CHARTE INFORMATIQUE

Remarques préliminaires

A. Résumé

La Charte d'utilisation des moyens informatiques est destinée aux utilisateurs des ressources informatiques mises à disposition par Médecins du Monde. Cette charte définit les règles d'utilisation de ces ressources informatiques auxquelles ces utilisateurs doivent se conformer. Cette charte rappelle les responsabilités de chaque utilisateur et informe les utilisateurs des contrôles mis en place par Médecins du Monde pour garantir la sécurité et l'efficience de ses SI.
Cette charte informatique représente les éléments essentiels de l'utilisation des moyens informatiques, elle peut être complétée par des chartes spécifiques à certains outils, notamment concernant l'usage de l'outil informatique de gestion des données médicales, l'utilisation du Wi-Fi pour les invités ou personnes de passage à Médecins du Monde, etc….
Cette charte sera soumise à la validation des instances représentatives de Médecins du Monde et sera diffusée par la Direction des Ressources Humaines à chacun des utilisateurs de Médecins du Monde.

B. Règles de mise à jour

Ce document doit être revu au minimum annuellement par le Service Informatique. Il doit prendre en compte :

- **les événements internes**, notamment : modifications des missions de Médecins du Monde, évolutions de la structure, évolutions de l'architecture technique ou applicative du système informatique ;
- **les événements externes**, notamment : changements de la législation, évolution de la politique contractuelle, nouvelles menaces ou nouveaux enjeux, nouveau(x) partenaire(s) ;
- **les améliorations identifiées** dans le cadre des processus de contrôle et d'audit mis en œuvre.

C. Enjeux

Les ressources informatiques de Médecins du Monde constituent un outil de travail mis à disposition des utilisateurs afin d'exercer leurs missions confiées par Médecins du Monde. **Le bon usage par les utilisateurs de ces ressources informatiques est essentiel à leur préservation.**
Tout mauvais usage des ressources informatiques peut entraîner des conséquences graves pour Médecins du Monde :

- **La mise en cause de la responsabilité de Médecins du Monde**

En cas d'utilisation illicite ou de dommages provoqués via ses ressources par un de ses salariés ou bénévoles, Médecins du Monde peut être considéré comme responsable et ses dirigeants poursuivis ;

- **La perte de confidentialité**

Une erreur dans le nom du destinataire d'un courriel, la copie d'informations confidentielles sur des ressources non convenablement protégées, ou le vol d'un ordinateur portable et des informations qu'il contient sont quelques-unes des menaces pouvant porter atteinte à la confidentialité des informations de Médecins du Monde ;

- **L'atteinte à l'image et à la réputation de Médecins du Monde**

Un message mal écrit, contenant des propos offensants, illicites ou inappropriés peuvent avoir un impact important sur l'image et la réputation de Médecins du Monde ;

- **La perte d'efficacité**

L'usage inapproprié des ressources comme l'accès à Internet ou la messagerie peut entraîner une perte d'efficacité des utilisateurs (nombre important de messages non pertinents à traiter, introduction d'un virus, saturation ou accès ralenti à Internet et à la messagerie, etc…).

Cette charte vise à renforcer le niveau de sensibilisation et de responsabilité des utilisateurs au bon usage des ressources informatiques mises à leur disposition par Médecins du Monde.

Elle définit, dans le respect des libertés individuelles et collectives :

- les droits et devoirs des utilisateurs en matière d'utilisation des ressources informatiques ;
- le cadre d'usage des ressources à titre professionnel[1] et les conditions associées à l'usage privé ;
- les moyens utilisés par Médecins du Monde pour assurer le contrôle d'accès et d'utilisation des ressources informatiques ;
- la conduite à tenir en cas d'incident lié aux SI.

Cette charte n'a pas pour objectif de couvrir l'exhaustivité des situations possibles. Elle n'a pas vocation à se substituer aux disposions légales et réglementaires. Elle précise les principes d'utilisation attendus des ressources informatiques.

