Charte d'utilisation des systèmes d'information

Objet de ce document : Charte d'utilisation des systèmes d'information de l'ICM : règles, droits, devoirs, contraintes et bonnes pratiques.

SOMMAIRE

1. Préambule

La charte a pour objet de définir les modalités et les conditions d'utilisation des moyens informatiques de l'ICM et d'Internet. Il s'agit d'un code de déontologie qui a pour objectif d'informer, de sensibiliser chaque utilisateur en proposant des règles d'utilisation, et de préciser la responsabilité en matière de droits et d'obligations de chacun. La transgression des règles de bonne conduite qui s'imposent peut conduire l'utilisateur à engager sa responsabilité civile ou pénale, ainsi que celle de l'institut.

La présente charte ne vise pas à être exhaustive en termes de droits qui doivent être respectés : elle contient les règles et obligations essentielles que l'utilisateur ne doit pas méconnaître sans préjudice du respect des autres lois, textes ou usages en vigueur.

Ce document est vivant: il est susceptible d'être modifié en fonction de l'évolution de la jurisprudence, de la législation, de la technologie et du système d'information de l'institut.

2. Consultation – Publicité

La présente charte constitue une annexe au Règlement Intérieur et à ce titre, sera transmise à l'Inspection du Travail et sera soumise, ainsi que ses éventuelles modifications, à la consultation des représentants du personnel.

Chaque utilisateur sera informé de son contenu.

3. Accès aux ressources informatiques

L'utilisation des ressources informatiques de l'ICM, l'usage des services réseau et internet 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, PDA (agenda), 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. De même toute modification des configurations logicielles des matériels mis à disposition par l'ICM est interdite.

Les utilisateurs disposent d'un compte individuel auquel ils accèdent en saisissant leur nom d'utilisateur et un mot de passe qu'ils choisissent eux-mêmes.

Le droit d'accès aux ressources informatiques de l'ICM 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, notamment en cas de départ de l'ICM. Il peut être retiré en cas de non respect de la présente charte.

4. Déontologie informatique

Chaque utilisateur est juridiquement responsable de l'usage qu'il fait des ressources informatiques et s'engage à respecter les règles de déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau, ou sur l'intégrité de l'outil informatique.

En particulier, il doit se garder :

- de masquer sa véritable identité,
- de s'approprier le mot de passe d'un autre utilisateur,
- de diffuser son mot de passe,
- de modifier, d'altérer ou de détruire des informations ne lui appartenant pas sur un des systèmes informatiques connectés au réseau de l'institut,
- de développer des outils mettant sciemment en cause l'intégrité des systèmes,
- de contourner les moyens de protection mis en place par l'ICM,
- d'accéder à des informations appartenant à d'autres utilisateurs sans leur autorisation, notamment le courrier électronique,
- de porter atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par l'intermédiaire de messages, textes ou images provocants ou à caractère raciste,
- d'interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés ou non au réseau (éteindre un serveur, déconnecter un câble réseau, introduire un virus…),
- de nuire à l'image de l'ICM par une mauvaise utilisation des outils,
- d'envoyer des données nominatives non cryptées par les outils de l'ICM.

Toute négligence grave ou répétée est considérée comme fautive et peut entraîner des mesures disciplinaires et la fermeture immédiate des droits d'accès.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation, le détournement à des fins personnelles et la nécessité de mettre en œuvre des moyens humains ou techniques supplémentaires pour en contrôler l'usage.

L'utilisateur a la charge, à son niveau, de contribuer à la sécurité générale. En particulier, il doit :

- assurer la protection de ses informations ; il est responsable des droits qu'il donne aux autres utilisateurs ; il lui appartient de protéger ses données en utilisant les moyens de sauvegarde mis à sa disposition,
- signaler toute tentative de violation de son compte, et, d'une manière plus générale, toute anomalie constatée,
- ne pas permettre à des personnes non autorisées par l'ICM l'usage ou l'accès à des données, des systèmes et des réseaux, soit à travers le matériel dont il a l'usage, soit par transfert volontaire de données par quelque moyen que ce soit (Internet, disquettes, CD, clés USB, …),

- choisir des mots de passe sûrs, les changer régulièrement, et veiller à leur secret,
- ne pas quitter son poste de travail ou un poste partagé sans se déconnecter ou verrouiller sa session[1].

De façon particulière, les utilisateurs ne doivent en aucun cas effectuer d'expérimentation sur la sécurité des systèmes et réseaux informatiques ou sur les virus informatiques.

Le développement, l'usage et la simple détention de logiciels ou programmes visant à contourner la sécurité des systèmes ou la protection des logiciels, sont strictement prohibés.

