Annexe 1
Au règlement intérieur

CHARTE INFORMATIQUE DE L'ETABLISSEMENT

Préambule

La présente Charte vaut règlement intérieur en ce qui concerne l'usage du système informatique de l'établissement Oniris.

L'utilisation de tout moyen informatique au sein d'Oniris suppose de la part des utilisateurs, le respect d'un certain nombre de règles dont le rôle est d'assurer la sécurité et la performance des matériels et outils informatiques, la préservation des données confidentielles ainsi que l'émission et la réception d'informations dans le respect des législations applicables.

Cette charte s'applique au sein d'Oniris en quelque lieu qu'ils soient, à l'ensemble des utilisateurs du système informatique. Elle s'impose aussi aux administrateurs dudit système.

Le terme « système informatique » désigne l'ensemble des moyens mis en œuvre au sein de l'établissement pour faciliter les échanges, le travail coopératif, la recherche d'information, le stockage d'information et de documents.
Le système informatique regroupe l'ensemble des « ressources informatiques » intégrées au sein de l'établissement, à savoir les composants matériels et réseaux qui peut le constituer notamment serveurs, réseau local ou distant (services Internet), réseau d'interconnexion interne, périphériques divers. Il intègre également les logiciels mis à disposition par l'établissement Oniris ainsi que l'ensemble des données et des fichiers utilisés ou produits par l'usage de ces logiciels.

Le terme « utilisateur » désigne toute personne susceptible de créer, de mettre en œuvre ou d'user d'une ou plusieurs ressources informatiques au sein de l'établissement.

Le terme « administrateur » désigne toute personne ayant la responsabilité d'une ou plusieurs ressources informatiques.

Cette Charte doit permettre de trouver un équilibre entre le respect des libertés individuelles et la sécurité informatique au sein de l'établissement Oniris. Elle a pour but de :
-souligner que les moyens informatiques sont des outils essentiellement professionnels
-poser les règles de sécurité inhérentes à toute utilisation du système informatique

-sensibiliser les utilisateurs sur la conséquence d'une mauvaise utilisation du système informatique
-rappeler les règles d'utilisation du système informatique de l'établissement et ses moyens de contrôle potentiels

Le non respect de l'ensemble des dispositions de ladite Charte est susceptible d'engager la responsabilité du contrevenant. Toute violation des règles présentes expose ladite personne à des sanctions disciplinaires, sans préjudice des poursuites pénales et/ou civiles pouvant être mises en oeuvre, conformément aux lois et règlements en vigueur.

Chapitre 1 : Utilisation du système informatique de l'établissement Oniris

Article 1 : Conditions d'accès

L'accès au système informatique d'Oniris a pour objet principal de mener des activités administratives ou liées à la recherche et l'enseignement. L'utilisation des ressources informatiques est subordonnée à l'obtention d'une autorisation délivrée par le Directeur Général.

L'autorisation, ouvrant droit à l'obtention d'un compte personnalisé avec mot de passe, n'est accordée qu'après acceptation de la présente Charte. L'autorisation délivrée à l'utilisateur est strictement personnelle. Nul n'est autorisé à utiliser le compte d'autrui ou à prêter le sien. Chaque titulaire d'un compte est responsable de l'ensemble des actes effectués avec celui-ci.

En principe, il est mis fin à l'autorisation lorsque l'activité qui justifiait son attribution a été menée. Dans le cas d'une boite de messagerie non nominative, le mot de passe de celle-ci doit être modifié par le nouveau responsable ou l'administrateur.

Article 2 : Respect général des lois et règlements en vigueur

Tout moyen informatique doit être utilisé conformément à la législation relative à l'utilisation des systèmes informatiques. Parmi les dispositions applicables à tout utilisateur de ressources informatiques figurent :
-la loi du 6/1/1978 dite Informatique et libertés
-la loi du 3/7/1985 qui, en particulier, interdit à tout utilisateur de reproduire tout ou partie d'un logiciel commercial pour un usage autre que sa sauvegarde (licences)
-la loi du 5/1/1988 sur la fraude informatique

Il incombe à chacun des utilisateurs, notamment les étudiants et stagiaires d'ONIRIS ainsi que les personnels enseignants et non-enseignants quelque soit leur statut, de respecter l'ordre public et les bonnes mœurs.

Article 3 : Respect spécifique des lois et règlements en vigueur

L'utilisateur doit strictement respecter la législation prohibant le harcèlement moral et sexuel ainsi que toute publication à caractère raciste, pédophile, injurieux et diffamatoire. En

particulier, l'utilisateur s'engage à ne pas émettre d'opinions personnelles susceptibles de porter préjudice à l'image et la réputation de l'établissement. Toute communication à diffusion publique précisera si l'utilisateur s'exprime à titre personnel ou en tant que membre de l'établissement.

Il est également interdit de diffuser tout ou partie d'une œuvre protégée par le code de la propriété intellectuelle. En particulier, les documents, photos, vidéos et tout autre support accessibles du fait du droit d'accès aux ressources informatiques sont exclusivement destinés aux bénéficiaires d'autorisation de l'établissement. L'utilisateur s'engage donc à ne transmettre aucun de ces fichiers informatiques à des tiers sans avoir reçu l'autorisation préalable de leurs auteurs. Cette autorisation sera impérativement expresse si la diffusion projetée implique le droit à l'image de la personne ou les personnes concernées.

Les produits de l'intelligence artificielle mis à la disposition du public sont soumis à l'obligation de dépôt légal.

