Charte De Confidentialité et de Sécurité pour les Intervenants Externes au Centre Hospitalier Universitaire de Martinique.

I. Préambule :

Le CHU de Martinique (CHUM) met à la disposition de ses utilisateurs des équipements informatiques (serveurs, PC, logiciels…), des moyens de communication (réseau intersites, liaisons avec des sites distants, messagerie, accès Internet…), ainsi que des données et informations qui sont nécessaires à l'accomplissement de leurs missions.

Chaque utilisateur doit être conscient que l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi, de la sécurité du CHUM et du bon usage.

La présente Charte définit les modalités et conditions générales d'utilisation de ces ressources au CHUM que tout Intervenant Externe doit respecter lorsqu'il intervient dans les locaux du CHUM ou lorsqu'il se connecte en local ou à distance sur des ressources CHUM.

II. A qui s'adresse cette charte :

Toute personne, ne faisant pas partie du personnel du CHUM, intervenant dans le cadre d'un contrat, d'un marché ou d'une convention, dans les locaux ou DATACENTER du CHUM ou se connectant en local ou à distance sur des ressources du CHUM, est soumise à la présente « Charte de Confidentialité et de Sécurité pour les Intervenants Externes au Centre Hospitalier Universitaire de Martinique ». Elle sera mise à disposition lors de l'établissement d'un contrat ou d'une convention avec le CHUM, jointe en tant que document à signer (Voir point IX).

III. Engagements de confidentialité :

Chaque Intervenant Externe est responsable de l'usage qu'il fait des Ressources du CHUM mises à sa disposition dans le cadre de sa mission. Il s'engage à respecter les règles de confidentialité et de sécurité de ces ressources et à prendre toutes précautions utiles afin de préserver la confidentialité et la sécurité des informations et notamment d'empêcher qu'elles soient déformées, endommagées ou communiquées à des personnes non autorisées.

Tout Intervenant Externe s'engage donc à respecter de façon absolue, les obligations ci-dessous.
Pendant l'exécution du contrat :

- Ne prendre aucune copie des documents et supports d'informations confiés, à l'exception de celles nécessaires pour les besoins de l'exécution de sa prestation ;
- Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées dans le contrat ;
- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;
- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat.

En fin de contrat ou d'intervention :

- Procéder à la destruction de tous documents, manuscrits ou informatisés, et fichiers stockant les informations saisies ou utilisées;
- Ou à restituer intégralement les supports d'informations.

IV. Engagements de sécurité :

Chaque Intervenant Externe s'engage à respecter les règles de la sécurité informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquence de perturber le système informatique et/ou nuire à la confidentialité, l'intégrité et la disponibilité des données.

Les codes utilisateurs octroyés sont **nominatifs**. Ils doivent être protégés par des mots de passe respectant la politique de sécurité du CHUM

- 8 caractères minimums (alphanumériques, majuscule, minuscule et caractères spéciaux)
- Changement du Mot de Passe tous les 120 Jours Maximum

Le CHU de Martinique se réserve le droit de forcer leur modification de façon régulière, après avoir informé au préalable les sociétés prestataires ou intervenants concernés.

Chaque société ou Intervenant Externe s'engage à transmettre immédiatement l'information d'une compromission de données, de mot de passe, ou en cas de départ de personnel, afin que le CHU prenne toutes les mesures adéquates pour maintenir son niveau de sécurité (désactivation de comptes, changement de mots de passe, etc.).

Chaque intervention effectuée sur place ou à distance par télémaintenance est réalisée, à la demande du personnel autorisé et identifié. Documentée, elle comporte l'identification de l'intervenant et est adressée au Service Informatique (à l'adresse « interventions@chu-martinique.fr ») et au personnel autorisé.

Toute intervention sur le système (préventive ou curative), effectuée par un Intervenant Externe, et son résultat sont consignés sous forme de rapport précisant l'objet, le cadre de l'intervention et le nom du responsable interne en charge du suivi de la prestation.

V. Conditions d'accès aux ressources informatiques

L'accès au service est toujours préalablement soumis aux Responsables d'Infrastructures (Réseaux et Serveurs) et au Responsable de la Sécurité, garants du respect des règles de sécurité du Système d'Information. Sans approbation de la présente charte aucun accès ne sera autorisé aux intervenants.

Ce droit est INCESSIBLE. Il disparaît dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé cet accès (Fin dc contrat ou fin dc mission…). Quand l'autorisation est donnée à une personne morale, cette dernière s'engage à mettre en œuvre, tous les moyens lui permettant de garantir le respect de cette convention par les personnes mandatées par elle.

Ces autorisations sont strictement dédiées à une ou des ressources nommément désignées et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment sur justificatif du Centre Hospitalier et Universitaire de Martinique et cessent en tout état de cause en même temps que l'activité professionnelle qui les a justifiées.

