CHAMBRE FRANÇAISE
DE COMMERCE ET D'INDUSTRIE
DU MAROC

CHARTE DU SYSTÈME D'INFORMATION CFCIM

SOMMAIRE

I. PREAMBULE

La présente charte définit les règles de bonne conduite et de sécurité que les utilisateurs sont tenus de respecter dans le cadre de l'utilisation du système d'information et de communication, et ce pour en assurer le bon usage et fonctionnement, dans le but de de promouvoir une utilisation loyale, responsable et sécurisée du système d'information de la CFCIM mis à disposition de l'ensemble des utilisateurs de la CFCIM.

Ces ressources et services constituent un élément nécessaire à l'exercice de l'activité de la CFCIM. Le non-respect des dispositions présentées ci-dessous est passible d'une sanction disciplinaire telle que prévue à l'article « G-Sanctions disciplinaires » du Règlement intérieur.

II. CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de la CFCIM, quel que soit leur statut, et dont ci-dessous la liste non-exhaustive :

- Les collaborateurs de la CFCIM, quel que soient la forme ou la durée de leur contrat de travail (CDI, CDD, contrat d'apprentissage, stagiaires ...) ;
- Les professeurs et étudiants au campus de la CFCIM ;
- Les visiteurs ;
- Les prestataires, sous-traitants de la CFCIM ;
- Les administrateurs du système d'information.

III. DEFINITION :

- **Utilisateurs :** toute personne autorisée à accéder aux locaux de la CFCIM, à ses outils informatiques ainsi qu'à ses moyens de communication.
- **Système d'information et de communication :** Il s'agit du parc informatique et des moyens de télécommunication de la CFCIM (ordinateurs, téléphones, photocopieurs, clés USB, etc.) et services (logiciels, intranet, messagerie, etc.)
- **Administrateurs système** : ils veillent au bon fonctionnement du système d'information, à sa disponibilité, sa maintenance, sa sécurité et à son évolution pour répondre au mieux aux besoins interne.

IV. DISPOSITIONS GENERALES :

1. Les règles de déontologie

Chaque utilisateur est responsable de l'usage qu'il fait des ressources du SI. Il s'engage à respecter les règles de la déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences dommageables voire graves, telles que les suivantes :

- Masquer sa véritable identité (un utilisateur doit, par exemple, indiquer sa véritable identité dans les correspondances par courrier électronique professionnel) ;
- S''approprier le mot de passe d'un autre utilisateur ;
- Modifier ou détruire des informations ne lui appartenant pas et se trouvant dans le système informatique de la CFCIM ;
- Accéder à des informations appartenant à d'autres utilisateurs sans leur autorisation ;
- Porter atteinte à l'intégrité d'un autre utilisateur, notamment par l'intermédiaire de messages, textes ou images provocants ;
- Interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés ou non au réseau ;
- Non-respect par l'utilisateur du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser.

2. Responsabilité de l'utilisateur

L'utilisateur est responsable des moyens informatiques mis à sa disposition. Il est responsable de la sécurité physique et des données contenues dans les moyens informatiques qui lui sont affectés ou qu'il utilise. Il doit contribuer à la sécurité du système d'information et ne pas effectuer d'opérations pouvant nuire au bon fonctionnement du système et à son intégrité. Il doit notamment :

