Annexe 6.b : Charte informatique de l'unité

CHARTE INFORMATIQUE

DE L'UNITE

Responsable informatique de l'unité : Henrique AFONSO – poste 2164

Dernière mise à jour : 25 Avril 2023

OBJET

La présente Charte a pour objet de définir les conditions d'utilisation et les règles de bon usage des ressources informatiques et des services internet disponibles au sein de l'Unité Mixte de Recherche « Institut des Sciences des Plantes de Montpellier » (IPSiM), dont les organismes de tutelle sont le CNRS, INRAE, l'Institut Agro Montpellier et l'Université Montpellier, et qui est située sur le campus commun Institut Agro/INRAE de Montpellier.

Elle précise la responsabilité des utilisateurs, dans le respect de la législation en vigueur, afin de promouvoir un usage correct des ressources informatiques, avec des règles minimales de courtoisie et de respect d'autrui.

La présente charte reprend l'essentiel des règles établies par les quatre textes suivants :

- « Charte utilisateur pour l'usage des ressources informatiques inra » du 13 juin 2008
- « Charte pour l'usage de ressources informatiques et de services Internet » du CNRS,
- « Charte régissant l'usage du système d'information de l'Université de Montpellier – du 07/05/2015
- « Charte déontologique RENATER » version 2014

La présente Charte est applicable à l'ensemble des agents et des personnes autorisées à utiliser les ressources informatiques de l'UMR IPSiM.

Le manquement aux règles édictées dans cette Charte peut donner lieu à l'application de sanctions disciplinaires ou pénales en fonction de la nature et de la gravité des faits reprochés et de leurs conséquences.

1. Définitions

On désignera de façon générale sous le terme « ressources informatiques » : les réseaux, les moyens informatiques de calcul ou de gestion locaux (serveurs, postes de travail, équipements d'acquisition, de stockage, de restitution et d'impression), ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau de l'unité, 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, 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 sous le terme « unité » l'UMR IPSiM.

2. Principes généraux d'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. Les activités professionnelles sont les activités de recherche, d'enseignement, de développement technique, de transfert de technologies, de diffusion d'informations scientifiques, techniques et culturelles, d'expérimentation de nouveaux services présentant un caractère d'innovation technique, ainsi que toute activité administrative, de gestion ou d'appui à la recherche découlant ou accompagnant ces activités.

Toutefois, une utilisation ponctuelle des ressources informatiques du laboratoire pour un motif personnel est autorisée, à la condition qu'elle reste dans des limites raisonnables.

L'utilisation des ressources informatiques de l'IPSiM, notamment l'ouverture d'un compte ou la connexion d'un équipement sur le réseau, est soumise à autorisation du Directeur de l'unité et du Responsable informatique. Ces autorisations 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 de plein droit lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée. Les utilisateurs disposeront cependant d'un délai de deux mois avant la fermeture effective des autorisations d'accès, afin de terminer les opérations en cours et d'effectuer les sauvegardes nécessaires.

L'unité peut en outre prévoir des restrictions d'accès spécifiques à son organisation (certificats électroniques, …).

3. Garanties accordées aux agents

Compte tenu des risques d'atteinte aux libertés individuelles du fait des multiples procédures de collecte d'informations et donc de traitements automatisés des données personnelles qui peuvent en découler, sont privilégiés :

- la discussion collective au niveau du Conseil d'Unité ;
- l'information préalable des agents ;
- le droit d'opposition dans le cadre du traitement de données nominatives ;
- le principe de proportionnalité : en ce sens, ne peuvent pas être apportées aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas proportionnées au but recherché ;
- le principe de protection de l'intimité de la vie privée de l'agent public sur son lieu de travail et donc du secret des correspondances et fichiers à caractère personnel ou syndical.

4. Règles d'utilisation, de sécurité et de bon usage des ressources informatiques, à respecter par les utilisateurs

En collaboration avec les services compétents de ses organismes de tutelle, l'unité, en fonction de l'état de l'art et des coûts liés à la mise en œuvre, s'engage à prendre les mesures adaptées à un niveau de sécurité approprié au regard des risques évalués et de la valeur des ressources et des informations à protéger. Chaque utilisateur est responsable de l'usage des ressources informatiques mises à sa disposition et s'engage à ne pas effectuer des opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement de ces ressources, sur l'intégrité des systèmes d'information, et sur les relations internes et externes de l'unité.

Chaque utilisateur a la charge, à son niveau, de contribuer à la sécurité générale des systèmes d'information. L'utilisation des ressources informatiques doit être rationnelle, et conforme à l'intérêt du service, contribuant ainsi à éviter sa saturation ou son détournement.

Toute anomalie constatée, susceptible d'affecter la sécurité des ressources informatiques, doit être signalée au Responsable informatique de l'unité ou au Service Informatique Mutualisé du centre INRAE de Montpellier (Équipe S.I.M.). Tout manquement à ces stipulations engage la responsabilité personnelle de l'utilisateur, qui en assume les entières conséquences.

4.1. Obligations à respecter par tout utilisateur

- 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 collectifs, mis à sa disposition.
- Il doit choisir des mots de passe sûrs, gardés secrets, et en aucun cas ne doit les communiquer à des tiers.
- Lorsqu'il quitte un poste de travail, il doit verrouiller ou fermer les sessions ouvertes, afin de ne pas laisser des ressources ou des services disponibles sans identification.
- Il doit se conformer aux obligations de discrétion professionnelle, de réserve, et de bonne moralité afférentes au statut d'employé dans un organisme public.
- Il doit respecter l'ensemble des lois d'ordre pénal ou civil en vigueur, notamment celles relatives :
    - aux publications à caractère raciste, pédophile, injurieux, diffamatoire,

    - au harcèlement sexuel ou moral,
    - à l'utilisation des logiciels,
    - au droit d'auteur.
- Il doit suivre les règles en vigueur au sein de l'unité pour toute installation de logiciel.