VI. Intervention dans les locaux de l'établissement :

Chaque Intervenant Externe, présent dans les locaux du CHU de Martinique ou de ses DATACENTER doit prendre connaissance des règles, et devra respecter les obligations suivantes :

- L'accès aux locaux informatiques du CHUM se fait sur présentation d'une pièce d'identité. Si un badge lui est remis, il est responsable de son utilisation. En cas de perte, il doit le signaler à son secrétariat d'attache. Ce badge est à restituer en fin de mission au CHUM.

- La connexion sur le réseau interne du CHU de Martinique, d'un ordinateur portable externe n'est pas autorisée sans l'approbation de la DSI. L'utilisation d'outils embarqués ou l'accès Internet (messagerie, FTP, etc.), via le réseau filaire seront impossibles.

- Un accès Wifi vers Internet pourra être octroyé, sous réserve de respecter les règles de bon usage et après une validation de la DSI.

- Dans l'éventualité d'une obligation absolue d'utiliser un ordinateur personnel connecté au réseau (ce dont les responsables de la DSI seront les seuls juges), l'intervenant s'engage à respecter les règles de bonne pratique : Poste à jour des correctifs de sécurité, disposant

d'un antivirus à jour, etc. Il s'engage à assurer la sécurisation des données du CHUM se trouvant en sa possession.

- Afin de s'assurer que tout périphérique externe (Clef USB, disque externe, etc.) qu'il connectera aux ressources du CHUM sera exempt de tout fichier malveillant, l'intervenant s'engage à faire effectuer une analyse antivirale, préalable, par l'outil de protection Antivirale de l'établissement.

- Si l'intervention s'effectue en dehors des locaux de la DSI, l'intervenant s'engage à ne pas tenter de se connecter sur une prise réseau. Il informera, au préalable de son intervention, le personnel de la DSI sur l'objet, le lieu géographique et le cadre de l'intervention ainsi que le nom du responsable interne en charge du suivi de la prestation.

- Ne pas altérer ou détruire, totalement ou partiellement, des données appartenant à un autre utilisateur ou au CHUM sans son autorisation, ne pas intégrer, par quelque moyen que ce soit, de données malveillantes (virus), de ne pas copier sur des supports médias quelconques tout ou partie de données sans autorisation du personnel du CHUM.

- Ne pas installer des logiciels sur un poste CHUM autre que dans les conditions visées aux licences souscrites par le CHUM, ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, ou saturer les ressources, ne pas modifier les configurations des matériels du CHUM sans autorisation de la DSI du CHUM, ne pas faire de copie de logiciels commerciaux pour quelque usage que ce soit. Toute copie effectuée doit respecter les règles relatives au droit de la propriété intellectuelle.

- Respecter les règles d'utilisation d'Internet, à savoir : ne pas consulter, télécharger, publier, diffuser, distribuer, au moyen des ressources du CHUM, des documents, fichiers, informations, vidéos, images…à caractère violent, pornographique, pédophile, d'incitation à la haine raciale, diffamatoire, illégal ou susceptible de porter atteinte au respect de la personne humaine et de sa dignité, aux bonnes mœurs et à l'ordre public.

VII. Intervention à distance ou par télémaintenance :

Afin de garantir la disponibilité et l'intégrité des données, et des applications, installées sur le Système d'Information Hospitalier du CHU de Martinique, des contrats de maintenance sont signés avec les éditeurs et fournisseurs choisis par l'établissement. Cette maintenance inclut généralement la possibilité d'effectuer des connexions à distance afin de pouvoir intervenir dans les plus brefs délais, si un problème est constaté ou si une mise à jour mineure est à prévoir. Les mises à jour majeures après accord de la DSI pourront se faire en télémaintenance.

Le fournisseur doit assurer la sécurité de sa plateforme d'intervention à distance, de la protection des données et des logiciels. Il doit restreindre les accès logiques des postes d'intervention aux seules personnes autorisées. Il doit être en mesure de déterminer en toute circonstance l'identité de toute personne qui se connecte ou s'est connectée sur sa plateforme et en assurer la traçabilité en vue d'être exploitée en cas de litige ou d'incident. Le fournisseur doit mettre en œuvre des moyens et des procédures conformes aux règles de l'art, pour lutter contre les incidents pouvant affecter la sécurité du Système Informatique Hospitalier du CHUM, ses informations ou la sécurité de l'intervention elle-même.

Les modes de connexions sont définis en concertation avec les sociétés prestataires, en conformité avec les règles en vigueur au sein de l'établissement.
Cela inclura tous types de connexions avec le CHU de Martinique.

Les prises en mains à distance directes sur les postes de travail, via des solutions externes (TeamViewer par exemple), ne sont pas autorisées.

Les codes utilisateurs et les droits nécessaires sont définis en concertation avec les fournisseurs, mais le CHUM reste maître, en dernier ressort, du choix final.

