Sciences Po Bordeaux

Charte des usages numériques

Sciences Po Bordeaux en tant que membre de Réaumur (cellule réseau universitaire) est tenu de respecter la charte suivante :

RÈGLEMENT INTÉRIEUR DU RÉSEAU RÉAUMUR

Version 2 – CA du 10/11/2004

Le réseau RÉAUMUR ne doit être utilisé qu'à des fins professionnelles d'enseignement et de recherche.

Ce réseau ne constitue en aucun cas un accès banalisé à l'Internet tel que peut en offrir un prestataire de services.

Le règlement intérieur précise les droits, devoirs, responsabilités de chacun pour l'utilisation du réseau RÉAUMUR.

Il complète et précise la charte du réseau RENATER, laquelle s'applique entièrement à RÉAUMUR.

Il n'est pas exclusif de règles d'utilisation des ressources informatiques énoncées par les organismes ou laboratoires.

Il définit les règles d'utilisation et d'administration de l'ensemble des systèmes connectés à RÉAUMUR.

Il précise également les règles d'utilisation des équipements informatiques distants accessibles à partir de RÉAUMUR, à travers le réseau régional ESRA, le réseau national RENATER, le réseau INTERNET mondial, ou tout autre moyen.

Tout signataire du document intitulé : " *Engagement des utilisateurs du réseau RÉAUMUR* " est tenu de se conformer au présent règlement intérieur, conformément à l'article I du document précité.

1.1. Les moyens informatiques concernés

Le règlement concerne l'ensemble des équipements informatiques connectés directement ou indirectement à RÉAUMUR.

Ils comprennent notamment les serveurs, stations de travail, micro-ordinateurs, ordinateurs portables ou tout autre équipement mobile communiquant (PDA, téléphone, ...), terminaux des salles en libre-service (travaux pratiques enseignements, bibliothèques, ...), des laboratoires, écoles, instituts, services administratifs...

1.2. Les utilisateurs

Toute personne utilisant un équipement connecté à RÉAUMUR est considérée comme utilisateur de RÉAUMUR.

L'accès aux moyens informatiques est donné par le service auquel on est rattaché, à titre temporaire. Il sera retiré dans le cas d'un comportement en désaccord avec les principes minima énoncés dans ce règlement et dans l'engagement des utilisateurs.

1.3. Le responsable sécurité, les administrateurs

Chaque machine connectée est gérée et contrôlée par un responsable sécurité connu de la cellule RÉAUMUR.

Le responsable sécurité peut déléguer la gestion des machines à des administrateurs.

Le responsable sécurité veille au bon respect des règles d'exploitation.

Il procède aux enquêtes et investigations nécessaires et répond aux besoins d'éventuelles procédures disciplinaires ou judiciaires.

2.1. Respect de l'identité

Le droit d'accès à un système est personnel et incessible. Notamment : les mots de passe ne doivent être ni communiqués, ni stockés.

En conséquence, il est interdit :

a) d'utiliser le compte d'un tiers,

b) d'envoyer, ou tenter d'envoyer des messages ou des courriers électroniques anonymes ou sous une identité usurpée.

2.2. Respect des règles de sécurité

L'utilisateur doit se mettre en conformité avec les mesures adoptées par le responsable sécurité de RÉAUMUR, notamment en matière de gestion de mot de passe.

Il doit signaler au responsable sécurité de sa machine toute tentative de violation ou d'effraction sur un compte, sur des données ou sur l'intégrité du système.

2.3. Respect de la confidentialité

Les données contenues dans des fichiers ou transmises sur les réseaux par des utilisateurs ou des administrateurs doivent être considérées comme privées, qu'elles soient ou non accessibles par les autres utilisateurs.

La possibilité d'accéder à un fichier n'implique pas le droit de le consulter.

Le fait d'avoir la possibilité de modifier un fichier n'implique pas que l'on ait le droit de l'altérer.