- Protéger l'accès à ses données et au réseau ;
- Respecter les consignes retranscrites dans la présente charte ;
- Signaler tout incident ou dysfonctionnement du système (apparition de virus, présence ou disparition inopinée de fichiers, etc.) au service concerné ;
- S'interdire de consulter, charger, stocker, publier ou diffuser via les moyens informatiques et de communication, des documents, informations, programmes, images, et fichiers multimédia, … contraire à la loi ou à l'ordre public ou portant atteinte aux ressources de la CFCIM et plus particulièrement à l'intégrité et à la conservation des données de la CFCIM, ou portant atteinte à la confidentialité des informations et données de la CFCIM et/ou de ses utilisateurs ou contraire aux bonnes mœurs ou susceptibles de porter atteinte au respect de la personne humaine et de sa dignité ;
- Agir en toutes circonstances avec responsabilité, respecter les règles et procédures en vigueur, agir pour le bien de la CFCIM et de ses partenaires ;
- Respecter toutes les mesures de précaution, voire de confidentialité, si cela est demandé, pour l'utilisation des informations afin de protéger les intérêts de la CFCIM ;
- Alerter sa hiérarchie s'il est témoin d'un événement constituant une violation de la présente charte.
- Utilise uniquement les droits d'accès qui lui sont attribués et autorisés, l'information et les systèmes d'information qui sont mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés.

3. Droit d'accès

Conformément à la Loi 09-08, promulguée par le Dahir n° 1-09-15 du 18 safar 1430, les utilisateurs ont la possibilité de consulter toutes les données à caractère personnel les concernant et que la CFCIM peut détenir.

A cette fin les utilisateurs peuvent exercer ce droit :

- Soit en adressant un courrier (avec accusé de réception) à l'adresse postale suivante : CFCIM, 15 Avenue Mers sultan, 20250, Casablanca, Maroc.
- Soit en envoyant une requête par mail à l'adresse électronique suivante : Protection.donnees@cfcim.org.

Dans les deux cas, le demandeur devra joindre un justificatif d'identité à sa demande.

V. REGLES DE SECURITE ET PROTECTION DES DONNEES

1. Accès par les utilisateurs au système d'information

La CFCIM met à la disposition des utilisateurs des moyens informatiques et de communication lorsque ces ressources sont utiles, voire nécessaires à l'accomplissement de leur mission.

L'utilisation de ces derniers est soumise à autorisation préalable de la direction générale de la CFCIM et du responsable hiérarchique. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers.

Chaque responsable hiérarchique doit s'assurer de l'adéquation des autorisations accordées avec le travail confié à chaque utilisateur.

1.1 L'authentification

L'accès à certains éléments du système d'information est protégé par des paramètres de connexion (identifiant, mot de passe). Lors de la première utilisation de ces identifiants, l'utilisateur devra modifier le mot de passe qui lui aura été communiqué par un mot de passe personnel qui devra respecter un certain degré de complexité et devra être modifié régulièrement.

Actuellement, le mot de passe doit être composé de 12 caractères minimums combinant majuscules, minuscules, chiffres et caractères spéciaux :

- Il doit être renouvelé régulièrement ;
- il ne doit pas être transmis à des tiers ni être aisément accessible ;
- Il doit être saisi par l'utilisateur à chaque accès et ne pas être conservé en mémoire dans le système d'information.

A défaut, l'utilisateur risque un blocage de son compte. L'authentification prévoit une restriction de l'accès au compte mise en place par le service de l'informatique interne (verrouillage du compte après 10 échecs)

2. Accès au poste de travail en cas d'absence

Dans le cas où il serait nécessaire pour le supérieur hiérarchique ou par tout autre collaborateur de la CFCIM d'accéder au poste de travail de l'utilisateur ou à sa session en son absence (congés, maladie ou autre…), celui-ci devra donner au préalable son consentement écrit par email ou par SMS à son supérieur hiérarchique. Il devra également en informer le service informatique ainsi que le service social.

3. Sauvegarde des données

La CFCIM met en place un mécanisme de sauvegarde des données informatiques professionnelles, charge à l'utilisateur d'en respecter les règles d'exploitation prescrites.

La sauvegarde des données personnelles de l'utilisateur est en revanche à la charge exclusive de l'utilisateur.

Il est conseillé d'effectuer des sauvegardes régulières et Il est convenu que la CFCIM ne pourra être tenue pour responsable d'une perte et/ou d'une dégradation de données liée à un dossier « Personnel ».