Chaque Intervenant Externe s'engage à respecter les règles de la sécurité informatique et notamment :

- De se connecter à partir d'un poste professionnel bénéficiant d'un antivirus à jour et des mises à jour des patchs correctifs de sécurité.
- S'il s'agit d'un PC portable, contenant des procédures d'intervention par exemple, les données devront être protégées pour éviter toute fuite d'information en cas de vol.
- Les connexions Wifi ne devront être effectuées qu'à partir de bornes sécurisées professionnelles, ou personnelles (dans le cas d'astreintes).
- L'Intervenant Externe doit veiller à ce qu'à l'issue de chaque intervention à distance, les données résiduelles (fichiers temporaires ou zones de mémoire vive) en provenance du CHUM soient effacées de la plateforme.
- En cas de télémaintenance permettant l'accès à distance aux fichiers du CHUM, tout Intervenant Externe s'engage à obtenir l'accord préalable du CHUM avant chaque opération de télémaintenance dont il prendrait l'initiative en précisant l'objet, le cadre de l'intervention et le nom du responsable interne en charge du suivi de la prestation.
- Toute intervention en télémaintenance, sur le système, effectuée par un Intervenant Externe est consignée sous forme de rapport précisant l'objet, le cadre de l'intervention, son résultat et le nom du responsable interne en charge du suivi de la prestation. Ce rapport devra être envoyé automatiquement à l'adresse « interventions@chu-martinique.fr ».

Le CHU de Martinique se réserve le droit de modifier les conditions d'accès, après information préalable des sociétés ou intervenants concernés :

- Comptes verrouillés puis déverrouillés à la demande, après envoi de mail à la DSI expliquant l'objectif et la nature de l'intervention,
- Mise en place d'outils de traçabilité.

VIII. Les contrôles assurés par le CHUM :

En vue d'assurer le bon fonctionnement, la sécurité et la qualité de service des systèmes informatiques, le CHUM met en place des personnes habilitées, qui ont accès aux informations relatives aux utilisateurs (fichiers, courriers électroniques, connexions à Internet…), y compris celles qui sont enregistrées sur le disque dur du poste de travail. Ces personnes sont tenues au secret professionnel. Le CHUM dispose :

- D'outils de contrôle de stockage et d'archivage des données et messages ;
- D'un système de journalisation des connexions, destiné à identifier et enregistrer toutes les connexions ou tentatives de connexion, avec conservation des données ne pouvant excéder un an;
- D'une traçabilité des actions (consultation, création, modification, suppression) sur les systèmes mis en œuvre ;
- De la possibilité de prise de contrôle à distance des postes de travail pour des dépannages et installations en respect de la règlementation.

Le CHUM utilise différents moyens techniques (consultation de la mémoire cache, contrôle des flux, installation de limites d'accès au serveur proxy, utilisation d'un pare-feu) pour procéder à des contrôles d'utilisation, conformes à la présente Charte, des ressources informatiques mises à disposition.

Le CHUM se réserve le droit d'utiliser des logiciels de filtrage afin d'interdire l'accès à certains sites Internet dont le contenu lui semble illicite ou en contradiction avec les objectifs de la présente charte. Le CHUM ne garantit pas que ce filtrage sera totalement efficace, ni exempt de toute interruption, faille ou erreur.

L'Intervenant Externe accepte que le CHUM puisse :

- Avoir connaissance des informations nécessaires à l'administration du réseau (données de volumétrie, incidents, nature du trafic engendré) et puisse prendre toutes mesures urgentes pour stopper la perturbation du service.
- Contrôler a posteriori l'utilisation de sa messagerie en analysant des indications générales de fréquence, de volume, de taille des messages, de format des pièces jointes, sans qu'il y ait contrôle sur le contenu des messages échangés.
- Contrôler a posteriori les données de connexion à Internet ainsi que les sites les plus visités.

IX. Sanctions encourues :

Le non-respect des règles et mesures de sécurité figurant dans la présente Charte, engage la responsabilité de l'Intervenant Externe et de sa société, dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables. Le CHUM rappelle que certains agissements (cas de malveillance avérée, non-respect des différentes Lois relatives à la confidentialité des informations) peuvent engager la responsabilité personnelle civile et/ou pénale de l'Intervenant Externe ou du Responsable de la Société.
Le CHUM pourrait engager des poursuites, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

X. Modalités d'exercice du droit d'accès :

Conformément à la loi "Informatique et Libertés" du 6 Janvier 1978 modifiée en 2004, l'Intervenant Externe comme tout utilisateur bénéficie d'un droit d'accès et de rectification aux informations qui le concernent. S'il souhaite exercer ce droit et obtenir communication des informations le concernant, il suffit d'adresser sa demande au Directeur Général du CHUM (ou la Direction Informatique) dans un délais d'un mois à partir de la date d'intervention concernée. Ces informations lui seront restituées dans un délai minimum d'un mois.

CENTRE HOSPITALIER UNIVERSITAIRE DE MARTINIQUE
Le Directeur Général Adjoint
S.BERNIAC