2.4. Respect de l'intégrité des systèmes

L'utilisateur ne doit en aucun cas modifier :

- le contenu des fichiers système,
- le contenu des fichiers de configuration réseau,
- le contenu des fichiers relatifs à la sécurité des machines ou équipements réseau.

L'utilisateur ne doit en aucun cas utiliser ou tenter d'utiliser les privilèges d'administration du système.

L'utilisation, le stockage de logiciels pouvant porter gravement atteinte à la sécurité des systèmes (virus, chevaux de Troie, vers, logiciel d'espionnage de lignes de communication...) sont interdits.

Un utilisateur qui pense avoir de bonnes raisons de faire des expériences relatives à la sécurité des moyens informatiques **doit discuter de ce projet avec le responsable sécurité de RÉAUMUR.**

2.5. Respect des restrictions légales d'utilisation

Les conditions d'acquisition de certains logiciels restreignent leurs conditions d'utilisation. Les réseaux ne doivent en aucun cas être utilisés pour outre passer ces conditions d'utilisation.

De même, il est nécessaire de respecter les règles qui régissent la propriété intellectuelle et artistique.

L'utilisateur a le droit de demander à un responsable sécurité ou à un administrateur de prendre les mesures appropriées pour mettre fin à tout abus dont il serait victime.

L'utilisateur a le droit et le devoir d'utiliser tous les moyens mis à sa disposition par le système d'exploitation pour garantir la confidentialité de ses données, restrictions de droits d'accès, cryptage, sauvegarde sur support amovible...

Les responsables sécurité et les administrateurs doivent informer tout utilisateur potentiel des règles édictées par le présent document.

La signature par l'utilisateur de l' « Engagement des utilisateurs du réseau RÉAUMUR », les exonère de cette obligation.

Les responsables sécurité appliquent et font appliquer par les administrateurs, les consignes de sécurité préconisées par la cellule réseau RÉAUMUR.

Les responsables sécurité informent le responsable sécurité de RÉAUMUR et leurs autorités hiérarchiques des problèmes de sécurité constatés. Ils collaborent aux enquêtes nécessaires pour établir les responsabilités.

Les comptes collectifs ouverts par les administrateurs, à titre exceptionnel (cf. article III.2 de l' «Engagement des utilisateurs du réseau RÉAUMUR») feront l'objet d'une évaluation par le responsable sécurité de RÉAUMUR.

Les responsables sécurité, et les administrateurs doivent impérativement respecter la confidentialité des fichiers des utilisateurs ainsi que de leur courrier électronique.

Les responsables sécurité, et les administrateurs ont le devoir d'informer les utilisateurs et la cellule réseau RÉAUMUR par les moyens les plus appropriés (circulaires, courrier électronique...) de toute intervention qu'ils seraient amenés à faire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques et plus particulièrement du service réseau. Ceci concerne notamment les interconnexions de réseaux, les équipements réseaux, le service du courrier électronique.

Les responsables sécurité et les administrateurs doivent prendre les mesures nécessaires au bon fonctionnement du réseau et au respect des règles d'utilisation ; dans ce cadre, ils peuvent avoir à examiner des fichiers privés ou des courriers, à fins de diagnostic et d'enquête, dans le respect de la confidentialité des informations privées des utilisateurs.

À titre conservatoire, ils peuvent prendre des mesures de restriction d'utilisation d'un compte ou d'un service.

Le responsable administratif du laboratoire ou du service définit en accord avec la cellule réseau RÉAUMUR les éventuelles modalités particulières d'accès au réseau. **Elles nécessitent la conclusion d'une convention entre les parties.**

Le responsable administratif du laboratoire ou du service engage les moyens financiers nécessaires à la mise en place et au fonctionnement des services utilisés par ce laboratoire ou ce service.