4. Protection des données informatiques

L'objectif de la protection du système d'information est de maintenir la continuité des services offerts à l'utilisateur en garantissant l'intégrité et la confidentialité des données. Ainsi, il est formellement interdit :

- D'installer des logiciels contournant directement ou indirectement la sécurité;
- D'utiliser des programmes qui saturent les ressources ou inondent la bande passante ;
- D'introduire des programmes nuisibles (virus ou autres) ;
- D'effectuer des actes de piratage ou d'espionnage ;
- De modifier la configuration des machines ;
- D'utiliser, ou essayer d'utiliser, des comptes autres que le sien ou de masquer sa véritable identité.

L'utilisateur doit aussi protéger l'accès au matériel informatique (PC, PC Portable, etc.) qui lui est affecté. Il doit fermer les sessions ouvertes à son nom avant de quitter les lieux, ou activer la mise en veille automatique (protégée par mot de passe) après une courte période d'inactivité.

5. Protection des données papier

Les collaborateurs doivent débarrasser leurs bureaux de documents amassés, notamment des ceux contenant des informations sensibles, des notes, des post-it, ou tout autre document sous forme papier.

Les collaborateurs doivent déposer les dossiers sensibles dans leurs casiers à clé.

Les imprimantes et photocopieurs sont protégés par des mots de passe à usage personnel.

Protection contre les programmes malveillants :

Les postes de travail sont équipés de logiciels antivirus à jours fournis par la CFCIM.

Les utilisateurs doivent veiller à :

- Ce que les logiciels antivirus soient toujours actifs ;
- Les utiliser pour détecter la présence d'un virus suspect ;
- Signaler immédiatement au service informatique tout problème lié à la détection des virus.

Il est rappelé que l'installation d'autres logiciels antivirus non fournis par la CFCIM est interdite, cette installation pouvant provoquer d'autres incidents.

6. Protection de la vie privée :

La CFCIM ne pourra accéder aux données, fichiers et messages électroniques expressément désignés comme personnels ou privés par un utilisateur, qu'en présence de celui-ci ou celui-ci dûment appelé ou en cas d'événements, risques ou circonstances particulières qui l'imposent.

Lors de son départ, l'utilisateur doit restituer au service de l'informatique interne les matériels mis à sa disposition.

Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le chef de service.

VI. UTILISATION DES MOYENS INFORMATIQUES ET DE COMMUNICATION DE LA CFCIM :

1. Utilisation des ressources matérielles

Les matériels mis à disposition par l'entreprise sont placés sous la responsabilité des collaborateurs qui en font usage. Leur protection requiert soin et vigilance en toutes circonstances.

- L'utilisateur s'engage à ne pas apporter volontairement de perturbations au bon fonctionnement des systèmes informatiques par des manipulations anormales du matériel ;
- Toute réaffectation de matériel informatique et des logiciels correspondants doit obligatoirement s'opérer en coordination avec le service concerné ;
- Chaque utilisateur s'engage à prendre soin des matériels informatiques mis à sa disposition. Il informe le responsable SI de toute anomalie constatée.
- L'utilisateur ne doit pas modifier les équipements mis à sa disposition par l'ajout de logiciels ou de matériels qui n'auraient pas été préalablement validés par la CFCIM et dont les licences, pour les logiciels, n'auraient pas été acquises régulièrement par la CFCIM.
- L'utilisateur ne doit pas supprimer ou désactiver ou chercher à contourner les mesures de sécurité (antivirus, firewall et autres) installées sur les équipements locaux, distants ou sur toute partie du système d'information.

1.1 Accès aux ressources matérielles

Chaque utilisateur ayant ouvert une session sur un PC, une station de travail, un portable ou un serveur doit veiller à la fermer avant de quitter les lieux (notamment au niveau des espaces ouverts).

