DEFINITION

Cette charte, associée au règlement intérieur d'AMIO, est avant tout un code de bonne conduite. Elle a pour objet de préciser la responsabilité des utilisateurs avec la législation afin d'instaurer un usage correct des ressources informatiques et des services internet, avec des règles minimales de courtoisie et de respect d'autrui.

On désignera de façon générale sous le terme **« ressources informatiques »**, les moyens et les services informatiques à partir desquels il est possible d'accéder au réseau d'AMIO, que ce soit à distance, directement ou en cascade.

On désignera par **« services internet »**, la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations divers : web, messagerie, intranet, forum…

On désignera sous le terme **« utilisateur »**, les personnes accompagnées ayant accès ou utilisant les ressources informatiques et services internet.

ACCES 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 de la formation professionnelle des utilisateurs lors de l'ouverture de l'enseignement.

L'activité professionnelle est celle prévue par les statuts d'AMIO, à savoir : les activités d'enseignement et de recherche.

L'utilisation des ressources informatiques partagées d'AMIO et la connexion d'un équipement sur le réseau sont en outre soumises à autorisation. 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 lors du départ, même provisoire, de l'utilisateur.

AMIO pourra en outre prévoir des restrictions d'accès spécifiques à son organisation (carte à puce d'accès ou d'authentification, filtrage d'accès sécurisé…).

REGLES D'UTILISATION, DE SECURITE 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 d'AMIO.

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 :

Ce projet est cofinancé par le Fonds social européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020

- l'utilisateur 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'enseignement 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 (usage de clients VPN interdit),

- il ne doit pas tenter de s'approprier le mot de passe d'un autre utilisateur,

- il ne doit pas mettre en place un programme pour contourner la sécurité,

- il doit respecter les règles d'accès aux salles contenant le matériel informatique,

- il ne doit pas utiliser un poste de travail sans une permission explicite de la personne à qui il est attribué.

RESPECT DE LA LOI INFORMATIQUE ET LIBERTES - CONFIDENTIALITE DES INFORMATIONS - DROIT D'ACCES – PROTECTION DES DONNEES - RGPD

Un Délégué à la Protection des Données (DPO) est nommé au sein de l'établissement. Il veille à ce que les dispositions du Règlement Européen sur la Protection des Données (RGDP) et de la loi informatique et libertés soient appliquées tant en termes de respect et de confidentialité des données personnelles qu'en matière de droits d'accès à ces données.

Une information sur les fichiers contenant des données personnelles sera affichée au panneau indiquant les mentions obligatoires à transmettre aux personnes accompagnées, au RDC du bâtiment Hébergement.

Un registre concernant le traitement des données est tenu par le DPO. Il précise, notamment, les finalités de chaque traitement, les durées de conservation, les mesures de sécurité ainsi que les habilitations pour l'accès aux données.

Un document relatif au consentement, au recueil et à l'échange de données, est remis à chaque personne accompagnée. Il mentionne les finalités des fichiers de données à caractère personnel ainsi que éléments réglementaires concernant le partage de données, l'information et les droits des personnes.

Ce projet est cofinancé par le Fonds social européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020

Pour l'accès aux différentes ressources, une Authentification Multi Facteur est requise. Il est demandé aux personnes accompagnées de communiquer un numéro de téléphone portable et adresse email ou l'installation d'une application d'authentification sur un périphérique tiers, afin de répondre à cette exigence. Par la signature de cette charte, la personne accompagnée s'engage à fournir ces éléments.

Pour toute information complémentaire, la personne accompagnée peut se rapprocher du DPO. Les durées de conservation des principaux traitements de données à caractère personnel respectent les règles suivantes :

- 20 ans après la sortie de la personne accompagnée pour le dossier médical
- 5 ans après la sortie de la personne accompagnée pour le dossier administratif et d'accompagnement (hors médical)
- Les comptes office 365 qui vous permettent d'accéder aux différentes ressources de AMIO (AMIO-FIT, applications MS365, messagerie ...) seront supprimés 1an et 1 jour après le départ de formation de l'auditeur ou de l'usager.
- Un mail sera envoyé à l'auditeur ou l'usager 2 mois avant la suppression du compte.
- La licence d'accès (A3) aux applicatifs Office 365 (Word, Excel....) sera supprimée 1 jour après le départ de formation de l'usager.
- La licence d'accès à LinkedIn Learning sera supprimée 3 mois après le départ de formation de l'auditeur ou de l'usager.

Il est donc important que les personnes accompagnées conservent leur attestation de présence dans l'établissement pour faire valoir leurs droits (notamment en termes de retraite). Il ne pourra pas leur être délivré de duplicata après cette période de 5 ans.

Conformément aux articles 16, 17, 18 et 21 du Règlement européen sur la Protection des Données entré en vigueur en mai 2018, les personnes accompagnées disposent d'un droit d'accès et de rectification ou d'effacement des informations qui les concernent. Ils peuvent également s'opposer au traitement des informations qui les concernent dans la limite des dispositions légales.

