Charte pour l'usage de ressources informatiques et de services Internet

Institut de Recherche en Astrophysique et Planétologie

Ce texte[1], associé au règlement intérieur de l'Institut de Recherche en Astrophysique et Planétologie (IRAP), a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation, afin d'instaurer un usage conforme des ressources informatiques et des services Internet relevant du CNRS et le cas échéant d'autres tutelles du laboratoire (UPS et CNES). Ces ressources et services constituent un élément important du patrimoine scientifique et technique du CNRS.
Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires qui s'imposent et notamment la sécurité, la performance des traitements et la conservation des données professionnelles.

Pour tout renseignement complémentaire, adressez-vous au service informatique : supportinfo@irap.omp.eu

1. Définitions

On désignera de façon générale sous le terme « **ressources informatiques** » : les réseaux, 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 de l'entité, les logiciels, les applications, les bases de données…

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, téléphonie IP (Internet Protocol), visioconférence…

On désignera sous le terme « **utilisateur** » : la personne ayant accès ou utilisant les ressources informatiques et services Internet quel que soit son statut.

On désignera l'Institut de Recherche en Astrophysique et Planétologie (IRAP) sous le terme « **entité** ».

On désignera les tutelles de l'Institut de Recherche en Astrophysique et Planétologie (IRAP) (CNRS, UPS...) sous le terme « **tutelles de l'entité** ».

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 sont destinés à l'activité professionnelle des utilisateurs conformément à la législation en vigueur. L'activité professionnelle doit être entendue comme celle définie par les textes spécifiant les missions des tutelles de l'entité.

L'utilisation des ressources informatiques partagées de l'entité et la connexion d'un équipement privé et extérieur (tels qu'un ordinateur, commutateur, modem, borne d'accès sans fil…) sur le réseau sont soumises à autorisation du responsable de l'entité et aux règles de sécurité de celle-ci. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée.

L'entité peut en outre prévoir des restrictions d'accès spécifiques à son organisation (certificats électroniques, cartes à puce d'accès ou d'authentification, filtrage d'accès sécurisé,…).

3. Règles d'utilisation et de sécurité

Tout utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès.

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 :

3.1 Règles de sécurité

[1] Issu du Bulletin Officiel du CNRS, décision n° 070007DAJ du 18 janvier 2007 portant approbation des modifications de la charte pour l'usage de ressources informatiques et de service Internet.

• il doit appliquer les recommandations de sécurité de l'entité et notamment se conformer aux dispositifs mis en place par l'entité pour lutter contre les virus et les attaques par programmes informatiques,

• il lui appartient de protéger ses données en utilisant différents moyens de sauvegarde individuels ou mis à sa disposition,

• il doit assurer la protection de ses informations et plus particulièrement celles considérées comme sensibles au sens de la politique de sécurité des systèmes d'informations (PSSI du CNRS). En particulier, il ne doit pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports non fiabilisés tels que ordinateurs portables, clés USB, disques externes, etc… Ces supports qualifiés d'« informatique nomade » introduisent une vulnérabilité des ressources informatiques et comme tels doivent être soumis aux règles de sécurité de l'entité et à une utilisation conforme aux dispositions de la présente charte,

• il doit garantir l'accès à tout moment à ses données professionnelles dans le cadre de la politique de recouvrement[2] de données mise en œuvre au sein de l'entité,

• il ne doit pas quitter son poste de travail ni ceux en libre-service en laissant des ressources ou services accessibles.

3.2 Règles d'utilisation

• Toute information est professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Ainsi, il appartient à l'utilisateur de procéder au stockage éventuel de ses données à caractère privé dans des répertoires explicitement prévus à cet effet et intitulés « privé ».
La protection et la sauvegarde régulière des données de ces dossiers incombent à l'utilisateur, la responsabilité de l'entité ne pouvant être engagée quant à la conservation de cet espace,

• il doit suivre les règles en vigueur au sein de l'entité pour toute installation de logiciel et ne pas télécharger ou utiliser de logiciels ou progiciels sur le matériel de l'entité sans autorisation explicite.
Notamment, il ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d'utilisation d'un logiciel. Les logiciels doivent être utilisés dans les conditions des licences souscrites,

• il doit veiller à la protection des différents moyens d'authentification personnels. En particulier, il doit choisir des mots de passe sûrs, gardés secrets et en aucun cas il ne doit les communiquer à des tiers. Si pour des raisons exceptionnelles et ponctuelles, un utilisateur se trouve dans l'obligation de communiquer son mot de passe, il devra veiller dès que possible au changement de ce dernier. Il doit également protéger son certificat électronique par un mot de passe sûr gardé secret. Comme la signature manuscrite, le certificat électronique est strictement personnel et l'utilisateur s'engage à n'autoriser personne à en faire usage à sa place,

• il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater,

• il s'engage à ne pas mettre à la disposition d'utilisateur(s) non autorisé(s) un accès aux ressources informatiques ou aux services internet, 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 masquer son identité,

• il ne doit pas accéder aux informations et documents conservés sur les ressources informatiques autres que ceux qui lui sont propres, et ceux qui sont publics ou partagés. Il ne doit pas tenter de les lire, modifier, copier ou détruire, même si l'accès est techniquement possible.

