CHIC MARMANDE - TONNEINS

ifps

INSTITUT DE FORMATION DES PROFESSIONNELS DE SANTÉ

CHARTE NUMERIQUE

Préambule

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet de l'Institut de Formation du CHIC de Marmande-Tonneins et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.

Elle pose des règles permettant d'assurer la sécurité et la performance du système d'information de l'établissement, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux utilisateurs, conformément à la politique de sécurité du système d'information définie par l'établissement.

Cette Charte a été validée par la direction de l'établissement de rattachement et présentée pour avis au Conseil Pédagogique. Elle constitue une annexe au Règlement Intérieur de l'Institut. L'équipe pédagogique et administrative ainsi que les formateurs non permanents sont invités à en prendre connaissance.

1. CHAMP D'APPLICATION

La présente Charte concerne les ressources informatiques, les services Internet et téléphoniques de l'institut de formation, ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe.

Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau
- Ordinateurs portables
- Serveurs
- Imprimantes simples ou multifonctions
- Tablettes
- Smartphones

Dans la présente Charte, sont désignés sous les termes suivants :

- **Ressources informatiques** : les moyens informatiques, ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'entité.
- **Outils de communication** : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'informations diverses (web, messagerie, forum, etc.).
- **Utilisateurs** : les personnes ayant accès ou utilisant les ressources informatiques et les services Internet de l'établissement.

2. CADRE REGLEMENTAIRE

Le cadre réglementaire de la sécurité de l'information est complexe. Il porte sur les grands thèmes suivants :

- Le traitement numérique des données, et plus précisément :
  - Le traitement de données à caractère personnel et le respect de la vie privée
  - Le traitement de données personnelles de santé
- La signature électronique des documents
- Le secret des correspondances
- La lutte contre la cybercriminalité
- La protection des logiciels et des bases de données et le droit d'auteur.

La présente Charte d'accès et d'usage du système d'information tient compte de la réglementation sur la sécurité de l'information en vigueur et des droits et libertés reconnus aux utilisateurs.

3. CRITERES FONDAMENTAUX DE LA SECURITE

3.1 PRINCIPES

L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatiques, imprimée ou écrite sur papier, imprimée sur des films (images), transmise par des réseaux informatiques privés ou internet, par la poste, oralement et/ou par téléphone…

La **sécurité de l'information** est caractérisée comme étant la préservation de :

- **Sa disponibilité** : l'information doit être accessible à l'utilisateur, quand celui-ci en a besoin

- **Son intégrité** : l'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie
- **Sa confidentialité** : l'information ne doit être accessible qu'aux personnes autorisées à y accéder
- **Sa traçabilité** : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

3.2 UNE MISSION SECURITE

La Direction du Système Informatique (DSI) à laquelle l'Institut de formation est rattaché fournit un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble, c'est-à-dire protéger les ressources contre des pannes, des erreurs ou des malveillances. Elle doit aussi protéger les intérêts économiques de l'établissement. Elle doit donc définir et empêcher les abus.

L'utilisation des ressources informatiques, l'usage des services Internet ainsi que du réseau pour y accéder sont limités au cadre exclusif de l'activité professionnelle, conformément à la législation en vigueur et aux règles de tolérance concernant la correspondance privée. Ainsi toute information est considérée comme professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Il appartient donc 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 ».

L'utilisation des ressources informatiques et la connexion au réseau d'un équipement sont soumises à autorisation de la Direction des Systèmes d'Information (DSI). Ceci est valable aussi bien pour les points d'accès (poste de travail dédié ou partagé), connexion sans-fil (Wi-Fi), ordinateur portable personnel, que pour les périphériques (imprimantes, graveurs de CD, scanners, appareils photos et caméras numériques, …). L'utilisation des périphériques de stockage externes (disques durs, clés USB, …) est soumise aux règles qui contribuent au maintien de la protection de l'information. Les raccordements des ressources informatiques ne pourront pas être modifiés sans autorisation préalable. Les utilisateurs disposent d'un compte individuel auquel ils accèdent en saisissant leur nom d'utilisateur (identification).

Le droit d'accès aux ressources informatiques de l'Institut de Formation est personnel, incessible et temporaire et peut être retiré à tout moment. Il disparaît notamment dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès.

