Centre Hospitalier Intercommunal Monts et Barrages

CHIMB – Chemin du Panaud – 87400 SAINT LEONARD-DE-NOBLAT – TEL. : 05.55.56.43.00
SITE JALOUNEIX-BERTROFF - ROUTE DU MONT – 87460 BUJALEUF – TEL : 05.55.69.53.53

CHARTE D'ACCES ET D'USAGE DU SYSTEME D'INFORMATION

Version 1.1 du 15 octobre 2021

Table des matières

1. OBJET DU DOCUMENT 2
2. CHAMP D'APPLICATION 2
3. CADRE REGLEMENTAIRE 3
4. CRITERES FONDAMENTAUX DE LA SECURITE 3
4.1 PRINCIPES 3
4.2 UNE MISSION SECURITE 3
4.3 UN ENJEU TECHNIQUE ET ORGANISATIONNEL 4
4.4 UNE GESTION DES RISQUES 4
5. REGLES DE SECURITE 4
5.1 CONFIDENTIALITE DE L'INFORMATION ET OBLIGATION DE DISCRETION 5
5.2 PROTECTION DE L'INFORMATION 5
5.3 USAGE DES RESSOURCES INFORMATIQUES 6
5.4 USAGE DES OUTILS DE COMMUNICATION 6
5.5 USAGE DES LOGINS ET DES MOTS DE PASSE (OU DE CARTES CPS OU EQUIVALENT) 8
5.6 IMAGE DE MARQUE DE L'ETABLISSEMENT 9
6. INFORMATIQUE ET LIBERTES 9
7. SURVEILLANCE DU SYSTEME D'INFORMATION 9
7.1 CONTROLE 9
7.2 TRAÇABILITE 9
7.3 ALERTES 10
8. RESPONSABILITES ET SANCTIONS 10
9. VALIDITE 10
10. DISPOSITIONS FINALES 10

1. OBJET DU DOCUMENT

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet du CHIMB 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. Préalablement à sa mise en œuvre, elle est notifiée au Directoire, à la Commission Médicale d'Etablissement et Comité Technique d'Etablissement. Toute personne autorisée à accéder au système d'information du CHIMB doit en prendre connaissance.

2. CHAMP D'APPLICATION

La présente Charte concerne les ressources informatiques, les services internet et téléphoniques du CHIMB, 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 ;
- Terminaux portables ;
- Imprimantes simples ou multifonctions ;
- Tablettes ;
- Smartphones ;
- Objets connectés de toutes natures.

Cette Charte s'applique à l'ensemble du personnel de l'établissement de santé, tous statuts confondus, et concerne notamment les agents permanents ou temporaires (CDD, stagiaires, internes, prestataires, fournisseurs, sous-traitants, …) utilisant les moyens informatiques de l'établissement et les personnes auxquelles il est possible d'accéder au système d'information à distance directement ou à partir du réseau administré par l'établissement.

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'établissement ;
- **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.

3. 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 ;
- Le droit d'accès des patients et des professionnels de santé aux données médicales ;
- L'hébergement de données médicales ;
- Le secret professionnel et le secret médical ;
- 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.

4. CRITERES FONDAMENTAUX DE LA SECURITE

4.1 PRINCIPES

Le CHIMB héberge des données et des informations médicales et administratives sur les patients qu'il reçoit (dossier médical, dossier de soins, dossier images et autres dossiers médicotechniques, …), et sur son personnel (paie, gestion du temps, évaluations, accès à Internet et à la messagerie, …). L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatiques, imprimée ou écrite sur papier, 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.

4.2 UNE MISSION SECURITE

Le CHIMB fournit un système d'information qui s'appuie très largement sur une infrastructure informatique. Le service informatique doit assurer la mise en sécurité de cette

infrastructure, c'est-à-dire protéger ces ressources contre des pannes, des erreurs ou des malveillances. Il doit aussi protéger les intérêts économiques de l'établissement en s'assurant que ces moyens sont bien au service de la production de soins. Il doit donc contribuer à empêcher les abus.