- L'accès au parc par les stagiaires et les visiteurs doit être placé sous le contrôle et la responsabilité de l'encadrant ;
- L'assignation des profils d'administrateurs est soumise à une étude et autorisée par le responsable du SI ;
- Les mots de passe utilisés par les administrateurs sont confidentiels et ne peuvent en aucun cas être divulgués ;
- L'accès des personnes étrangères aux locaux de l'entité informatique, ne peut se faire qu'en présence du personnel de cette entité ;
- Chaque entité doit veiller à contrôler l'accès aux locaux contenant des équipements informatiques mis à sa disposition

2. Utilisation des terminaux mobiles

Les utilisateurs peuvent disposer d'un terminal mobile, smartphone, tablette, pour leur activité professionnelle.

Il est rappelé que les consignes suivantes doivent être respectées par l'ensemble des utilisateurs détenteurs de terminaux mobiles :

- S'assurer que le mécanisme de verrouillage automatique est activé sur le terminal mobile, et si nécessaire mettre un mot de passe et configurer le verrouillage automatique ;
- Ne jamais laisser le terminal mobile sans surveillance (hôtels, cafés, lieux public, …) ;
- S'assurer que l'accès au terminal mobile est assujetti à une authentification (au minimum par mot de passe complexe) ;
- Changer de mot de passe régulièrement ;
- Ne jamais prêter son identifiant/mot de passe ni utiliser l'identifiant d'autrui ;
- Configurer le terminal mobile de manière à empêcher des connexions automatiques aux réseaux WI-FI, Bluetooth, … inconnus ou non sécurisés (gare, hôtel, aéroport, …).
- Désactiver les périphériques Bluetooth, WI-FI, … lorsqu'ils ne sont pas utilisés. Par ailleurs et par mesure de précaution, ces périphériques doivent être configurés de manière à ne pas être visibles aux utilisateurs d'autres terminaux ;
- Déconnecter toutes les sessions applicatives à la fin de l'utilisation du terminal mobile ;
- Respecter les consignes de sécurité complémentaires relatives à l'utilisation de la messagerie électronique ;
- Respecter les consignes de sécurité complémentaires relatives à l'utilisation d'Internet.

VII. UTILISATION DES LOGICIELS APPLICATIFS, PROGICIELS ET BUREAUTIQUE

Seuls les logiciels ayant été approuvés par l'entreprise et pour lesquels elle dispose des droits d'utilisation peuvent être installés dans le Système d'Information.

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par la personne habilitée à cette fin par le responsable de l'entité.

Par ailleurs, seul le service informatique chargé des installations de logiciels est autorisé à réaliser ou à distribuer des copies de logiciels fournies par la CFCIM.

VIII. UTILISATION DE LA MESSAGERIE ELECTRONIQUE

La CFCIM fournit à chaque utilisateur, en complément de l'utilisation de la messagerie, une adresse électronique qui lui permet d'échanger des courriels.

Les messages électroniques constituent des écrits pouvant engager la CFCIM. En conséquence, l'utilisateur doit faire usage de la messagerie électronique de la CFCIM dans le cadre exclusif de ses activités professionnelles et dans le respect de la législation en vigueur.

Ainsi l'utilisateur :

- Est responsable du contenu qu'il insère ou envoie par le biais de sa messagerie électronique ;
- A l'interdiction de lire ou de prendre connaissance de tout message électronique étant destiné à une autre personne ;
- Ne doit pas se connecter ou essayer de se connecter sur un serveur que via les canaux prévus ;
- Ne doit pas se livrer à des actions mettant en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- Ne doit pas s'approprier l'identité d'une autre personne et ne doit pas intercepter des communications entre tiers ;
- 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 ;
- Ne pas répondre ou ouvrir les pièces jointes d'un message dont l'objet ou l'expéditeur semble douteux ;
- Doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques ;
- Doit éviter de faire circuler des messages courriels non professionnels ou portant atteinte à l'intégrité d'un autre utilisateur ou à sa sensibilité, notamment par les messages comportant des images provocantes ou à caractère injurieux, raciste…