4. DROITS ET DEVOIRS DES UTILISATEURS

4.1 CONDITIONS D'ACCES

Tout utilisateur est responsable de l'utilisation qu'il fait des ressources informatiques de l'Institut de Formation. Le droit d'accès est soumis à autorisation et assorti de moyens d'identification. Il peut être retiré si les conditions d'accès ne sont plus respectées ou si le comportement de l'utilisateur est contraire à la Charte. Les moyens d'accès ou d'identification (clé USB, code, mot de passe, etc...) sont remis à titre personnel et sont non cessibles. Ils ne peuvent être prêtés, donnés ou vendus à des tiers et sont rendus en fin d'activité. L'utilisateur doit prévenir les autorités de tout accès frauduleux ou tentative d'accès aux ressources qu'il utilise. Il est responsable de la protection de ses fichiers et de l'accès à ses données.

4.2 RESPECT DU CARACTERE CONFIDENTIEL DES INFORMATIONS

Les fichiers possédés par un utilisateur sont considérés comme privés, qu'ils soient ou non accessibles à d'autres utilisateurs. La lecture, la copie ou la modification d'un fichier ne peut être réalisée qu'après accord explicite et par écrit de son propriétaire. Si, dans l'accomplissement de son travail, l'étudiant est amené à constituer des fichiers tombant sous le coup de la loi "Informatique et Libertés", il devra auparavant demander l'autorisation à son propriétaire.

4.3 RESPECT MUTUEL DES PERSONNES

L'étudiant ne doit ni porter atteinte à la vie privée et à la personnalité de quiconque, ni nuire à l'activité professionnelle d'un tiers par l'utilisation de moyens informatiques.

4.4 RESPECT DE L'INTEGRITE DES RESSOURCES INFORMATIQUES

Aucune recherche sur la sécurité des ressources informatiques et des systèmes ne peut être effectuée sans autorisation préalable. Le développement, l'installation ou la simple copie d'un programme ayant les propriétés ci-dessous est interdite :

- Programme pour contourner la sécurité
- Programme saturant les ressources informatiques

5. RESPECT DE LA LEGISLATION CONCERNANT LA PROPRIETE INTELLECTUELLE

La reproduction, la représentation ou la diffusion d'une œuvre de l'esprit ou d'une création protégée au titre de droits voisins est soumise au respect des droits de propriété intellectuelle et nécessite une cession et/ou une autorisation émanant des titulaires des droits patrimoniaux et moraux prévus par le Code de la Propriété Intellectuelle, sous peine de constituer le délit de contrefaçon de droit d'auteur.

De même, les signes distinctifs et inventions étant susceptibles de protection au titre d'un droit de propriété intellectuelle, leur reproduction, représentation ou diffusion est susceptible de constituer, à défaut de telles cessions et/ou autorisations, le délit de contrefaçon de marque ou de logo.

En ce qui concerne plus particulièrement la reproduction et/ou l'utilisation d'un logiciel, il est rappelé qu'en l'absence d'autorisation du titulaire des droits de propriété intellectuelle sur ce logiciel ou en cas de non-respect des conditions et limites définies par celui-ci (en ce qui concerne notamment les copies de sauvegarde), cette reproduction et/ou utilisation peut également être constitutive du délit de contrefaçon.

II est enfin rappelé que les bases de données et les contenus en ligne sont protégés au bénéfice de leur auteur, outre par le droit d'auteur, par un droit spécifique.

6. PRESERVATION DE L'INTEGRITE DES SYSTEMES INFORMATIQUES

L'étudiant 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, sniffer...

7. USAGE DES SERVICES INTERNET

L'utilisation d'Internet doit être en rapport avec les activités pédagogiques de l'IFSI ; par conséquent, les règles déontologiques qui encadrent toute activité, règles fixées dans les bulletins officiels, doivent être respectées. L'utilisateur a droit à une information relative à l'utilisation des services Internet proposés par l'établissement. L'accès au réseau ne pourra être utilisé comme support d'activités à but lucratif ou de nature à porter atteinte à la libre concurrence. En particulier, la consultation d'Internet au sein de l'établissement ne doit pas être un moyen pour les utilisateurs de se procurer ou de participer à des jeux, des activités commerciales ou toute autre activité en contradiction avec la législation ou la déontologie propre au système éducatif. De même, les utilisateurs du réseau s'engagent à respecter le principe de laïcité (non-discrimination, neutralité religieuse et neutralité politique). Ils s'engagent également à ne pas utiliser les Services Internet pour la diffusion de « virus », « cheval de Troie », messages publicitaires en masse, chaînes de lettre ou mailing (junk mail, spam).