4.3 UN ENJEU TECHNIQUE ET ORGANISATIONNEL

Les enjeux majeurs de la sécurité sont la qualité et la continuité des soins ainsi que le respect du cadre juridique sur l'usage des données personnelles de santé. Pour cela, le service informatique du CHIMB, en étroite relation avec le Responsable Sécurité et Système d'Information (RSSI), déploie un ensemble de dispositifs techniques mais aussi organisationnels. En effet, au-delà des outils, la bonne utilisation des moyens informatiques est essentielle pour garantir un bon niveau de sécurité. La sécurité peut être assimilée à une chaîne dont la solidité dépend du maillon le plus faible. Certains comportements humains, par ignorance des risques, peuvent fragiliser le système d'information.

4.4 UNE GESTION DES RISQUES

L'information médicale, qu'elle soit numérique ou non, est un composant sensible qui intervient dans tous les processus de prise en charge des patients. Une information manquante, altérée ou indisponible pourrait avoir des conséquences importantes pour le patient (exemples : erreur dans l'identification d'un patient (homonymie par exemple), perte de données suite à une erreur d'utilisation d'une application informatique, …). La sécurité repose donc sur une gestion des risques potentiels, des suivis d'incidents, des dispositifs d'alertes. La communication vers les utilisateurs est un volet important de cette gestion et la présente Charte d'accès et d'usage du système d'information s'inscrit dans cette démarche.

5. REGLES DE SECURITE

L'accès au système d'information du CHIMB est effectué selon les métiers de l'agent définis dans le logiciel de paye pour les personnels rémunérés par l'établissement. Pour les intervenants extérieurs et stagiaires, l'accès est défini par le service informatique en concertation avec les maîtres de stages et avec les responsables de services.

La présente Charte d'accès et d'usage du système d'information est remise à l'agent au moment de l'embauche pour le personnel rémunéré par l'établissement. La signature du récépissé vaut autorisation d'accès au système d'information. Le récépissé est classé au dossier administratif de l'agent.

Concernant les intervenants extérieurs et les stagiaires, la charte est communiquée via les maîtres de stages ou responsable de services. Le récépissé est classé au service informatique.

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 cessation, même provisoire, de l'activité professionnelle de l'utilisateur, ou en cas de non-respect des dispositions de la présente Charte par l'utilisateur.

L'obtention d'un droit d'accès au système d'information de l'établissement de santé donne à l'utilisateur des droits mais également des responsabilités qui sont précisées dans les paragraphes ci-dessous.

5.1 CONFIDENTIALITE DE L'INFORMATION ET OBLIGATION DE DISCRETION

Le personnel de l'établissement est soumis au secret professionnel et/ou médical. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données de santé. Les membres du personnel se doivent de faire preuve d'une discrétion absolue dans l'exercice de leurs missions respectives. Un comportement exemplaire est exigé dans toute communication, orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés. Il est ainsi interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courriers électroniques dont l'utilisateur n'est ni directement destinataire, ni en copie.

L'accès aux données de santé à caractère personnel des patients par des professionnels habilités se fait dans la majorité des cas par l'utilisation d'une carte CPS ou CPE. En l'absence de tel dispositif ou de sa défaillance, l'accès est conditionné par la détention d'un login et d'un mot de passe robuste.

L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ ou confidentielles couvertes par le secret professionnel.

5.2 PROTECTION DE L'INFORMATION

Les postes de travail permettent l'accès aux applications du système d'information. Ils permettent également d'élaborer des documents bureautiques. Il est important de ne stocker aucune donnée ni aucun document sur ces postes (disques durs locaux). Les bases de données associées aux applications sont implantées sur des serveurs centraux eux-mêmes situés dans des salles protégées. De même, les documents bureautiques produits doivent être stockés sur des serveurs de fichiers. Ces espaces sont à usage professionnel uniquement. Le stockage de données privées sur des disques réseau est interdit.

Le cas échéant, ceux qui utilisent un matériel portable (exemples : poste, tablette, smart phone, …) ne doivent pas le mettre en évidence pendant un déplacement, ni exposer son contenu à la vue d'un voisin de train … ; le matériel doit être rangé en lieu sûr. De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD, clé USB, disque dur, …). Aucune donnée de santé à caractère personnel des patients ne doit être stockée sur des postes ou périphériques personnels.

