CHARTE INFORMATIQUE DE L'ETABLISSEMENT
SCHOOL INFORMATION TECHNOLOGY CHARTER

Préambule
Preamble

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.

This charter represents the internal regulations regarding the use of Oniris' Information Technology system.

The use of all means of Information Technology within Oniris implies that users must follow certain rules. The objective of these rules is to ensure the security and performance of IT facilities and tools, the preservation of confidential data as well as transmission and reception of information in accordance with applicable legislations.

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 :
Version définitive

-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.

Within Oniris, this charter applies to all users of the IT system, wheresoever located. It also applies to administrators of that system.
The term "Information Technology System" refers to a set of means implemented within the institution to facilitate exchanges, cooperative work, information research, information and document storage.

The IT system is composed of a set of "IT resources" integrated within the institution, namely hardware and network components, particularly servers, local and remote networks (Internet services), internal interconnection networks, and various peripheral devices. It is also composed of software provided by Oniris as well as all data, and all files used or created when using these software applications.

The term « user » refers to all people likely to create, implement or use one, or several, IT resources within the institution.

The term « administrator » refers to all people responsible for one, or several, IT resources.

This charter must allow for a balance between the respect of individual freedom and IT security within Oniris. The goal is to:

-Emphasize that IT means are mainly professional tools
-Establish the inherent security rules for all IT system use
-Make users aware of the consequences of any misuse of the IT system
-Remind users of the institution's rules regarding IT system use and possible means of control.

Failure to comply with all conditions of this charter is liable to result in legal liability. Any infringement of these rules renders the offender to disciplinary sanctions, without prejudice of criminal and/or civil proceedings that could be implemented, in compliance with the laws and regulations in force.

Chapitre 1 : Utilisation du système informatique de l'établissement Oniris
Chapter 1: The use of Oniris' IT system

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 1: Access conditions
Access to Oniris' IT system is primarily so as to carry out administrative or research and teaching activities.
The use of IT resources is subject to the acquisition of an authorisation granted by the Director-General.

The authorisation, which grants the user the right to a personalised account with password, is only granted upon signature of this charter agreement. The authorisation issued to the user is strictly personal. Nobody is authorised to use or lend other users' accounts. Each account holder is responsible for all activities associated with his/her account.

In principle, the authorisation ends when the activity that justified the account assignment in the first place is carried out.

Regarding anonymous mailboxes, the password must be modified by the new person in charge of the account, or the administrator.

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 2: General compliance with the laws and regulations in force
All Information Technology means must be used in compliance with the legislation concerning

the use of IT systems. Below are some of the dispositions applicable to all users of IT resources:

-The "Data Protection Act" of 6 January 1978
-The law of 7 March 1985 which especially prohibits all users to reproduce all, or partially, commercial software for other purposes than it's backup (licenses)
-The "Computer Fraud" law of 1 May 1988

Each user, especially students and Oniris' interns, as well as teachers and others staff members, regardless of their status, shall respect the public order and good conduct.

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 3: Specific compliance with the laws and regulations in force
The user must strictly comply with the legislation which prohibits psychological and sexual harassment, as well as all publications of content that is, or likely to be racist, paedophile, abusive and defamatory. The user agrees to avoid any personal opinion likely to be detrimental to the institution's image and reputation. All public communication must state if the user is speaking on behalf of him/herself or as a member of the institution.

It is also forbidden to circulate all, or part of, a work protected by the intellectual property code. Any document, photo, video and other copyright materials that are available because of IT resources access rights, are exclusively intended for those beneficiaries having received authorisation from the institution. The user agrees to not transmit any IT files to a third party, without having received prior permission from the owner. It must be expressly authorised if the intended circulation involves the Image Rights of the person, or people, involved.
Artificial Intelligence products available to the public are under the obligation of legal deposit.

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 4: Protection of Information Technology integrity
Each user is subject to the proper functioning regulations of the IT system enacted by the institution. The user is responsible for being aware of all updates regarding these regulations. The user is responsible for his/her use of the IT resources, from the IT hardware that must be used carefully, to IT access rights exclusively granted by the institution to the user.