D. Champ d'application

Ce document s'applique à **l'ensemble des utilisateurs des ressources informatiques** mises à disposition par Médecins du Monde.
On entend par **ressources informatiques** l'ensemble des matériels et outils informatiques (logiciels, applications, postes de travail, serveurs, supports de stockage, etc…), les informations quel que soit leur support de stockage et les moyens de communication liés à l'information (téléphone, télécopie, systèmes de messagerie, Internet, Intranet, forums etc…).
On entend par **utilisateurs** tous les acteurs de Médecins du Monde comprenant les salariés de Médecins du Monde (CDI, CDD), les intérimaires, les stagiaires, les prestataires externes ainsi que les bénévoles, les membres et les élus de Médecins du Monde.
Ce document ne s'applique pas aux bénéficiaires et usagers des services fournis par Médecins du Monde.

E. Responsabilités

Chaque utilisateur est responsable des ressources informatiques qu'il utilise et doit en assurer, à son niveau, la protection afin qu'elles demeurent disponibles, sécurisées et performantes. **Chaque utilisateur s'engage à respecter les principes et règles détaillés dans cette charte.**
Les responsables hiérarchiques, les responsables de structures et les délégués régionaux doivent s'assurer de la connaissance et de l'application de cette charte dans leur périmètre. Ils doivent relayer cette charte et son contenu auprès des utilisateurs dans leur périmètre de responsabilité.
La charte est diffusée en annexe du contrat de travail ou de stage Médecins du Monde, afin que chaque utilisateur en ait connaissance. Elle est annexée aux contrats de prestation et de partenariat impliquant l'utilisation des ressources informatiques de Médecins du Monde. La charte du bénévole et des membres de Médecins du Monde fait référence à la charte, laquelle est mise à la disposition des bénévoles via l'Intranet.

[1] Dans ce document, on entend par usage professionnel, l'ensemble des activités des salariés, bénévoles, stagiaires, membres associatifs et prestataires exercées au nom et pour le compte de Médecins du Monde.

Droits et devoirs

1. CONDITIONS GENERALES

1.1 Autorisation d'accès

L'accès aux ressources informatiques de Médecins du Monde par un utilisateur est soumis à l'approbation de son responsable hiérarchique pour les salariés, de son délégué régional ou de son responsable d'activité pour les bénévoles ou du responsable de la mission confiée à un prestataire externe, du référent du stagiaire pour un stagiaire.

1.2 Usage professionnel et privé

Les ressources informatiques de Médecins du Monde sont mises à la disposition des utilisateurs pour exercer leurs missions confiées par Médecins du Monde.
Un usage privé raisonnable des ressources de Médecins du Monde est toléré lorsqu'il s'inscrit dans le cadre des nécessités de la vie courante, et à condition que cet usage ne constitue pas une entrave à l'usage professionnel. L'utilisation à des fins privées des ressources informatiques mises à disposition par Médecins du Monde conduit l'utilisateur à assumer l'entière responsabilité pénale et civile de l'utilisation qu'il fera des ressources informatiques à des fins privées.
Les informations à usage privé doivent être marquées de manière explicite et non ambiguë par la dénomination **«usage personnel**» ou similaire ; les informations à usage privé doivent être stockées dans des espaces physiques ou virtuels nommés «usage personnel» ou similaire ; tout message à usage privé doit comporter la mention « usage personnel» ou similaire dans son objet ou être classé dans des dossiers nommés «usage personnel».
Toute autre information sera considérée comme une information professionnelle.

1.3 Respect du cadre législatif national : informations proscrites ou contraires à la morale

Il est **strictement interdit** de stocker, émettre ou faire suivre sciemment des informations contraires à la morale et/ou proscrites par les lois en vigueur, sauf à ce que ces informations aient un lien direct avec la fonction et qu'elles ne soient pas contraires à l'ordre public, notamment des informations :

- à caractère violent, pornographiques ou susceptibles de porter atteinte à la dignité, à l'honneur ou à l'intégrité de la personne humaine, ainsi qu'à la protection des mineurs ;
- susceptibles d'encourager à la commission de crimes et délits, d'inciter à la consommation de substances illicites, à la discrimination, à la haine, ou à la violence ;
- faisant l'apologie des crimes contre l'humanité ou du terrorisme ;
- constitutives de harcèlements quels qu'ils soient ;
- à caractère diffamatoire, injurieux, vulgaire, obscène, menaçant pour la vie privée d'autrui ;
- violant les règles et la législation en vigueur sur la propriété intellectuelle : il est interdit à tout utilisateur de copier ou d'utiliser illicitement des logiciels ou informations protégés par une licence, des droits d'auteurs ou tout droit de propriété.