Il faut également mettre sous clé tout dossier ou document confidentiel lorsqu'on quitte son espace de travail.

Les médias de stockage amovibles (exemples : clefs USB, CD-ROM, disques durs …) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) ou risques de perte de données. Leur usage doit faire l'objet d'une très grande vigilance. L'établissement se réserve le droit de

limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques.

L'utilisateur ne doit pas transmettre de fichiers sensibles à une personne qui en ferait la demande et qu'il ne connaitrait pas, même s'il s'agit d'une adresse électronique interne à l'établissement.

5.3 USAGE DES RESSOURCES INFORMATIQUES

Seules des personnes habilitées de l'établissement de santé (ou par son intermédiaire la société avec laquelle il a contracté) ont le droit d'installer de nouveaux logiciels, de connecter de nouveaux PC au réseau de l'établissement et plus globalement d'installer de nouveaux matériels informatiques.

L'utilisateur s'engage à ne pas modifier la configuration des ressources (matériels, réseaux, …) mises à sa disposition, sans avoir reçu l'accord préalable du service informatique (ou par son intermédiaire la société avec laquelle il a contracté).

Les logiciels commerciaux acquis par l'établissement ne doivent pas faire l'objet de copies de sauvegarde par l'utilisateur, ces dernières ne pouvant être effectuées que par le service informatique.

5.4 USAGE DES OUTILS DE COMMUNICATION

Les outils de communication tels que le téléphone, le fax, Internet ou la messagerie sont destinés à un usage exclusivement professionnel. L'usage à titre personnel, dans le cadre des nécessités de la vie privée, est toléré à condition qu'il soit très occasionnel et raisonnable, qu'il soit conforme à la législation en vigueur et qu'il ne puisse pas porter atteinte à l'image de marque de l'établissement de santé. Il ne doit en aucun cas être porté à la vue des patients ou de visiteurs et accompagnants.

- **Usage du téléphone et du fax**

Le téléphone et le fax sont des moyens potentiels d'échanges de données qui présentent des risques puisque l'identité de l'interlocuteur qui répond au téléphone ou de celui qui réceptionne un fax n'est pas garantie.

Il ne faut ainsi communiquer aucune information sensible par téléphone, notamment des informations nominatives, médicales ou non, ainsi que des informations ayant trait au fonctionnement interne de l'établissement. Exceptionnellement, une communication d'information médicale peut être faite après avoir vérifié l'identité de l'interlocuteur téléphonique. Si un doute subsiste, le numéro de téléphone de l'interlocuteur indiqué doit être vérifié, le cas échéant, dans les annuaires de patients ou professionnels.

La communication d'informations médicales (exemples : résultats d'examens, …) aux patients et aux professionnels extérieurs est strictement réglementée. Les utilisateurs concernés doivent se conformer à la réglementation et aux procédures de l'établissement en vigueur.

- **Usage d'Internet**

L'accès à l'Internet a pour objectif d'aider les membres du personnel à trouver des informations nécessaires à leurs missions, ou dans le cadre de projets spécifiques.

Il est rappelé aux utilisateurs que, lorsqu'ils « naviguent » sur l'Internet, leur identifiant est enregistré. Il conviendra donc d'être particulièrement vigilant lors de l'utilisation de l'Internet et à ne pas mettre en danger l'image ou les intérêts de l'établissement de santé.

Par ailleurs, les données concernant l'utilisateur (exemples : sites consultés, messages échangés, données fournies à travers un formulaire, données collectées à l'insu de l'utilisateur, …) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciales. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur l'Internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle.

Il est interdit de se connecter ou de tenter de se connecter à Internet par des moyens autres que ceux fournis par l'établissement. Il est interdit de participer à des forums, blogs et groupes de discussion à des fins non professionnelles et de se connecter sur des sites à caractère injurieux, violent, raciste, discriminatoire, pornographique, diffamatoire ou manifestement contraires à l'ordre public.

Tous les accès Internet sont tracés et enregistrés et conservés par un dispositif de filtrage et de traçabilité. Il est donc possible pour l'établissement de connaître, pour chaque salarié, le détail de son activité sur l'Internet.