4.2. Interdictions et consignes à respecter par tout utilisateur

- Les équipements informatiques personnels ne sont autorisés à se connecter que sur le reseau wi-fi Eduroam ou Wifi-Campus.
- Les accès extérieurs au campus en VPN ne sont autorisés que pour des machines professionnelles dotées par le laboratoire.
- **Il est formellement interdit d'installer le client VPN de l'établissement sur un poste personnel.**
- Tout utilisateur ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues pour ce serveur ou sans y être autorisé par les responsables habilités.
- Il ne doit pas tenter de lire, modifier, déposer ou détruire des données sur un serveur autrement que par les dispositions prévues pour 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 connecter un matériel sur le réseau sans autorisation.
- Il ne doit pas mettre à la disposition de personnes non autorisées un accès aux ressources informatiques disponibles dans l'unité.
- Il ne doit pas, par quelque moyen que ce soit, proposer ou rendre accessible aux tiers des informations confidentielles ou contraires à la législation en vigueur.
- Il ne doit pas télécharger ou diffuser des données en violation des lois protégeant les droits d'auteur, quel que soit le domaine (écrits, images, logiciels, bases de données, …).
- Il ne doit pas contourner les restrictions d'utilisation d'un logiciel.

4.3. Utilisation et protection des ressources informatiques à des fins personnelles

L'utilisation des ressources informatiques de l'unité pour motif personnel ne doit pas être susceptible d'amoindrir les conditions d'accès professionnel à ces ressources. Elle est autorisée dans la mesure où elle ne porte pas atteinte au bon fonctionnement du service, et ne met pas en cause sa productivité. L'ensemble des règles de cette Charte s'applique également pour ce type d'utilisation.
Le devoir de réserve incombant à tout employé dans un organisme public doit être respecté.
Les informations à caractère personnel gérées par les utilisateurs doivent être placées dans un dossier personnel aisément identifiable comme tel, notamment grâce à son intitulé devant inclure la mention « personnel ». Aucun autre utilisateur que le propriétaire n'est autorisé à accéder au contenu de ces dossiers.
La messagerie électronique peut également être utilisée pour un usage personnel, dans les limites imposées par le bon fonctionnement du service. Conformément aux principes de droit, il est considéré qu'un message envoyé ou reçu depuis un poste de travail mis à la disposition de l'utilisateur par l'unité revêt un caractère professionnel, sauf indication manifeste dans le sujet du message.

5. Modalités d'application

La présente charte s'applique à l'ensemble des personnes, personnels ou non de l'unité, tous statuts confondus, autorisées à utiliser les ressources informatiques de l'unité. Lorsqu'un compte est ouvert pour un utilisateur, celui-ci doit déclarer avoir pris connaissance de la présente charte et des documents associés, et s'engager à les respecter. Cette déclaration sera effectuée par la procédure en vigueur au moment de l'ouverture du compte.

Pour obtenir des informations complémentaires ou pour signaler des problèmes de sécurité, les utilisateurs peuvent s'adresser au Responsable informatique de l'unité et/ou à l'Équipe informatique du Centre INRAE de Montpellier (Équipe S.I.M.).

6. 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 la législation applicable et notamment de la loi sur l'informatique et les 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, dès lors que ces informations ne remettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du service.

7. Procédures de contrôle et de sanctions

Le Directeur d'unité est chargé de faire respecter la Charte. Il est notamment responsable de l'appréciation des limites imposées pour l'utilisation des ressources pour un motif personnel, dans l'intérêt du bon fonctionnement du service.
Le Responsable informatique de l'unité veille à assurer le fonctionnement normal et la sécurité des réseaux et des systèmes d'information.

7.1. Rapport d'incident

En cas de constatation, par quelque personne que ce soit d'une situation susceptible de compromettre l'intégrité de ressources informatiques, cette personne doit immédiatement prévenir le Responsable informatique de l'unité ou de l'Assistance Informatique Institut Agro Montpellier – INRAE (Equipe S.I.M.), qui doit signaler l'incident à l'administrateur des ressources informatiques concernées et au Responsable Sécurité des Systèmes d'Information (RSSI) des établissements concernés.

7.2. Mesures conservatoires

Face à un rapport d'incident, l'administrateur des ressources concernées prend toute mesure conservatoire nécessaire pour éviter cette compromission ou son aggravation, conformément aux règles de l'art. Les mesures conservatoires incluent, entre autres, la déconnexion d'un équipement du réseau, et la restriction des autorisations d'accès. Lorsque la gravité de la situation l'amène à prendre des mesures conservatoires, l'administrateur doit rendre compte immédiatement à ses supérieurs hiérarchiques et fonctionnels.

7.3. Droits de l'utilisateur en cas de constatation de manquement aux règles de la Charte

L'utilisateur mis en cause peut fournir des justifications et formuler des observations à partir du dossier d'enquête qui lui est transmis.

7.4. Sanctions et recours

Dans le cadre des lois et règlements en vigueur, toute sanction sera assise sur le principe de proportionnalité. En fonction de la gravité des faits, la sanction ira d'une simple mise en garde par l'autorité hiérarchique jusqu'aux sanctions disciplinaires prononcées après consultation préalable d'un conseil de discipline. Toute mesure susceptible de faire grief ne pourra être prononcée sans une communication préalable par l'administration du dossier administratif de l'intéressé.