Inserm

Institut national
de la santé et de la recherche médicale

Charte de l'utilisateur des ressources informatiques et des services Internet de l'INSERM

Ce texte est avant tout un code de bonne conduite. Il a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques et des services Internet, en respect des dispositions légales et réglementaires en vigueur, avec des règles minimales de courtoisie et de respect d'autrui.

Pour tout renseignement complémentaire, les utilisateurs peuvent s'adresser, selon le cas, au responsable de leur Unité, Équipe, Département ou Service, au Responsable Régional Informatique de l'Administration déléguée dont ils dépendent, ou au Responsable de la Sécurité des Systèmes d'Information de l'INSERM.

1 Définitions

On désignera sous le terme « entité » les structures créées par l'INSERM pour l'accomplissement de ses missions, telles que les Unités de Recherche, les Équipes, ainsi que les Départements et Services administratifs.

On désignera de façon générale sous le terme « ressources informatiques », les moyens informatiques de calcul ou de gestion locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par une entité de l'INSERM.

On désignera par « services Internet », la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses : Web, messagerie, forum...

On désignera sous le terme « utilisateur », les personnes ayant accès ou utilisant les ressources informatiques et services Internet d'une entité de l'INSERM.

2 Accès aux ressources informatiques et services Internet

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder ne sont autorisés que dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

L'activité professionnelle est celle prévue par les statuts du GIP RENATER auquel est lié l'INSERM, à savoir : les activités de recherches, d'enseignements, de développements techniques, de transferts de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentations de nouveaux services présentant un caractère d'innovation technique, mais également toute activité administrative et de gestion découlant ou accompagnant ces activités.

L'utilisation des ressources informatiques partagées de l'entité et la connexion d'un équipement sur le réseau sont en outre soumises à autorisation. Ces autorisations, délivrées par le Directeur de l'entité, sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

L'entité pourra en outre prévoir des restrictions d'accès spécifiques à son organisation : (Cryptage d'accès ou d'authentification, filtrage d'accès sécurisé...)

3 Règles d'utilisation, de sécurité et de bon usage

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de son entité.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

En particulier :

- il doit appliquer les recommandations de sécurité de l'entité à laquelle il appartient ;
- il doit assurer la protection de ses informations et il est responsable des droits qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition ;
- il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater ;
- il doit suivre les règles en vigueur au sein de l'entité pour toute installation de logiciel ;
- il choisit des mots de passe sûrs, gardés secrets et en aucun cas ne doit les communiquer à des tiers ;
- il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage ;
- il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité ;
- il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement. En particulier, il ne doit pas modifier le ou les fichiers contenant des informations comptables ou d'identification ;
- il ne doit pas quitter son poste de travail ni ceux en libre-service en laissant des ressources ou services accessibles et il doit se déconnecter, sauf avis contraire de l'administrateur du réseau.

4 Conditions de confidentialité

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie. Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers relevant de la loi Informatique et Libertés, il devra auparavant en avoir fait la demande à la CNIL en concertation avec le Directeur de l'entité, le Département Animation et Partenariats Scientifiques et le Service juridique de l'INSERM et en avoir reçu l'autorisation. Il est rappelé que cette autorisation n'est valable que pour le traitement défini dans la demande et non pour le fichier lui-même.

5 Respect de la législation concernant les logiciels

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par la personne habilitée à cette fin par le responsable de l'entité.

Par ailleurs l'utilisateur ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d'utilisation d'un logiciel.

Il est rappelé que les logiciels commerciaux disponibles pour les utilisateurs de l'INSERM sont l'objet de licences par lesquelles des droits d'usage sont concédés à l'INSERM. Ces licences font l'objet de contrats conclus par l'INSERM. Il est de la responsabilité des personnels de respecter les termes de ces licences et de ces contrats ; y manquer serait une faute professionnelle.

De même, l'installation sur un système informatique mis en oeuvre par l'INSERM d'un logiciel dont le droit d'usage est acquis à titre privé par un membre du personnel n'est pas autorisée.

