée, ce qui exclut l'utilisation à des fins personnelles, l'utilisation dans un but commercial, l'utilisation abusive d'un équipement de l'enseignement pour la recherche et vice-versa. 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 système et/ou du réseau

Sur de nombreux systèmes, l'administrateur a techniquement tous les pouvoirs, il a de ce fait des devoirs importants, en particulier celui de ne pas abuser de ses pouvoirs. D'après le code pénal, l'administrateur système est personnellement responsable de la sécurité de la machine et/ou du réseau dont il a la charge.

Tout administrateur système a le droit :

- d'être informé des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible,
- d'accéder aux informations privées à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations,
- d'établir des procédures de surveillance de toutes les tâches exécutées sur la machine, afin de déceler les violations ou les tentatives de violation de la présente charte, après autorisation du responsable informatique et en relation avec le correspondant sécurité du réseau...

Tout administrateur système a le devoir :

- d'informer les utilisateurs sur l'étendue des pouvoirs dont lui-même dispose techniquement de par sa fonction,
- 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,
- de respecter les règles générales d'accès au réseau définies pour le réseau *Osiris*,
- de respecter les règles de confidentialité, en limitant l'accès à l'information confidentielle au strict nécessaire et en respectant un "secret professionnel" sur ce point,
- de respecter, s'il est lui-même utilisateur du système, les règles qu'il est amené à imposer aux autres utilisateurs,
- de modifier le système dans le sens d'une meilleure sécurité, dans l'intérêt des utilisateurs,
- d'informer immédiatement le responsable informatique et le correspondant sécurité de l'Université de toute tentative (fructueuse ou non) d'intrusion sur son système, ou de tout comportement dangereux d'un utilisateur,
- de coopérer avec les correspondants sécurité du réseau en cas d'attaque impliquant une machine qu'il administre.

Sanctions encourues en cas de non respect

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

- disciplinaire :
    - le responsable informatique 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,
- pénale :

  L'évolution des techniques électroniques et informatiques a conduit le législateur à définir des sanctions pénales d'une grande sévérité à la mesure du risque que peut faire courir aux libertés individuelles, l'usage incontrôlé des fichiers ou des traitements informatiques.

Cette charte, partie intégrante du règlement interne de l'ISU est portée à la connaissance de tous les utilisateurs et s'impose à tous.

Adoptée par le Conseil d'Administration de L'International Space University le
25 août 2006