LABORATOIRE
DE L'ACCÉLÉRATEUR
LINÉAIRE

CHARTE DE BON USAGE DES RESSOURCES INFORMATIQUES
DU
LABORATOIRE DE L'ACCÉLÉRATEUR LINÉAIRE D'ORSAY

Préambule.

Les systèmes et équipements informatiques du Laboratoire de l'accélérateur linéaire, UMR 6423, mis à la disposition des personnels sont dédiés à la recherche, à l'enseignement, et l'administration. La plupart de ces équipements sont reliés en réseau local , 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 peuvent 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'ensemble du personnel du laboratoire. Elle est supposée connue de tous, et elle fait partie intégrante du règlement intérieur du Laboratoire de l'accélérateur linéaire.

Les différents acteurs.

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

- les utilisateurs : l'ensemble des personnes utilisant les systèmes informatiques mis à leur disposition,
- les administrateurs système et/ou réseau et correspondants sécurité informatique, responsables techniquement du bon fonctionnement des outils informatiques,
- les responsables fonctionnels : la direction du laboratoire , les responsables de groupe ou d'unité , les enseignants encadrant des étudiants dans le cadre d'activités faisant appel à des ressources 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 le laboratoire et l'IN2P3.
- 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 ; ces règles sont tenues à la disposition de chaque utilisateur par le responsable fonctionnel 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. Chacun doit signaler toute tentative de violation de son compte.
- Nul ne peut céder ses droits à autrui. Les autorisations d'accès aux ressources informatiques sont strictement personnelles, et ne peuvent être cédées, temporairement ou définitivement, à quiconque (collègues, amis et membres de la famille inclus) quelle que soit la confiance vis à vis de ces personnes.
- 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, occupation de serveurs distants, etc.).
- 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. Il est interdit d'installer un logiciel pouvant mettre en péril la sécurité des moyens informatiques.
- Chacun doit se limiter à un usage strictement professionnel des équipements mis à sa disposition et respecter les fonctions qui leurs sont assignées, ce qui exclut l'utilisation à des fins personnelles, l'utilisation dans un but commercial.
- Nul ne peut modifier un équipement, tant du point de vue matériel que logiciel système, ni connecter une machine au réseau local sans l'accord explicite de l'administrateur système et/ou réseau.
- Il ne pourra être invoqué préjudice ou demandé réparation suite à une altération, destruction ou perte de confidentialité de traitement d'informations extra-professionnelles par les administrateurs systèmes dans l'exercice de leur activité si de tels traitements étaient cependant mis en oeuvre sur un moyen informatique du laboratoire par un utilisateur qui le ferait alors à ses "risques et périls".

- Nul ne peut connecter un équipement qui n'est pas propriété du laboratoire sur le réseau local sans l'accord des administrateurs systèmes, qui ont autorité pour en requérir alors les moyens de l'administrer sans restriction. La présente charte s'applique alors à cet équipement, et son propriétaire en devient utilisateur au titre de la charte.

Droits et devoirs spécifiques des administrateurs système et/ou du réseau.

Sur de nombreux systèmes, l'administrateur a techniquement des pouvoirs étendus , il a de ce fait des devoirs importants, en particulier celui de ne pas abuser de ses pouvoirs. L'administrateur système est responsable de la sécurité de la machine et/ou du réseau dont il a la charge. Le correspondant sécurité informatique appartient implicitement à cette catégorie.

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, sur les systèmes qu'il administre, aux informations privatives à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations, en s'efforçant tant que la situation ne l'exige pas de ne pas les altérer.
- 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, sous l'autorité de son responsable fonctionnel et en relation avec le correspondant sécurité informatique,
- de prendre des mesures conservatoires si l'urgence l'impose, sans préjuger des sanctions résultants des infractions à la présente charte qui sont de la responsabilité des responsables fonctionnels.

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,
- de respecter les règles générales d'accès au réseau définies pour le réseau local, et au-delà de l'IN2P3, Renater et l'Internet en général.
- 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 configurer et administrer le système dans le sens d'une meilleure sécurité, dans l'intérêt des utilisateurs,
- d'informer le responsable sécurité informatique de l'IN2P3 de la mise en oeuvre de procédures exceptionnelles de surveillance ou d'investigations,
- d'informer immédiatement son responsable fonctionnel et le responsable sécurité informatique de l'IN2P3 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 des réseaux extérieurs en cas d'incident de sécurité impliquant une machine qu'il administre.

Droits et devoirs spécifiques des responsables fonctionnels.

Les responsables fonctionnels de systèmes informatiques ont le droit :

- d'interdire temporairement ou définitivement l'accès aux ressources informatiques à un utilisateur qui ne respecte pas la présente charte,
- de saisir l'autorité hiérarchique des manquements graves résultant du non respect de cette charte pouvant déclencher des procédures disciplinaires ou pénales.

Les responsables fonctionnels de systèmes informatiques ont le devoir :

- d'informer tous les acteurs, de diffuser la présente charte par tous moyens appropriés,
- de nommer un correspondant de la sécurité informatique,
- de communiquer, au correspondant sécurité informatique du laboratoire, le nom des administrateurs système de toutes les machines placées sous leur autorité ,
- de soutenir de leur autorité les administrateurs système et le correspondant sécurité informatique dans leur travail de mise en application de cette charte.

Sanctions encourues en cas de non respect.

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

- 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,
- civile et/ou pénale :

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

Cette charte, partie intégrante du règlement intérieur du Laboratoire de l'accélérateur linéaire est portée à la connaissance de l'ensemble du personnel et s'impose à tous.

Adoptée par le Conseil du Laboratoire de l'accélérateur linéaire, le 28 novembre 1998 ,

Le directeur du Laboratoire de l'accélérateur linéaire