Les personnes accompagnées peuvent faire valoir ces droits auprès de la Direction ou du médecin pour la partie liée aux données médicales en écrivant un courriel à l'adresse contact@2isa.com ou en écrivant un courrier aux coordonnées mentionnées dans le Livret d'accueil. Elles peuvent également saisir le Délégué à la Protection des Données à l'adresse suivante regis.coiffard@2isa.com.

Si la personne estime qu'elle ne parvient pas à exercer ses droits « informatique et libertés »,elle peut saisir la CNIL : https://www.cnil.fr.

CONDITIONS DE CONFIDENTIALITE

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

Ce projet est cofinancé par le Fonds social européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020

de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les avaient 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 sa formation, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi Informatique et Libertés, il devra auparavant s'assurer que l'enseignant en a fait la demande à la CNIL en concertation avec la Direction et en avoir reçu l'autorisation. Il est rappelé que cette autorisation n'est valable que pour le traitement défini dans la demande et pas pour le fichier lui-même.

RESPECT DE LA LEGISLATION 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. La copie d'un logiciel constitue le délit de contrefaçon sanctionné pénalement. L'auteur de la contrefaçon engage directement sa responsabilité, il peut être poursuivi devant les tribunaux (code de la propriété individuelle). Ces sauvegardes ne peuvent être effectuées que par la personne habilitée à cette fin par le Directeur de l'enseignement.

Par ailleurs, la personne ne doit pas utiliser de logiciels à caractère ludique, (pendant les heures de formation), et ne doit pas contourner les restrictions d'utilisation d'un logiciel.

PRESERVATION DE L'INTEGRITE DES SYSTEMES INFORMATIQUES

L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes 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… (Article 323-2 nouveau code pénal).

La simple accession à un système sans autorisation constitue un délit même s'il n'en est résulté aucune altération des données au fonctionnement dudit système. Si de telles altérations sont constatées les sanctions prévues sont doublées (Article 323-1 du nouveau code pénal).

Les actes consistant à empêcher un système de fonctionner par exemple par l'introduction de « virus » sont visés par l'article 323-2 du nouveau code pénal.

L'introduction ou la modification frauduleuse de données font l'objet des articles 323-3 et 323-4 du nouveau code pénal.

USAGE DES SERVICES INTERNET (WEB, MESSAGERIE, INTRANET, FORUM…)

L'utilisateur doit faire usage des services internet dans le cadre exclusif de ses activités sur la formation professionnelle et dans le respect de la législation en vigueur, lors des heures d'ouverture du Centre pour la formation.

Ce projet est cofinancé par le Fonds social européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020

En dehors des heures de cours, l'utilisateur fera usage d'internet en respect de toutes les règles 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 (enseignant, gestionnaire réseau),

- il ne doit pas chercher à utiliser les ressources d'internet, en contournant les outils de contrôle en place, par l'utilisation de programme ou site illicite ou « hacké »,

- 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 respectera le secret de la correspondance (lourdes sanctions article 226-15 et 432-9 du nouveau code pénal),

- 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 discussion…

- il n'émettra pas d'opinions personnelles susceptibles de porter préjudice aux différentes autorités desquelles il dépend,

- il doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire, pendant les heures de vacation sur internet, l'utilisateur s'interdit les téléchargements de gros fichiers.

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

ANALYSE ET CONTROLE 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.

Ce projet est cofinancé par le Fonds social européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020

L'administrateur peut dans le cadre de ses missions déchiffrer des données tout en restant soumis à une obligation de confidentialité.

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 06/01/78 dite « informatique et liberté » :

http://www.cnil.fr

SANCTIONS

Les gestionnaires réseaux et les formateurs sont tenus de faire respecter la charte.

Les utilisateurs peuvent demander l'aide des susnommés pour faire respecter leurs droits.

Les utilisateurs ne respectant pas les règles et obligations définies dans la présente charte et ceux qui ne signalent pas les tentatives de violation de leur compte sont passibles de sanctions.

Ils peuvent être sommairement déconnectés par les gestionnaires du réseau qui peuvent surveiller en détail les sessions de travail d'un utilisateur s'il existe un soupçon de non-respect de la charte.

Ils peuvent être traduits devant la Direction pour se voir appliquer les sanctions prévues dans le code du travail (avertissement, blâme, exclusion temporaire, exclusion définitive).

Ils peuvent faire l'objet de poursuites pénales engagées à la demande d'AMIO.

APPLICATION

La présente charte s'applique à l'ensemble des personnes accompagnées d'AMIO utilisant les moyens informatiques du Centre.

Elle est annexée au règlement intérieur et remis aux personnes accompagnées lors de leur arrivée en formation.