Tout étudiant qui ne se sera pas conformé à ces règles engagera sa responsabilité en cas de détériorations d'informations ou d'infractions aux dispositions en vigueur.

La création ou l'usage de tout service d'échange d'informations, matériel ou logiciel, local ou hébergé, est soumis à l'accord du Comité Exécutif, se prononçant après avis du comité web (dans le cas de service en ligne) et de la Direction des Systèmes d'Information.

8. LES MESSAGERIES

Chaque utilisateur peut bénéficier d'une adresse électronique de son choix. Toutefois il est demandé à chaque étudiant de créer une adresse électronique sous le format nom.prenom20XX.20XX@gmail.com.

Seule cette adresse sera utilisée pour toute correspondance entre les équipes pédagogiques et du secrétariat pour communiquer avec l'étudiant.

9. UTILISATION IDENTITAIRE

9.1 DROIT IMAGE ET REPUTATION

Les étudiants doivent signer une autorisation de la libre utilisation de leur voix et de leur image, (Article 9 du code civil). Ce document est signé en début de formation.

Concernant le droit à l'image et à la réputation de l'IFSI et de son hôpital de rattachement : l'utilisation des mots « Centre Hospitalier Intercommunal Marmande -Tonneins – CHIC MT», « IFSI Marmande-Tonneins » sont contrôlés sur la toile, ainsi que sur les réseaux sociaux publics. Le droit au respect de la réputation s'entend comme celui de ne pas voir entacher

l'honneur et la considération que les autres nous portent. La diffamation est une atteinte injustifiée à la réputation. Au sens large, elle recouvre l'injure et les autres messages qui jettent le discrédit sur l'IFSI ou sur le CHIC MT.

9.2 UTILISATION DU LOGO «CHIC MT » ET « IFSI CHIC MT » ET CHARTE GRAPHIQUE DE CELUI-CI

Le logo relève du "droit de marque", défini par la convention de Paris pour la protection de la propriété industrielle (1883). L'utilisation d'un logo est interdite dans tous les cas où elle peut entraîner une confusion avec son utilisation. L'autorisation d'emploi par un tiers sans autorisation ni de la part de la direction de l'IFSI, ni de la part du service de communication du centre hospitalier est proscrite.

10 LES SANCTIONS EN CAS DE NON-RESPECT DES RESTRICTIONS

Le non-respect de la présente charte ainsi que des textes de loi en vigueur peut exposer le contrevenant à des sanctions disciplinaires.

10.1 MESURES D'URGENCE

Le responsable informatique de l'IFSI peut en cas d'urgence : déconnecter un utilisateur avec ou sans préavis selon la gravité de la situation, isoler ou neutraliser provisoirement toute donnée ou fichier manifestement en contradiction avec la charte ou qui mettrait en péril la sécurité des moyens informatiques. La directrice peut exiger un retrait des codes d'accès.

10.2 LA FRAUDE INFORMATIQUE

La sanction de la fraude informatique relève de la compétence de la Chambre correctionnelle du Tribunal de Grande Instance. La fraude informatique est définie et sanctionnée par les articles 323-1 à 323-7 du nouveau code Pénal dans les termes suivants :

- Art.323-1 du code pénal : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est deux ans d'emprisonnement et de 30 000 euros d'amende ».

- Art.323.2 du code pénal : « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 euros d'amende ».

- Art.323.3 du code pénal : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier des données qu'il contient est puni de trois ans d'emprisonnement et de 45 000 euros d'amende ». La tentative de ces délits est punie des mêmes peines que le délit lui-même.

- Art.323-5 dispose notamment que les personnes physiques coupables des délits précités encourent les peines complémentaires suivantes : « interdiction pour une durée de cinq ans d'exercer les droits civiques, civils et de famille (droit de vote, d'être éligible, de témoigner en justice, d'être tuteur ou curateur…), interdiction pour une durée de cinq ans d'exercer une fonction publique, ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise… ».

La présente charte numérique s'applique à l'ensemble des étudiants utilisant les moyens informatiques de l'établissement, qui accèdent aux services de la salle informatique de l'IFSI et du matériel audio-visuel (portables, barco…). Elle est une annexe du règlement intérieur de l'IFSI du CHIC MT avec les conséquences y afférentes au plan disciplinaire en cas de manquements aux obligations qu'elle crée.

En raison de l'évolution rapide des technologies, cette charte pourra faire l'objet de modifications.