Il est rappelé que l'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le service informatique interne, et validées par la direction générale :

- Volumétrie de la messagerie,

- Taille maximale de l'envoi et de la réception d'un message (25 Mo)

- Nombre limité de destinataires simultanés lors de l'envoi d'un message (500)

Les utilisateurs peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (Webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé par l'utilisateur dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

IX. UTILISATION D'INTERNET

Les collaborateurs de la CFCIM, explicitement autorisés, ont accès à Internet. Ils l'utilisent dans un cadre professionnel et à titre d'information personnelle.

Les règles d'utilisation en vigueur sont :

- L'usage du réseau Internet est réservé à des activités répondant aux exigences professionnelles, et il est interdit en particulier la consultation de sites dont le contenu serait violent, offensant ou inapproprié tels que ceux appelant à la haine raciale à la violence, à la discrimination, etc. ;
- Les données publiées sur le net doivent être obtenues licitement sans porter atteinte au droit des tiers et sans y impliquer la CFCIM ;
- Ne pas fournir d'informations personnelles liées à la CFCIM ou ses partenaires, lors de l'accès à des sites à des fins personnelles ;
- Ne pas créer de comptes pour le téléchargement d'applications sans l'autorisation du responsable informatique ;
- Ne pas utiliser abusivement internet quand l'accès n'est pas purement professionnel ;
- Il est formellement interdit d'utiliser l'accès à internet accordé par la CFCIM pour porter atteinte, par n'importe quel moyen, à toute autre institution ou tiers, notamment à son patrimoine informationnel et/ou physique ;
- Ne pas ouvrir de liens inconnus ou dont le contenu n'est pas sûr ;
- Ne pas télécharger ni installer de données douteuses.

Il est rappelé qu'internet ne garantit aucune confidentialité sur les échanges qui y sont réalisés (fichiers, mails ou autres). Il est de la responsabilité de l'utilisateur d'estimer le niveau de confidentialité de l'échange qu'il désire réaliser et d'utiliser les outils qui permettent d'obtenir le niveau de confidentialité souhaité et qui peuvent être mis à disposition par l'entreprise uniquement pour une utilisation professionnelle.

1.1 Usage des réseaux sociaux, site internet /intranet de la CFCIM :

Il est rappelé que les réseaux sociaux n'offrent que des garanties très limitées en termes de confidentialité et de protection des données qui y sont déposées ainsi que d'authentification des utilisateurs qui y sont connectés. L'utilisation non conforme à la présente charte de ces

services est susceptible d'engager la responsabilité des utilisateurs. A ce titre, une vigilance renforcée de leur part est donc indispensable.

Ces services ne doivent donc pas être utilisés pour la diffusion ou le partage d'informations confidentielles de la CFCIM.

Les utilisateurs doivent veiller au respect des lois et règlements et par conséquent ne doivent pas faire de commentaires injurieux, diffamatoires ou racistes. Les collaborateurs sont personnellement tenus pour responsables des contenus ou commentaires publiés sur ces réseaux.

Seul le service communication et marketing pourra identifier préalablement, notamment sur l'intranet, les réseaux sociaux et sur le site internet de la CFCIM, les documents et informations qui peuvent être communiqués à l'extérieur, dans le cadre du respect de la réglementation relative à la propriété intellectuelle, au respect des droits d'auteur et à la réglementation sur la protection des données personnelles, et après obtention d'une autorisation de la direction générale.

1.2 Connexion à des réseaux wifi publics ou semi publics :

Le VPN étant installé par défaut sur les ordinateurs de la CFCIM, les utilisateurs sont invités à se connecter lors de leurs déplacements au réseau VPN de la CFCIM, et ce afin de sécuriser les échanges de données.