Tout travail, de recherche ou autre, qui pourrait amener l'utilisateur au non respect des règles ainsi définies ne pourra être accompli qu'avec l'autorisation de la DSI et dans le respect strict des règles qui seront alors définies.

5. Règles

5.1. Respect de la législation concernant la propriété intellectuelle

5.1.1. Logiciels

La mise à disposition des logiciels est effectuée par l'ICM par l'intermédiaire de la DSI en fonction des contrats de licence et droits d'usage passés avec des fournisseurs. Elle s'inscrit dans un cadre législatif et réglementaire.

Il est interdit de réaliser des copies de logiciels commerciaux pour quelque usage que ce soit.

L'utilisateur ne doit pas installer de logiciels lui-même, y compris ludiques, ni contourner les restrictions d'utilisation d'un logiciel.

5.1.2. Créations protégées par le droit d'auteur

Il est interdit de télécharger des vidéos, photographies, images, fichiers sonores ou autres créations protégées par le droit d'auteur ou un droit privatif sans avoir au préalable obtenu l'accord du titulaire de ces droits.

5.2. Respect de la législation concernant les données nominatives

Toute constitution, à l'aide des moyens informatiques de l'institut ou sur son réseau de traitements de données nominatives doit faire l'objet, préalablement à leur mise en œuvre, d'une déclaration ou d'une demande d'avis auprès de la Commission nationale informatique et libertés.

La DSI est garante du respect de la loi "Informatique et Libertés". A ce titre, la DSI prépare les documents de déclaration ou de demande d'avis pour tous les traitements automatisés d'informations nominatives mis en œuvre à l'initiative de la direction de l'institut. Les déclarations et demandes d'avis sont signés et adressées à la CNIL par la direction générale.

[1] la session peut être verrouillée manuellement ou par paramétrage de l'écran de veille.

Si dans l'accomplissement de son travail, l'utilisateur est amené à constituer des fichiers tombant sous le coup de la loi "Informatiques et Libertés", il doit auparavant en avoir demandé l'autorisation à la DSI et doit lui fournir tous les éléments nécessaires pour l'élaboration des documents de demande d'avis à la CNIL.

5.3. Usage des services Internet

L'utilisateur doit faire usage des services Internet dans le cadre de ses activités professionnelles et dans le respect des principes généraux et des règles propres aux sites consultés ainsi que dans le respect de la législation en vigueur.

L'utilisateur de la messagerie doit veiller à diffuser ses messages aux seuls destinataires concernés afin d'éviter l'encombrement inutile de la messagerie ainsi qu'une dégradation du service.

Tout utilisateur de l'Internet ne doit pas :

- harceler par e-mail (envoi de messages abusifs, pourriels (spams)…) un individu à l'aide des outils informatiques,
- se connecter ou essayer de se connecter sur un site sans y être autorisé (tentatives de piratage, usurpation d'identité, usage de comptes / mots de passes volés ou à l'insu de leur propriétaire, …),
- naviguer sur un site réputé interdit (site pornographique, pédophile, négationniste…),

Le non respect par l'utilisateur de ces principes pourra entraîner des sanctions disciplinaires, lesquelles peuvent aller jusqu'au licenciement pour faute grave ou lourde.

5.4. Exemples de risques et conséquences

La transmission d'informations nominatives ou la divulgation d'autres informations sensibles en clair par messagerie sont des atteintes à la confidentialité qui engagent la responsabilité de l'utilisateur responsable et de l'entreprise pour défaut de sécurité.

Le téléchargement par le web de logiciels douteux peut rendre possible l'intrusion de virus informatique et la divulgation d'informations.

Un mot de passe laissé en clair à coté d'un poste de travail peut être la porte ouverte à une introduction frauduleuse dans notre système d'information, qui pourrait aller jusqu'à la destruction de fichiers sur un serveur critique.

Le branchement d'un ordinateur sur le réseau téléphonique de l'ICM via un modem est une porte ouverte à une intrusion via l'autocommutateur, ce type de branchement n'est donc pas autorisé.

6. Information sur la gestion du système d'information

La gestion du système d'information nécessite des moyens pour satisfaire aux exigences légales, assurer son bon fonctionnement et sa sécurité. Les outils mis en place, notamment de surveillance n'ont pas d'autre but que de détecter les actions potentiellement dommageables pour le ICM, de protéger le système d'information et les utilisateurs. Le Code pénal fixe également une obligation de moyens quant à la sécurité des informations détenues par le ICM qui engage la responsabilité des utilisateurs et de l'ICM en cas d'accès illicite à des données nominatives.