1.4 Protection des données à caractère personnel

Conformément à la loi 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, la création, le traitement, le stockage et la diffusion de données à caractère personnel doivent être soumis préalablement à toute exploitation au Correspondant

Informatique et Liberté CIL de Médecins du Monde. Ces déclarations sont gérées exclusivement par le CIL au sein du Service Juridique de Médecins du Monde : juridique@medecinsdumonde.net/blandine.contamin@medecinsdumonde.net

1.5 Respect des législations étrangères

Les logiciels installés sur le poste de travail répondent au cadre d'utilisation fixée par la législation française. L'utilisateur veille à prendre toutes les précautions utiles en cas de déplacement à l'étranger sur les droits d'utilisation des logiciels. Ces précautions concernent plus particulièrement l'usage des outils de chiffrement ou de signature électronique qui peut être réglementé dans des pays étrangers. Elles concernent également la navigation sur Internet, filtrée dans certains pays. Il convient donc de se renseigner au préalable auprès du référent sécurité et/ou du conseil juridique disponible.

2. PROTECTION DES EQUIPEMENTS

L'utilisateur est responsable de la protection des équipements mis à sa disposition par Médecins du Monde.

2.1 Equipements validés

Seuls les équipements fournis ou validés par le Service Informatique ou le support informatique de proximité peuvent être installés et connectés aux réseaux internes et postes de travail informatiques de Médecins du Monde.
Dans ce document, on entend par support informatique de proximité :
- pour les utilisateurs du siège : le support informatique du Service Informatique ;
- pour les utilisateurs en région où à l'international les personnes en charge de la maintenance des postes informatiques dans la structure.

2.2 Modification de la configuration

Afin de maintenir un niveau de sécurité approprié, l'utilisateur ne doit jamais modifier la configuration de son poste de travail informatique et des autres équipements mis à sa disposition par Médecins du Monde.
En particulier, l'utilisateur ne doit pas :

- ajouter ou retirer un composant matériel (disque dur, carte réseau, etc.) non conforme aux directives du Service Informatique ou du support de proximité de Médecins du Monde ;
- désinstaller ou désactiver les logiciels et mécanismes de sécurité (logiciel antipollution, pare-feu, paramétrage des mots de passe, installation des correctifs de sécurité etc…) ;
- télécharger et installer des logiciels non validés par Médecins du Monde. L'installation de tout logiciel non validé doit faire l'objet d'une demande au support informatique de proximité. Celui-ci validera ou fera valider le composant logiciel (licences, impacts techniques sur la configuration, maintenance et support etc….) et l'installera ou le fera installer ;

En cas de possession d'un ordinateur portable fourni par Médecins du Monde, l'utilisateur doit se connecter régulièrement au réseau informatique de Médecins du Monde pour assurer la mise à jour régulière des dispositifs de sécurité du poste. Il est à noter que les ordinateurs portables mis à disposition par Médecins du Monde ne peuvent être utilisés par des personnes externes à Médecins du Monde.

2.3 Protection physique

Afin de limiter le risque de vol ou de perte des équipements mis à sa disposition, l'utilisateur veille en particulier à :

- utiliser les moyens de protection mis à disposition pour garantir la protection des équipements « mobiles » (ordinateurs portables, assistants personnels, téléphones portables, etc.) et de leurs accessoires (clé USB,

disque dur externe, batteries etc …) : rangement dans un tiroir ou une armoire fermant à clé, utilisation d'un câble antivol etc … ;

- ne pas laisser ses équipements sans surveillance dans des lieux dont l'accès n'est pas contrôlé : l'utilisateur fait preuve d'une vigilance particulière dans les lieux publics et les transports en commun.