Ce contrôle des accès aux sites visités permet de filtrer les sites jugés indésirables, notamment des sites dangereux pour la sécurité du réseau. Il permet de détecter, de bloquer et ou de signaler les accès abusifs (en matière de débits, volumes, durées), ou les accès à des sites illicites et/ou interdits.

- **Usage de la messagerie**

L'usage de la messagerie est autorisé à l'ensemble du personnel. La messagerie permet de faciliter les échanges entre les professionnels de l'établissement.

Les utilisateurs doivent garder à l'esprit que leurs messages électroniques peuvent être stockés, réutilisés, exploités à des fins auxquelles ils n'auraient pas pensé en les rédigeant, constituer une preuve ou un commencement de preuve par écrit ou valoir offre ou acceptation de manière à former un contrat entre le CHIMB et son interlocuteur, même en l'absence de contrat signé de façon manuscrite.

Un usage privé de la messagerie est toléré s'il reste exceptionnel. Les messages personnels doivent comporter explicitement la mention « privé » dans l'objet. A défaut, les messages seront réputés relever de la correspondance professionnelle. Les messages marqués « privé » ne doivent pas comporter de signature d'ordre professionnel à l'intérieur du message.

L'usage des listes de diffusion doit être strictement professionnel.

Il est strictement interdit d'utiliser la messagerie pour des messages d'ordre commercial ou publicitaire, du prosélytisme, du harcèlement, des messages insultants ou de dénigrement, des textes ou des images provocants et/ou illicites, ou pour propager des opinions personnelles qui pourraient engager la responsabilité de l'établissement ou porter atteinte à son image. Les utilisateurs sont tenus par leurs clauses de confidentialité et de loyauté contractuelles dans le contenu des informations qu'ils transmettent par email.

Afin de ne pas surcharger les serveurs de messagerie, les utilisateurs doivent veiller à éviter l'envoi de pièces jointes volumineuses, notamment lorsque le message comporte plusieurs destinataires. Seules les pièces jointes professionnelles de type « documents » ou « images » sont autorisées. Il est rappelé que le réseau Internet n'est pas un moyen de transport sécurisé. Il ne doit donc pas servir à l'échange d'informations médicales nominatives en clair. En l'absence de dispositif de chiffrement de l'information de bout en bout, les informations médicales doivent être rendues anonymes.

Il est strictement interdit d'ouvrir ou de lire des messages électroniques d'un autre utilisateur, sauf si ce dernier a donné son autorisation explicite.

5.5 USAGE DES LOGINS ET DES MOTS DE PASSE (OU DE CARTES CPS OU EQUIVALENT)

Chaque utilisateur dispose d'un compte nominatif lui permettant d'accéder aux applications et aux systèmes informatiques de l'établissement. Ce compte est personnel. Il est strictement interdit d'usurper une identité en utilisant ou en tentant d'utiliser le compte d'un autre utilisateur ou en agissant de façon anonyme dans le système d'information.

Pour utiliser ce compte nominatif, l'utilisateur dispose dans la majorité des cas d'une carte CPS (ou équivalent) à laquelle est associé un code personnel à 4 chiffres.

Pour les personnes ne détenant pas de carte CPS/CPE, l'utilisation d'un login et d'un mot de passe est requise. Le mot de passe choisi doit être robuste (8 caractères minimum, mélange de chiffres, lettres et caractères spéciaux), de préférence simple à mémoriser, mais surtout complexe à deviner. Il doit être changé à minima 1 fois par an. Le mot de passe initial est fourni par le service informatique, il est strictement confidentiel. Il ne doit pas être communiqué à qui que ce soit : ni à des collègues, ni à sa hiérarchie. Il peut être modifié sur demande auprès du service informatique.

De fait, chaque utilisateur est responsable de son login et de son mot de passe et/ou de sa carte CPS/CPE, et de l'usage qui en est fait. Il ne doit ainsi pas permettre à des tiers non autorisés l'accès aux systèmes et aux réseaux de l'établissement dont il a l'usage. La plupart des systèmes informatiques et des applications de l'établissement assurent une traçabilité complète des accès et des opérations réalisées à partir des comptes sur les applications médicales et médico-techniques, les applications administratives, le réseau, la messagerie, l'Internet, … Il est ainsi possible pour l'établissement de vérifier a posteriori l'identité de l'utilisateur ayant accédé ou tenté d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.