L'usage de logiciels commerciaux est régi par des contrats et protégé par des lois qui entraînent une responsabilité personnelle de leur utilisateur, que la responsabilité propre de l'INSERM en tant que personne morale ne saurait exonérer.

6 Préservation de l'intégrité des systèmes informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux (internes ou extérieurs à l'INSERM) que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques...

Tout travail de recherche ou autre, risquant de conduire à la violation de la règle définie dans le paragraphe précédent, ne pourra être accompli qu'avec l'autorisation du responsable de l'entité et dans le strict respect des règles qui auront alors été définies.

Il est de la responsabilité de l'utilisateur de s'assurer de l'installation sur l'ordinateur qu'il utilise régulièrement de logiciels de protection contre les logiciels parasites évoqués ci-dessus. Le Département du Système d'Information organise la distribution des logiciels de protection appropriés.

7 Usage des services Internet (Web, messagerie, forum...)

7.1 Règles de bon usage

L'utilisateur doit faire usage des services Internet dans le cadre exclusif de ses activités professionnelles et dans le respect de principes généraux et des règles propres aux divers sites qui les proposent ainsi que dans le respect de la législation en vigueur.

En particulier :

- il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités ;
- il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers ;
- il ne doit pas utiliser ces services pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- il ne doit pas déposer des documents sur un serveur sauf si celui-ci le permet ou sans y être autorisé par les responsables habilités ;
- il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions...
- il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'INSERM ou à ses agents ;
- il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique ou diffamatoire.

7.2 Publication sur l'Internet

La mise à la disposition du public d'un serveur WWW appartenant au domaine `inserm.fr`, ou affichant le logo de l'INSERM ou manifestant de toute autre façon son appartenance à l'INSERM engage la responsabilité de l'INSERM et expose son image. L'ouverture d'un tel site est donc soumise à l'autorisation du Département de l'Information Scientifique et de la Communication. La publication de documents sur un site autorisé se fera ensuite sous la responsabilité des responsables d'entité, sous le contrôle *a posteriori* du Département de l'Information Scientifique et de la Communication, et selon les principes énoncés par la Charte de bonne

utilisation du réseau Internet dans les laboratoires INSERM, disponible sur le serveur http://www.inserm.fr

7.3 Responsabilité légale

La publication d'informations et de documents sur un support public tel que le WWW entraîne une responsabilité personnelle de leur auteur devant la loi, que la responsabilité de l'INSERM en tant que personne morale ne saurait exonérer.

8 Analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

9 Rappel des principales lois françaises :

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique :

- la loi du 6/1/78 dite « informatique et liberté », (cf. http://www.cnil.fr/) ;
- la législation relative à la fraude informatique, (article 323-1 à 323-7 du Code pénal),(cf. http://www.legifrance.gouv.fr/citoyen/code.cgi)
- la législation relative à la propriété intellectuelle(cf. http://www.legifrance.gouv.fr/citoyen/code.cgi) ;
- la loi du 04/08/1994 relative à l'emploi de la langue française,(cf. http://www.culture.fr/culture/dglf/) ;
- la législation applicable en matière de cryptologie.(cf. http://www.telecom.gouv.fr/francais/activ/techno/crypto0698_1.htm).

10 Application

La présente charte s'applique à l'ensemble des agents de l'INSERM tous statuts confondus, et plus généralement à l'ensemble des personnes, permanentes ou temporaires, utilisant les moyens informatiques de l'entité ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau administré par l'entité.

Elle sera annexée, à titre d'information, aux contrats de travail conclus avec les agents contractuels et vacataires qui auront accès au système informatique de leur entité.

Elle sera en outre signée par toutes personnes accueillies à l'INSERM et ayant accès audit système.

NOM PRENOM DEPARTEMENT
DATE
SIGNATURE
(Précédée par la mention “Lu et approuvé, bon pour accord”)