4. Respect de la loi informatique et libertés[3]

Si, dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers soumis aux dispositions de la loi informatique et libertés, il doit accomplir les formalités requises par la CNIL par l'intermédiaire de la direction des systèmes d'information du CNRS en concertation avec le directeur de son entité et veiller à un traitement des données conforme aux dispositions légales. Il est rappelé que cette procédure n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui-même.

---

2 Le recouvrement est le dispositif de secours permettant à une personne habilitée d'accéder à des données lorsque le mécanisme principal n'est plus utilisable (perte ou destruction de clé, oubli de mot de passe,...) ou en cas d'empêchement de l'agent détenteur.

3 Le guide CNIL du CNRS, édité en 2006, reprend les principes clés pour la création ou l'utilisation des traitements de données à caractère personnel (les droits et obligations de chacun et les formalités à engager).

5. Respect de la propriété intellectuelle

L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

6. Préservation de l'intégrité des ressources informatiques

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux 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.

7. Usage des services Internet (web, messagerie, forum, téléphonie IP…)

7.1 Internet

Internet est un outil de travail ouvert à des usages professionnels dont l'utilisation doit respecter des principes généraux et des règles propres aux divers sites qui les proposent, ainsi que dans le respect de la législation en vigueur.

En particulier, l'utilisateur :

• 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,

• ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède,

• ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers,

• ne doit pas utiliser ces services pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur,

• ne doit pas déposer des données sur un serveur interne ou ouvert au grand public (google, free, orange, …) ou sur le poste de travail d'un autre utilisateur sans y être autorisé par les responsables habilités,

• doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions…,

• n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice aux tutelles de l'entité,

• doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire.

L'entité ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé à ces règles.

7.2 Messagerie électronique

La messagerie électronique est un outil de travail ouvert à des usages professionnels.

• Tout message sera réputé professionnel sauf s'il comporte une mention particulière et explicitée dans son objet indiquant son caractère privé ou s'il est stocké dans un espace privé de données.

• Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

• La transmission de données classifiées[4] est interdite sauf dispositif spécifique agréé et la transmission de données dites sensibles doit être évitée ou effectuée sous forme chiffrée.

• L'utilisateur doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages de masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

L'évolution permanente des technologies de l'informatique met à disposition des utilisateurs de nouveaux services qui peuvent être accessibles depuis le réseau de leur entité. Ces nouvelles technologies, qui peuvent présenter un risque de vulnérabilité particulier, ne peuvent être utilisées qu'après accord préalable du responsable de l'entité et dans le strict respect de la politique de sécurité des systèmes d'informations (PSSI du CNRS)

8. Analyse et contrôle de l'utilisation des ressources

Pour des nécessités de maintenance et de gestion technique, de contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus, l'utilisation des ressources informatiques et des services internet, ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de le législation applicable et notamment de la loi sur l'informatique et des libertés.

L'utilisateur dont le poste fait l'objet d'une maintenance à distance doit être préalablement informé.

Les personnels en charge des opérations de contrôle sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, en particulier lorsqu'elles sont couvertes par les secrets des correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service.

9. Traçabilité

Le CNRS est dans l'obligation légale de mettre en place un système de journalisation des accès Internet, de la messagerie et des donnés échangées. Par conséquent des outils de traçabilité sont mis en place sur tous les systèmes d'information. Le CNRS a procédé auprès de la CNIL à une déclaration qui mentionne notamment la durée de conservation des traces et durée de connexion, en application de la loi en vigueur.

10. Rappel des principales dispositions légales

Il est rappelé que l'ensemble des agents de l'entité, quel que soit leur statut, sont soumis à la législation française en vigueur et notamment :

• la loi du 29 juillet 1881 modifiée sur la liberté de la presse,
• la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés,
• la législation relative aux atteintes aux systèmes de traitement automatisé de données (art. L 323-1 et suivants du code pénal),
• la loi n° 94-665 du 4 août 1994 modifiée relative à l'emploi de la langue française,
• la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,
• les dispositions du code de propriété intellectuelle relative à la propriété littéraire et artistique.

11. Application

La présente charte s'applique à l'ensemble des agents de l'entité quel que soit leur statut, et plus généralement à l'ensemble des personnes, permanents ou temporaires qui utilisent, à quelque titre que ce soit, les ressources informatiques et services internet de l'entité, ainsi que ceux auxquels il est possible d'accéder à distance directement ou en cascade à partir du réseau de l'entité.

Date :

Nom :

« Reconnaît avoir pris connaissance des 4 pages composant la charte informatique de l'IRAP. »

Signature :

4 Il s'agit des données classifiées de défense qui couvrent le « confidentiel défense », le « secret défense » et le « très secret défense ».