C'est pourquoi il est important que l'utilisateur veille à ce que personne ne puisse se connecter avec son propre compte. Pour cela, il convient de fermer ou verrouiller sa session lorsqu'on quitte son poste. Il ne faut jamais se connecter sur plusieurs postes à la fois. Pour les postes qui ne sont pas utilisés pendant la nuit, il est impératif de fermer sa session systématiquement avant de quitter son poste le soir.

Il est interdit de contourner ou de tenter de contourner les restrictions d'accès aux logiciels. Ceux-ci doivent être utilisés conformément aux principes d'utilisation communiqués lors de formations ou dans les manuels et procédures remis aux utilisateurs.

L'utilisateur s'engage enfin à signaler toute tentative de violation de son compte personnel.

5.6 IMAGE DE MARQUE DE L'ETABLISSEMENT

Les utilisateurs de moyens informatiques ne doivent pas nuire à la réputation de l'établissement en utilisant des moyens, que ce soit en interne ou en externe, à travers des communications d'informations à l'extérieur de l'établissement ou du fait de leurs accès à Internet.

6. INFORMATIQUE ET LIBERTES

Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée auprès du Délégué à la Protection des Données du CHIMB, qui étudie alors la pertinence des données recueillies, la finalité du fichier, les durées de conservation prévues, les destinataires des données, le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour protéger les données. Le DPD procède ensuite aux opérations de déclaration et d'information réglementaires.

7. SURVEILLANCE DU SYSTEME D'INFORMATION

7.1 CONTROLE

Pour des nécessités de maintenance et de gestion, l'utilisation des ressources matérielles ou logicielles, les échanges via le réseau, ainsi que les rapports des télécommunications peuvent être analysés et contrôlés dans le respect de la législation applicable, et notamment de la loi Informatique et Libertés.

7.2 TRAÇABILITE

En relation avec le RSSI, le service informatique du CHIMB assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition, pour des raisons d'exigence règlementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

Par conséquent, les applications de l'établissement, ainsi que les réseaux, messagerie et accès Internet intègrent des dispositifs de traçabilité permettant d'enregistrer :

- L'identifiant de l'utilisateur ayant déclenché l'opération ;
- L'heure de la connexion ;
- Le système auquel il est accédé ;
- Le type d'opération réalisée ;
- Les informations ajoutées, modifiées ou supprimée des bases de données en réseau et/ ou des applications de l'hôpital ;
- La durée de la connexion (notamment pour l'accès Internet).

Le personnel du service informatique respecte la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

7.3 ALERTES

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité ou manquement substantiel à cette charte doit être signalé au Responsable de la Sécurité du Système d'Information.

La sécurité de l'information met en jeu des moyens techniques, organisationnels et humains. Chaque utilisateur de l'information se doit d'avoir une attitude vigilante et responsable afin que les patients bénéficient d'une prise en charge sécurisée et que leur vie privée ainsi que celle du personnel du CHIMB soient respectées.

8. RESPONSABILITES ET SANCTIONS

Les règles définies dans la présente Charte ont été fixées par la Direction du CHIMB dans le respect des dispositions législatives et réglementaires applicables (CNIL, Agence du Numérique en Santé (ANS), ...).

L'établissement ne pourra être tenu pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera pas conformé aux règles d'accès et d'usage des ressources informatiques et des services internet décrites dans la Charte. En cas de manquement aux règles de la présente Charte, la personne responsable de ce manquement est passible de sanctions. Le retrait partiel ou total, temporaire ou définitif des moyens informatiques pourra par ailleurs être mis en œuvre.

Enfin, outre ces sanctions et selon la gravité du manquement, la Direction pourra engager des actions civiles ou pénales.

9. VALIDITE

La présente charte entre en vigueur au 01 septembre 2021 au sein de l'établissement.

10. DISPOSITIONS FINALES

Chaque collaborateur signe une déclaration par laquelle il confirme avoir pris connaissance des règles applicables décrites dans la présente charte. Il s'engage à les respecter.