X. GESTION DES PRESTATAIRES ET SOUS-TRAITANTS DE LA CFCIM :

Pour les prestataires et sous-traitants de la CFCIM, les droits d'accès sont déterminés et attribués selon le contrat signé et la présente charte d'accès et d'usage du système d'information est systématiquement annexée au contrat.
Ce droit d'accès est strictement personnel et concédé à l'utilisateur pour des activités exclusivement professionnelles. Il ne peut être cédé, même temporairement à un tiers. Tout droit prend fin lors de la cession, même provisoire, de l'activité professionnelle de l'utilisateur.

Le non-respect des dispositions de la présente charte par l'utilisateur entraine systématiquement une sanction disciplinaire pouvant aboutir à une rupture du contrat avec le prestataire. Le mauvais usage des droits d'accès est de la même manière susceptible d'être sanctionné par des dispositions légales ou réglementaires.

XI. SURVEILLANCE DU SYSTEME D'INFORMATION

1. Principe :

Pour assurer la sécurité et le bon fonctionnement du système d'information et le respect de sa charte informatique, La CFCIM est amenée à mettre en place des outils de surveillance et de mesure sur les différentes ressources du système, en conservant une traçabilité des accès aux ressources informatiques (systèmes, données) et des échanges sur les réseaux et en particulier sur internet.

2. Filtrage :

La CFCIM a mis en place, pour répondre à ses obligations légales et assurer la sécurité du système d'information, un dispositif technique destiné à empêcher l'accès à des sites dont les contenus présentent un danger pour le système d'information car susceptibles de transmettre des virus et autres codes dangereux.

En revanche, le service informatique peut, après vérification et sur demande d'un utilisateur compte-tenu de la nature de ses fonctions et/ou des tâches à réaliser, débloquer les accès à certains sites ou services.

En ce qui concerne les mails entrants, la CFCIM a mis en place un mécanisme de filtrage qui permet de supprimer les mails non sollicités (SPAM) et/ou représentant des menaces pour le système informatique et les utilisateurs. Les filtrer en entrée permet d'économiser les ressources informatiques de l'entreprise aussi bien en termes de réseau que de stockage et de protéger les utilisateurs contre certains types de menaces.

Les utilisateurs ont la possibilité de consulter la liste des mails envoyés à leur adresse et rejetés par le système. Ils peuvent constituer leurs propres listes blanches et listes noires d'expéditeurs à autoriser ou à interdire expressément.

3. Les systèmes automatiques de traçabilité

Le service informatique de la CFCIM opère sans avertissement des investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, susceptibles de mettre en péril son fonctionnement ou son intégrité.

Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l'évènement. Le service informatique est le seul utilisateur de ces informations qui sont effacées à l'expiration d'un délai de 2 à 3 mois.

3.1 Eléments surveillés

Les données suivantes, sachant que cette liste n'est pas exhaustive, sont susceptibles d'être enregistrées :

- L'heure de la connexion ;
- L'identifiant de l'utilisateur ayant déclenché l'opération ;
- L'identification de l'équipement à partir duquel a eu lieu la tentative d'accès à un site bloqué ;
- Le système via lequel il a accédé ;
- Le type de transaction réalisé (copie, impression, transfert vers une autre machine) ;
- La durée de la connexion ;
- Les tentatives infructueuses, notamment celles concernant les opérations interdites ;
- Le nombre de messages émis et reçus classés par volume et par nature des pièces jointes ;
- Si l'accès au réseau de l'entreprise est opéré de l'extérieur via internet (accès de type "VPN"), l'identifiant de l'utilisateur connecté est également stocké.

Ces enregistrements permettent d'analyser la traçabilité à des fins d'études statistiques et de surveillance du système d'information de la CFCIM.

4. Gestion du poste de travail à distance :

A des fins de maintenance informatique, le service informatique peut accéder à distance à l'ensemble des postes de travail.

Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur qui aura préalablement été informé de la finalité de l'opération.