ANNEXE

PRINCIPAUX TEXTES RÉPRIMANT LES ATTEINTES À LA SÉCURITE DES MOYENS INFORMATIQUES

Version 2 – CA du 10/11/2004

Tout utilisateur autorisé ou non encourt, en plus des sanctions disciplinaires, des sanctions pénales et civiles, prévues par plusieurs textes législatifs, en raison de comportements liés à l'utilisation de l'informatique. En particulier la loi réglemente la fraude informatique (Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique), la protection des logiciels et des progiciels (Loi nº 2004-204 du 9 mars 2004), la protection des fichiers nominatifs (Loi nº2004-801 du 6 août 2004 relative à l'informatique, aux fichiers et aux libertés)

Ces textes législatifs définissent un certain nombre de délits et de peines.

À titre d'exemple :

Code Pénal – Articles L323-1 à L323-3-1

Article L323-1 : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.
Article L323-2 : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Article L323-3 : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.
Article L323-3-1 : Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles L323-1 à L323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Loi nº 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité
Code de la Propriété Intellectuelle - Articles. L335-2 et suivants

La reproduction d'un logiciel autre qu'une copie de sauvegarde, de même que l'utilisation d'un logiciel non expressément autorisé, sont passibles d'une peine d'emprisonnement de 2 ans et d'une amende de 150 000 euros.
De même, les bases de données bénéficient également d'un régime de protection particulier prévu par le Code de la Propriété Intellectuelle (Art. L341-1 et suivants du C.P.I.).

Code Pénal – Article L226-16

Article L226-16 : Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2º du I de l'article L45 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

ENGAGEMENT DES UTILISATEURS DU RESEAU RÉAUMUR

Version 2 – CA du 10/11/2004

INTRODUCTION

Tout utilisateur d'un équipement informatique connecté à RÉAUMUR, est informé que ce réseau est destiné exclusivement à véhiculer le trafic engendré par des activités de recherche, de développement technologique et d'enseignement supérieur. Les activités d'administration et de gestion des centres de recherche ou d'enseignement supérieur sont assimilées à la recherche ou à l'enseignement supérieur.

ARTICLE I

Tout utilisateur d'équipement informatique connecté à RÉAUMUR s'engage à prendre connaissance du Règlement Intérieur de ce Réseau et à s'y conformer. De la même manière, il reconnaît avoir pris connaissance des recommandations jointes à cet engagement.

ARTICLE II

Sont passibles de poursuites disciplinaires, civiles, pénales, tous les actes réalisés dans l'intention de nuire ou susceptibles de nuire à tout utilisateur d'un équipement informatique au moyen de RÉAUMUR.

ARTICLE III

Tout compte identifie un utilisateur, personne physique, responsable de l'utilisation de ce compte.
Toute usurpation de compte est susceptible de poursuites. - A titre exceptionnel, des comptes collectifs peuvent être ouverts sous la responsabilité d'une personne prenant à sa charge les responsabilités liées à la nature de ce compte.
Tout utilisateur d'un applicatif d'accès banalisé (exemple : accès au catalogue des bibliothèques, au service de la scolarité...) s'engage à rester dans les limites de cet applicatif.

ARTICLE IV

Tout utilisateur s'engage à ne pas prêter son compte et à ne pas le rendre accessible par négligence. Il se met en conformité avec les mesures adoptées par le responsable Sécurité de RÉAUMUR, notamment en matière de gestion de mots de passe.

ARTICLE V

Chaque équipement connecté à RÉAUMUR est contrôlé par un responsable Sécurité. Ce dernier dispose à cette fin des moyens d'investigations nécessaires lui permettant d'examiner éventuellement les données des utilisateurs dans le respect de la confidentialité.

ARTICLE VI

Dans les conditions fixées par le Règlement Intérieur concernant le fonctionnement de RÉAUMUR, le responsable Sécurité doit informer les instances concernées de toutes infractions ou violations constatées ou suspectées.

ARTICLE VII

Tout utilisateur s'engage à signaler au responsable Sécurité de sa machine, toute tentative de violation ou d'effraction sur son compte, ses données et l'intégrité du système. La non observation de cet article peut entraîner des restrictions d'utilisations à titre conservatoire, pour les besoins de l'enquête.