Article 4 : Protection de l'intégrité du système informatique

Chaque utilisateur est soumis aux règles de bon fonctionnement du système informatique édictées par l'établissement ; il lui incombe de prendre connaissance de toutes les informations diffusées qui y sont relatives. Il est responsable de l'utilisation qu'il fait des ressources informatiques à partir du matériel qu'il utilise soigneusement et des droits d'accès au système informatique de l'établissement dont il dispose exclusivement.

L'utilisateur s'engage à ne pas effectuer d'opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du système informatique de l'établissement. Il reste attentif à ne pas créer de failles de sécurité, notamment constitutives suites à l'instauration de passerelles avec les systèmes extérieurs, l'introduction de « logiciels parasites » ou encore l'utilisation détournée des moyens mis à sa disposition.

Pour des raisons de sécurité, seuls les équipements achetés sur le budget de l'école ou des unités et validés par le service informatique seront connectés au réseau. Les ordinateurs personnels ne pouvant être utilisés que sur le réseau Wifi mis à disposition dans certains locaux.

Article 5 : Préservation de l'intégrité du système informatique

L'utilisateur doit contribuer à la sécurité du système informatique en signalant au service informatique compétent toute anomalie susceptible d'entraver son bon fonctionnement. Il s'engage à ne pas masquer son identité et à ne pas usurper celle des autres. L'utilisation de moyens de cryptage doit faire l'objet d'une autorisation préalable du Directeur Général de l'établissement.

L'utilisateur ne peut ajouter de périphériques ou de logiciels supplémentaires (à l'exception de logiciels libres ou sous licences) destinés à l'activité professionnelle. Le service informatique est le seul autorisé à installer des composantes système sur le matériel concerné.

Article 6 : Préservation des données confidentielles

Chaque utilisateur n'a le droit d'accéder qu'à ses propres documents ou à ceux qui sont publics. En particulier, il est formellement 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 correspondances privées de type courrier électronique dont l'utilisateur n'est destinataire, ni directement, ni en copie.

L'utilisateur est tenu à une stricte confidentialité sur toute information relative au fonctionnement interne de l'établissement dont il a eu connaissance, notamment celle qui concerne la sécurité du système informatique, la mise en œuvre du contrôle d'accès aux locaux ou encore les données figurant dans les logiciels de gestion.

Article 7 : Règles d'usage des ressources informatiques

L'utilisateur ayant en charge une partie des données constituant le système d'information de l'établissement, il lui appartient de les protéger en utilisant les moyens de sauvegarde individuels ou collectifs mis à sa disposition.

Il est recommandé à l'utilisateur de changer régulièrement son mot de passe délivré à titre personnel, unique et confidentiel. Dans le cadre d'une communication professionnelle, l'utilisateur s'engage à n'utiliser que l'outil de messagerie mis à sa disposition par l'établissement. Une grande vigilance doit être apportée aux messages informatiques adressés en un seul envoi à une liste d'utilisateurs. L'intérêt réel de la correspondance et la taille des éventuelles pièces jointes doivent être pris en compte avec discernement.

L'utilisateur doit s'assurer lors d'une absence momentanée de son poste informatique de verrouiller ou de fermer les sessions ouvertes afin de ne pas laisser des ressources ou des services disponibles sans identification. Dans un souci d'économies d'énergies, l'utilisateur s'engage à mettre, quotidiennement ou en cas d'absence prolongée, son poste hors tension après avoir fermé l'ensemble des applications.

Lorsque les organisations syndicales utilisent des listes de diffusion, elles devront indiquer aux destinataires des messages syndicaux qu'ils peuvent demander à tout moment à en être radiés. Les partenaires sociaux sont tenus de faire droit à ces demandes dans les plus brefs délais.

Chapitre 2 : Rôle de l'administrateur du système informatique de l'établissement

Article 8 : Garantie du bon fonctionnement du système

L'administrateur est chargé par le Directeur Général de l'établissement de veiller au bon fonctionnement des ressources informatiques mises à disposition des utilisateurs au sein d'Oniris. Il lui appartient d'informer l'utilisateur des diverses contraintes d'exploitation et peut prendre toute disposition consistant à pallier un incident de fonctionnement ou de sécurité.

Afin d'assurer la sécurisation du système informatique, l'administrateur peut mettre en place des dispositifs de filtrage des communications. Il prend garde à ce que le système informatique soit utilisé à bon escient, dans le respect des règles s'imposant à tout utilisateur.

Article 9 : Surveillance et contrôle proportionnés

Chaque ordinateur présent sur le réseau possède sa propre identification. Chaque page visitée, chaque courrier électronique envoyé ou reçu, laisse une trace identifiant clairement le poste de l'utilisateur.

L'administrateur peut avoir accès, de par sa fonction, à des données personnelles. Dans le respect de la législation et des dispositions de la présente charte, seuls des contrôles visant au maintien de la sécurité du système informatique peuvent être réalisés. Ainsi, l'administrateur peut procéder à un contrôle « à postériori » des données de connexion au système informatique d'Oniris, restitué de manière globale et non nominative. En cas de dysfonctionnement manifeste, il peut procéder à des investigations plus poussées pour identifier le poste concerné ; ce contrôle nécessitant une information de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Article 10 : Respect du droit au respect de la vie privée

Le secret de correspondance de l'utilisateur est garantit par l'établissement ONIRIS, en particulier dans sa situation d'employeur. Il appartient à chaque utilisateur de placer leurs informations à caractère personnel dans un dossier intitulé « Données privées », accessibles en principe qu'après information préalable de l'intéressé.

Il convient de rappeler que tout dossier, fichier, document crée grâce aux moyens informatiques figurant au sein d'ONIRIS est présumé avoir un caractère professionnel, de sorte que l'administrateur peut y avoir accès sans que l'employé ne soit présent.

Nantes le, ...

NOM et Prénom (précédés de la mention "lu et approuvé")

Signature :