.3. PROTECTION DES INFORMATIONS

L'utilisateur a la responsabilité de protéger les informations stockées sur les ressources informatiques mises à sa disposition (disque dur interne, ordinateur portable, disque dur externe, clé USB, CD ou DVD, etc…). Il doit faire preuve de discernement et respecter les règles de classification et de protection des informations établies par Médecins du Monde.

3.1 Droits d'accès

Les habilitations (compte et mot de passe) aux Systèmes d'Information (SI) de Médecins du Monde attribuées à chaque utilisateur sont strictement personnelles et ne peuvent pas être cédées, temporairement ou non, à un tiers même à ses responsables (sauf dans la situation particulière décrite dans le paragraphe).

L'utilisateur doit prendre toutes les mesures nécessaires pour limiter les accès frauduleux aux moyens informatiques, et à ce titre il doit notamment :

- veiller à la confidentialité des comptes utilisateurs ainsi que des codes, mots de passe, cartes, clé ou tout autre dispositif de contrôle d'accès qui lui sont confiés à titre strictement personnel, en particulier en n'affichant pas ses mots de passe. Le mot de passe choisi par l'utilisateur doit obligatoirement comporter au moins 10 caractères et de types différents (chiffre et lettre) et être mis à jour tous les 6 mois. Un rappel automatique de mise à jour sera adressé dans ce sens à chaque utilisateur et une assistance par le Service Informatique est disponible.
- ne pas prêter, vendre ou céder les comptes utilisateurs, codes et autres dispositifs de contrôle d'accès ou en faire bénéficier un tiers ;
- verrouiller ou fermer toutes les sessions en cours sur son poste de travail informatique en cas d'absence, même momentanée ;
- s'assurer que les fichiers qu'il juge confidentiels ne soient pas accessibles à des tiers.

L'accès au poste de travail s'effectue à partir des seuls éléments d'identification et d'authentification communiqués par Médecins du Monde.

L'utilisateur ne doit pas utiliser ou tenter d'utiliser des ressources informatiques pour lesquelles il n'a pas reçu de droits d'accès. Les utilisateurs ne doivent pas utiliser une fausse identité ou masquer leur véritable identité.

3.2 Protection des documents

L'utilisateur doit favoriser tous les comportements visant à assurer le niveau de sécurité correspondant à la sensibilité des informations et des ressources utilisées et, en particulier :

- dans le cadre de l'utilisation de supports amovibles (disque dur, clé USB etc…) et des équipements nomades (ordinateur portable, téléphone mobile, etc…), les protéger physiquement (coffre) ou utiliser les dispositifs de chiffrement des données sensibles stockées sur ces supports ;
- faire des sauvegardes régulières de ses données locales sur son poste de travail ; ces sauvegardes doivent elles-mêmes respecter les règles permettant d'assurer la confidentialité des données concernées ;
- détruire les données qui ne sont plus nécessaires ;
- vider régulièrement la corbeille virtuelle et les répertoires temporaires du poste de travail : corbeille du poste de travail, historique de navigation Internet, Cookies Internet etc …
- gérer les impressions selon leur sensibilité et récupérer les documents sensibles sur les imprimantes, fax et copieurs.

.4. UTILISATION DES MOYENS DE COMMUNICATIONS

Les contenus fournis via Internet sont rarement garantis quant à leur qualité, leur statut légal ou leur droit d'usage à titre professionnel. L'utilisateur doit faire preuve de la plus grande vigilance pour ce qui concerne la confidentialité, l'intégrité et la fiabilité des éléments envoyés, reçus ou consultés sur Internet.

4.1 Conditions d'accès

L'accès aux moyens de communication électroniques depuis le réseau interne de Médecins du Monde s'effectue exclusivement avec les moyens mis à disposition par Médecins du Monde. La connexion de tout autre moyen d'accès externe (tel que, point d'accès Wi-Fi, passerelle de réseau extérieur etc…) sur le réseau interne de Médecins du Monde est interdite.
Les accès à Internet et à la messagerie requièrent une authentification de l'utilisateur. Les moyens d'authentification (mot de passe, code confidentiel etc…) **sont strictement personnels** et l'utilisateur est responsable de leur confidentialité.