ARTICLE VIII

Tout utilisateur d'un équipement informatique connecté à RÉAUMUR s'interdit toute utilisation d'une machine locale ou distante sur laquelle il ne possède pas de numéro de compte (à l'exception des services anonymes. Exemple : ftp anonymous...). Des poursuites pénales pourront être engagées en application de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (articles L323-1 à L323-3-1 du Code Pénal)

ARTICLE IV

Chaque utilisateur est responsable de l'utilisation des logiciels et matériels mis à sa disposition.
Il est rappelé que l'usage et l'installation de logiciels (programme, plug-in, agent, démon…) même libre de droit est soumis à autorisation écrite du service informatique copie devant être remise au secrétariat général.

Sciences Po Bordeaux se réserve le droit de suspendre l'accès aux ressources de toute personne contrevenant aux règles établies, et de prendre toute mesure administrative qu'elle jure adéquate.
L'entité ne peut être tenue responsable en cas en cas d'indisponibilité du système et de perte de données et / ou de temps dans le cadre de l'utilisation des ressources informatiques. De plus l'entité encourage les utilisateurs à mettre en oeuvre tout moyen de sauvegarde personnel. L'effacement ou la perte de données stockées ou utilisées sur le système ne relève pas de la responsabilité de l'entité.

Recommandation d'utilisation du réseau

Quelques exemples de pratiques inacceptables

Version 2 – CA du 10/11/2004

Les recommandations présentées ci-dessous ne constituent pas une liste exhaustive mais seulement un ensemble d'informations concrètes.

LE RÉSEAU EST DESTINÉ EXCLUSIVEMENT À DES FINS PROFESSIONNELLES D'ENSEIGNEMENT ET DE RECHERCHE.

LE RESEAU RÉAUMUR N'EST PAS UN ACCÈS BANALISÉ À INTERNET.

Parmi les pratiques peu recommandables et donc inacceptables, on peut citer les exemples suivants :

1. Donner ses mots de passe ou prêter ses comptes (ex: par l'intermédiaire de rhost).
2. Laisser son poste de travail sans surveillance.
3. Rechercher ou transférer ou tenter de par quelque moyen que ce soit (ex: P2P, ftp, fsp, irc/dcc, échanges MSN Messenger, mail, www...).
   - › toute copie frauduleuse de documents ou logiciels (ex: logiciel piraté, warez),
   - › tout document facilitant le piratage de logiciel (ex: cracks, num. de série),
   - › tout document ou logiciel servant à pirater les machines (ex : scanner, sniffer, cracker, rootkit, ...)
   - › tout document aidant au développement de virus.
4. Violer les règles d'utilisation de certains documents (ex : diffuser par le WEB des textes, sons et images soumis aux droits d'auteurs et de propriété intellectuelle et artistique).
5. Utiliser des logiciels exclusivement employés pour récupérer des documents volumineux et non professionnels, voire illégaux (P2P type Gnutella, Kazaa, Edonkey, SoulSeek, PeerEnabler,...).
6. Chercher à obtenir ou utiliser des accès illégaux sur une machine même sans intention de nuire.
7. Ne pas respecter la législation sur les moyens de chiffrement.
8. Utiliser/installer le logiciel Skype interdit par le MENESR.

Si vous pensez avoir de bonnes raisons d'effectuer une action mentionnée ci-dessus vous devez IMPÉRATIVEMENT en demander l'autorisation à vos responsables puis à la cellule RÉAUMUR. Dans le cas contraire, vous seriez considéré comme ayant délibérément enfreint le règlement avec tous les risques et désagréments que cela comporte.

La Cellule RÉAUMUR et Sciences Po Bordeaux effectue les contrôles permettant de vérifier le respect de ces règles.

→ Pour plus d'informations : http://www.reaumur.u-bordeaux.fr