6.1. Les responsabilités des administrateurs

Les administrateurs sont les personnes qui gèrent les postes de travail déployés dans l'institut, les serveurs sur lesquels sont installés les différents outils et services mis à la disposition des utilisateurs (messagerie, accès internet, partage de fichiers, bases de données, applications métier, espace de stockage, etc) ainsi que le réseau.

- Les administrateurs ont la charge de la bonne qualité du service fourni aux utilisateurs dans la limite des moyens alloués. Ils ont le droit d'entreprendre toute démarche nécessaire au bon fonctionnement des ressources informatiques de l'ICM ;
- Les administrateurs ont le devoir d'informer, dans la mesure du possible, les utilisateurs de toute intervention nécessaire, susceptible de perturber ou d'interrompre l'utilisation habituelle des moyens informatiques ;
- Les administrateurs ont le devoir d'informer immédiatement la DSI de toute tentative d'intrusion sur un système, ou de tout comportement délictueux d'un utilisateur ;
- Les administrateurs doivent impérativement respecter la confidentialité des fichiers des utilisateurs. Ainsi, en cas de départ d'un salarié, les administrateurs ne peuvent transférer les fichiers et messages vers un autre utilisateur sans autorisation explicite du salarié partant ;
- La DSI fait signer aux intervenants extérieurs un accord de confidentialité au sujet des informations du système d'information ;
- En cas de ré-affectation ou de mise au rebut d'un matériel, les administrateurs s'engagent à effacer préalablement les données enregistrées sur celui-ci ;

La liste des administrateurs est détenue est tenue à jour par la DSI.

6.2. Les fichiers de logs

Toute activité sur le réseau et les systèmes informatiques de l'ICM est susceptible de faire l'objet d'une surveillance par les administrateurs et les personnels dûment autorisés par la DSI.

L'ensemble des services utilisés génère, à l'occasion de leur emploi, "des fichiers de logs". Ces fichiers sont essentiels à l'administration des systèmes. Ils servent en effet à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations (exemple pour la messagerie: expéditeur, destinataire(s), date, …), mais aussi l'identification des sites web visités, les heures de connexion, le nom de la machine depuis laquelle les services sont utilisés, etc…

Ces systèmes ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une réquisition judiciaire et après information du directeur général, ces fichiers peuvent être mis à la disposition ou transmis aux autorités compétentes. La durée de conservation de ces fichiers de trace ne pourra être supérieure à un an.

Les navigateurs Web utilisent un système de "cache" qui conserve en local l'historique des pages visitées par l'utilisateur. De manière similaire, certains sites web stockent sur le poste de travail des données leur permettant de réafficher certaines informations propres à l'utilisateur à chaque visite dans de petits fichiers appelés cookies. Ces fichiers contiennent donc des informations nominatives (nom d'utilisateur sur le site, adresse e-mail, etc.).

6.3. Les outils de protection

Des outils sont mis en place pour protéger les postes des utilisateurs contre les virus et les pourriels (spams) :

- Les logiciels "antivirus" sur les postes des utilisateurs sont généralement paramétrés avec la stratégie suivante : si un virus est détecté, le logiciel tente de réparer le fichier, si la tentative échoue, le fichier est détruit.
- Un antivirus est également mis en place sur les serveurs de messagerie évitant ainsi de recevoir des virus et aussi d'en émettre à l'extérieur de l'ICM. De plus, certains fichiers joints aux messages peuvent être automatiquement éliminés en raison des risques d'infection qu'ils sont susceptibles de véhiculer.
- D'autres logiciels pourront être mis en place pour protéger au mieux les données des utilisateurs et les applications de l'ICM, notamment des logiciels anti-pourriels.

6.4. Sécurité physique

Les accès à la salle informatique et aux locaux techniques d'étages sont strictement réservés aux membres de la DSI. L'accès par toute autre personne doit être dûment autorisé par la DSI.

7. Glossaire

On désigne sous le terme "**utilisateur**", la personne ayant accès ou utilisant des ressources informatiques et services Internet.

On désigne sous le terme "**ressources informatiques**", les moyens informatiques permettant la recherche, l'envoi, le partage et le stockage d'information.

On désigne par "**services Internet**" la mise à disposition de moyens d'échanges et d'informations diverses par un ensemble de réseaux numériques interconnectés, interactifs : messagerie électronique, Web…

On désigne par "**administrateur**" les personnes qui gèrent les ressources informatiques (serveurs, bases de données, logiciels, réseau, postes de travail, …). Leurs rôles et responsabilités sont détaillés au §6-"Information sur la gestion du système d'information".

8. Interlocuteur

L'interlocuteur principal côté DSI concernant les divers aspects de la présente charte ou toute autre question de sécurité des SI est :
Caroline VIDAL
Tel. 01.57.27.40.41
Mail : caroline.vidal@icm-institute.org