4.2 Messagerie électronique

Comme précisé dans la partie «Usage professionnel et privé», les messages à titre privé doivent être explicitement distincts. Un message sera considéré à usage personnel :

- si son objet contient la mention «**usage personnel**»
- ou s'il est stocké dans un répertoire physique ou virtuel nommé «**usage personnel**»

L'appréciation du caractère «usage personnel» d'un message relève de la responsabilité de l'utilisateur.
Lors de l'envoi d'un message «usage personnel», l'utilisateur doit s'assurer que le contenu du message ne peut induire en erreur le destinataire sur la nature personnelle de la communication. L'utilisateur ne devra pas utiliser sa signature professionnelle. Pour rappel, les salariés veilleront au contenu afin de respecter leur obligation de loyauté envers leur employeur.
Il est rappelé que pour les messages non sécurisés par des moyens de chiffrement spécifiques, la sécurité offerte par la messagerie électronique sur Internet est comparable à celui de l'envoi d'une carte postale. Tout le monde peut la lire et son délai d'acheminement, pas plus que sa réception, ne sont garantis.
L'émetteur d'un message professionnel doit donc faire preuve de discernement et protéger les informations non publiques envoyées par messagerie en se référant aux règles de classification et de protection établies par Médecins du Monde.
Par ailleurs, l'utilisateur ne doit pas :

- envoyer des messages dont le contenu peut porter atteinte à l'image ou à la réputation de Médecins du Monde, en particulier lors d'échanges avec les partenaires ou les donateurs;
- envoyer ou faire suivre des messages non sollicités (spams ou pourriels[2]), de messages contenant des informations illicites ou offensantes, ou encore de messages de type « chaînes » ;
- mettre en œuvre, sans validation par Médecins du Monde, des fonctions d'envoi ou de redirection automatique des messages lui étant destinés vers une adresse de messagerie externe à Médecins du Monde;
- modifier un message émanant d'un tiers sans l'indiquer avant de le rediffuser ;
- prendre connaissance d'informations pour lesquelles il ne bénéficie pas du droit d'accès.

Ces dispositions s'appliquent plus particulièrement aux courriers électroniques dont l'utilisateur n'est ni destinataire directement, ni en copie.
L'envoi de messages à l'ensemble des utilisateurs de Médecins du Monde ou d'une structure est en principe interdit, sauf autorisation expresse. La procédure d'autorisation doit être définie dans le cadre du règlement de chaque structure.

[2] Le spam ou pourriel, désigne une communication électronique, notamment du courrier électronique non sollicité par les destinataires, expédié en masse à des fins publicitaires ou malhonnêtes.

L'utilisateur fait preuve de vigilance à l'égard des messages qu'il reçoit. A ce titre, l'utilisateur ne doit pas :

- ouvrir les messages dont l'origine, l'objet ou le contenu est douteux ;
- enregistrer et exécuter les pièces jointes suspectes ;
- prendre de décision importante à la seule vue d'un message électronique. En cas de doute, il contacte l'émetteur du message ou à défaut le support informatique de proximité pour s'assurer de l'authenticité et de la véracité des informations reçues.

L'inscription sur des listes de diffusion externes d'une adresse de messagerie Médecins de Monde est réservée à un usage strictement professionnel. Lors de l'inscription, l'utilisateur doit systématiquement vérifier qu'il existe une procédure de désabonnement.

4.3 Navigation

Un usage raisonnable de l'accès à Internet est admis lorsqu'il s'inscrit dans le cadre des nécessités de la vie courante, et à condition que cet usage ne constitue pas une entrave à l'usage professionnel.