LA CHARTE D'ACCES AU RESEAU DE L'AMIO ET A INTERNET

Cette convention associée au règlement intérieur et à la charte internet a pour objet de préciser la responsabilité des utilisateurs. Elle permet le partage équitable des ressources informatiques et des services internet définis dans la charte internet. Elle est susceptible d'évoluer et de s'adapter en fonction des besoins et du comportement des utilisateurs.

POSSIBILITES ET AVANTAGES

Ce projet est cofinancé par le Fonds social européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020

- Accès internet - bâtiment Formation.
- Accès aux différents serveurs, documentations et informations de l'intranet.
- Accès internet - bâtiment Hébergement dans les 80 chambres
- Accès messagerie externe 2isa.org

Ce qui vous est fourni à l'Hébergement :

- le câble de connexion à la prise murale est fourni par AMIO et réservé exclusivement à cet usage; il reste la propriété d'AMIO et fera partie de l'état des lieux de la chambre.

La Responsable Hébergement fera signer un document qui confirmera l'utilisation de ce câble et la lecture de la convention.

- L'accès au réseau.

REGLES DE BONNE CONDUITE

Le débit internet est partagé entre tous les utilisateurs. Le débit ne peut-être satisfaisant pour tous que par le respect des plages horaires.

Une sensibilisation à la sécurité et aux règles de bonne conduite et de savoir-vivre de l'utilisateur du réseau est proposée à chaque nouvelle promotion.

Un logiciel permet de bloquer l'accès de certains sites, d'éditer des statistiques d'utilisation de la bande passante poste par poste. L'intégralité des connexions internet pour chaque utilisateur sont enregistrées dans une base de données et conservées pendant 1 an.

A l'Hébergement, chaque utilisateur doit s'authentifier pour se connecter à internet.

PLAGES HORAIRES

Pour éviter la saturation de la bande passante du réseau internet, les plages horaires, les jours, et les types de fichiers en téléchargement dans les sens entrant et sortant ont été définis de la façon suivante :

- Le jour pendant les heures de cours :

Accès interdit depuis les chambres de l'hébergement : pas de dérogation possible même pendant les horaires d'accès pédagogique à internet, pas de FTP, impossible d'accéder aux chambres depuis les salles de cours.

- Le jour de 6h du matin à 00h et en dehors des heures de cours :

Accès autorisé au web, en respectant la charte internet.

- La nuit de 00h à 6h du matin :

Ce projet est cofinancé par le Fonds social européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020
UNION EUROPEENNE

Accès autorisé avec respect de la charte internet.

Téléchargement possible de tous types de fichiers.

Les jours fériés, les plages horaires sont celles du dimanche. Les jours de départ en congés, l'après-midi, les horaires restent ceux des horaires de cours, pour simplifier la gestion des plages horaires. La plage horaire A est mise en place par un programmateur pour couper le réseau des chambres des personnes accompagnées.

En résumé : pas de téléchargement pendant les heures de cours, et téléchargement possible la nuit de minuit à 6 heures en utilisant les logiciels à programmation horaire.

OBLIGATIONS

Appliquer les conventions d'appellation des prises et des postes.

Utiliser exclusivement le câble de connexion fourni à la prise murale de la chambre ; il reste la propriété d'AMIO et fera partie de l'état des lieux de la chambre. La Responsable Hébergement fera signer des documents qui confirmeront l'utilisation de ce câble et la lecture de la charte.

Ne pas abuser des messages à diffusion générale. Les messages à caractère publicitaire sont interdits.

Respecter les droits d'auteur ou copyright.

Installer un Antivirus et le tenir à jour.

Avertir par la messagerie le service informatique (credo@2isa.com) pour tout incident concernant le réseau.

De façon générale, le propriétaire du PC est responsable de l'utilisation de son ordinateur, exemple : en cas de prêt d'un portable, emprunt… L'adresse MAC unique de la carte réseau est un identifiant.

Le stagiaire est responsable de son matériel et notamment de l'utilisation de sa connexion, ainsi que de la propagation des virus.

SANCTION

Une seule sanction en cas d'abus ou de gêne des autres utilisateurs du réseau, et de non-respect de la convention d'appellation des postes : retrait de l'accès au réseau pendant un mois (date à date).

Ex : saturation de la bande passante sur internet ou sur le réseau local, attaque logicielle, cheval de Troie. Atteinte à la sécurité et la confidentialité des données, accès malveillants sur les dossiers partagés par les utilisateurs avec la volonté de nuire, acte illégal… La sanction sera appliquée en accord avec la direction.

Ce projet est cofinancé par le Fonds social européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020
UNION EUROPEENNE

Charte remise en deux exemplaires,

Celui-ci est conservé par la personne et l'autre sera conservé par le Centre.

Signé le :

Pour AMIO: La personne accompagnée

Ce projet est cofinancé par le Fonds social européen dans le cadre du programme opérationnel national "Emploi et Inclusion" 2014-2020