Dans le cadre de mises à jour et d'évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté à son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des postes de travail et s'interdit dans ce cas d'accéder aux contenus.

XII. GESTION DES INCIDENTS

Tout incident relatif à la sécurité des informations doit être signalé sans délai par l'utilisateur au service informatique et à son supérieur hiérarchique, notamment lorsqu'il s'agit de :

- Vol de matériel ;
- Courriers électroniques usurpant l'identité de personnes ou d'organismes, à des fins d'escroquerie ou de vol d'informations ;
- Comportements anormaux du poste de travail suite à la consultation de certains sites.

A des fins de gestion d'incidents, le CFCIM peut exercer ses pouvoirs et ses prérogatives dans le cadre de toute utilisation inappropriée de ses systèmes d'information ou des informations qui y sont détenus.

Pour planifier et gérer les incidents informatique, toutes les demandes d'assistance des utilisateurs doivent impérativement être formulées via l'application GLPI disponible sur l'intranet.

XIII. ADMINISTRATEURS DU SYSTEME D'INFORMATION

Par la nature de ses fonctions, l'administrateur est conduit à avoir accès à l'ensemble des informations relatives aux utilisateurs, y compris celles qui sont enregistrées sur leur poste de travail.

Toutefois, l'administrateur est soumis à une obligation de confidentialité et de discrétion professionnelle. Il ne peut donc divulguer les informations qu'il est amené à connaître dans le cadre de ses fonctions, en particulier lorsqu'elles sont couvertes par le secret des correspondances ou qu'elles relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité.

De plus, aucune exploitation de ces informations à des fins autres que celles liées au bon fonctionnement et à la sécurité des ressources informatiques, services internet et services intranet, ne saurait être opérée.
L'administrateur ne peut prendre connaissance ou tenter de prendre connaissance du contenu des répertoires, fichiers ou messages manifestement et explicitement désignés comme personnels, qu'en présence de la direction générale et avec son accord.
En cas d'urgence ou de nécessité vis-à-vis de la législation ou de la sécurité et dans l'hypothèse où il y accéderait, il s'engage à en assurer la confidentialité et l'intégrité dans les conditions de la présente charte.

L'administrateur s'engage à prendre toutes les mesures de sécurité nécessaires à la protection des informations et au maintien de leur confidentialité.

1. L'authentification :

L'accès aux systèmes d'information est protégé par un mot de passe individuel. Ce mot de passe doit être mémorisé par l'administrateur, Il ne doit pas être transmis ou confié à un tiers ou être rendu accessible.

Toutefois, une enveloppe fermée et cachetée contenant les mots de passe des collaborateurs est en possession de la direction générale, à l'issue de tests de conformité effectué par le service IT qui s'assure au préalable de l'exactitude des données remises

Le login et le mot de passe doivent être saisis lors de chaque accès au système d'information.

Le mot de passe est composé de 14 caractères qui doivent obligatoirement être une combinaison de :

- Caractères alphanumériques ;
- Chiffres ;
- Majuscules ;
- Minuscules ;
- Caractères spéciaux.

XIV. DISPOSITIONS FINALES

1. Sanctions

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre, sous forme d'avertissements, de limitation ou de suspension d'utilisation de l'ensemble ou d'une partie du système d'information et de communication, voire à des sanctions disciplinaires proportionnées à la gravité des faits commis.

Dans ce dernier cas, les procédures prévues par le Règlement intérieur de la CFCIM et par le Code du travail seront appliquées.

2. Modification de la charte

Cette charte est susceptible d'être modifiée à chaque fois que l'usage des ressources informatiques, le changement des dispositions réglementaires et/ou les évolutions technologiques l'imposent.

3. Engagement et acceptation

La présente charte doit être signée par chaque utilisateur du système d'information de la CFCIM. Par ailleurs, l'utilisateur sera informé des éventuelles mises à jour apportées au document.