The user agrees to avoid actions that might have harmful consequences on the institution's IT operating system. The user must be attentive so as to not create security threats, especially constituent threats due to bridges created with external systems, the introduction of "parasite software programmes" or the misappropriate use of means made available.

For security reasons, only the equipment purchased with the institution's, or unit's, budget, and approved by the Information Technology services, can be connected to the network. Personal computers cannot be connected to the wireless network available in some premises.

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 5: Preservation of Information Technology integrity
The user must contribute to the IT system security by notifying the competent IT services of all incidents likely to hinder its proper functioning. The user agrees to not hide his/her identity and to not usurp those of others. The use of encryption is subject to prior authorisation from the institution's Director-General.

The user cannot add peripheral devices or additional software (except Free Open-Source or licenced Software) intended for professional activity. Only the IT services are authorised to install further components on a specific hardware.

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 6: Preservation of confidential data
Users have access solely to personal or public documents. Furthermore, it is strictly prohibited to have knowledge of information held by other users, even if they had not explicitly protected this information. This rule also applies to private correspondences, such as electronic mail, of which the user is not the addressee, neither directly, nor in copy.

The user is required to maintain strict confidentiality regarding all of the institution's internal operating information, especially that which concerns IT security, the implementation of premises access control or management software data.

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.

Article 7: Use of IT resources rules
The user, who is responsible for a portion of the institution's IT system data, is also responsible for protecting this data by using the individual or collective backup facilities available.
The user is recommended to regularly change the assigned personal, unique and confidential password. When communicating professionally, the user agrees to use only the email address made available by the institution. Attention must be paid to electronic mails sent all at once to

a distribution list. All users

must take into account the importance of the messages and size of attached documents when sending an electronic mail.

The user must lock, or close, open sessions when momentarily leaving their computer so as to avoid making resources or services without any identification available to others. For purposes of energy conservation, the user agrees to switch off his/her computer on a daily basis, or in the case of an extended leave of absence, without forgetting to close all applications.

Trade Unions using mailing lists must indicate in their messages that all recipients may request to be eradicated from the mailing list. Social partners must respect these requests within a timely manner.

Chapitre 2 : Rôle de l'administrateur du système informatique de l'établissement
Chapter 2: The role of the institution's IT system administrator

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 8: Ensuring proper system functioning

Under the responsibility of the Director-General, the administrator's task is to monitor the proper functioning of the IT resources available to the users within Oniris. The administrator must inform all users of the various operational constraints, and may take all measures needed to address a break down or security breach.

In order to ensure the IT system security, the administrator may implement communication filter measures. The administrator verifies that the IT system is used properly and in accordance with the rules applying to all users.

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 9: Surveillance and relevant controls
Each computer connected to the network has its own identification. Each visited web page, each sent or received electronic mail, leaves a record that clearly identifies the user's computer.

As part of the administrator's responsibilities, he/she may access personal data. In accordance with the legislation and regulations of this charter, only controls regarding the maintenance of the IT system's security can be carried out. As such, the administrator can proceed with an "a posteriori" control of Oniris' IT system login information, which would be reproduced in a global and anonymous manner.

In case of obvious malfunction, the administrator may carry out further investigations in order to identify the computer involved. The administrator must inform the CNIL (Commission Nationale de l'Informatique et des Libertés) of this control.

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

Le secret de correspondance de l'utilisateur est garanti 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.

Article 10: Compliance with the right to privacy
The privacy of user correspondence is guaranteed by Oniris, particularly as an employer.

Each user must keep personal data in a file entitled "private information", in principle only available after prior notification from the concerned party.

It is important to remember that all folders, files and documents created via Oniris' IT facilities should be created for professional purposes, so that the administrator may have access to them without the presence of the user.

Nantes, le

NOM et Prénom (précédés de la mention "lu et approuvé")
First Name SURNAME (preceded by the handwritten words "Read and approved"

Signature :