L'utilisateur doit exercer une vigilance toute particulière lors de la navigation sur Internet ; il lui est notamment interdit de :

- visualiser, télécharger, transmettre ou conserver des contenus illicites ou attentatoires à l'image de Médecins du Monde ; en cas d'accès accidentel à un site Internet illégal ou non autorisé par Médecins du Monde, l'utilisateur doit se déconnecter immédiatement de ce site ;
- communiquer son identifiant personnel sur des sites Internet consultés ;
- communiquer ses coordonnées, en particulier son adresse électronique, sur des sites sans rapport avec son activité professionnelle ou dont l'image est incompatible avec celle de Médecins du Monde.

Toute ouverture d'un outil de communication en ligne (forum professionnel ou d'une communauté ou d'un site internet) par un utilisateur en tant que représentant de Médecins du Monde ou d'une de ses entités nécessite l'autorisation de sa direction ainsi que la consultation préalable de la Direction de la Communication et du Développement et du Service Juridique de Médecins du Monde.

La participation à des forums, blogs, groupes de discussions ou à des réseaux sociaux à titre professionnel, en tant que représentant de Médecins du Monde est subordonnée aux mêmes conditions.

Lors de l'utilisation de ces outils de communication en ligne, l'utilisateur veillera, en tant que représentant de Médecins du Monde, à respecter le droit de la presse, le secret professionnel, le respect de la vie privée, notamment en cas de publication de photo, et respectera les orientations et consignes internes de Médecins du Monde.

Il est rappelé toutefois qu'il agit au nom de Médecins du Monde et qu'il doit veiller, à ce titre, à ne pas porter atteinte aux intérêts de cette dernière. Il lui appartient en cas de doute de consulter préalablement la Direction de la Communication de Médecins du Monde.

Dans le cadre de l'usage de messagerie instantanée à titre privé ou de la participation à des forums, blogs, groupes de discussion ou à des réseaux sociaux à titre privé, l'utilisateur aura recours obligatoirement à une adresse de messagerie privée. Il veillera à ce que le contenu des messages ne permette aucune confusion laissant à penser qu'il s'exprime au nom de Médecins du Monde ou que le message est rédigé dans le cadre de l'exercice de ses fonctions. En particulier, il n'utilisera pas les emblèmes et logos de Médecins du Monde. Cette disposition ne libère pas l'utilisateur de son devoir de réserve et de discrétion.

4.4 Utilisation de son propre matériel

La messagerie peut être installée sur le téléphone portable personnel ou l'ordinateur personnel d'un utilisateur. Médecins du Monde ne saurait néanmoins être tenue responsable de dégâts sur le matériel résultant d'un tel usage. Le Service Informatique de Médecins du Monde n'a aucune obligation de fournir

une aide sur le matériel personnel. Dans le cas où le service informatique serait amené à intervenir il ne saurait être tenu responsable d'éventuels dégâts résultant de cette intervention.
L'acceptation de l'installation de la messagerie sur certains téléphones portables peut donner l'accès au Service Informatique au contenu du téléphone à des fins de suppression de données de Médecins du Monde en cas de suppression de compte. Un message demandant une validation de l'utilisateur est dans ce cas affiché lors du paramétrage du compte sur le téléphone.

5. CONTROLES ET COLLECTE D'INFORMATIONS

Afin de garantir le bon fonctionnement technique et la sécurité de ses Systèmes d'Information, et de préserver ses intérêts, Médecins du Monde se réserve le droit de limiter, d'analyser et de contrôler les traces d'utilisation des ressources matérielles et logicielles, ainsi que des échanges, quels que soient leur nature ou leur objet, effectués via ses Systèmes d'Information.
Dans ce cadre, Médecins du Monde utilise notamment des journaux conservant les traces de certaines actions des utilisateurs.

Les actions de contrôle et d'analyse mises en œuvre par Médecins du Monde sont réalisées en cas de détection d'un comportement anormal ou dans les cas spécifiques prévus par la loi. Elles n'ont pas vocation à surveiller de façon systématique l'activité de chaque utilisateur.
Ces actions de contrôle et d'analyse sont réalisées exclusivement par les administrateurs informatiques dans le respect de la législation applicable, et notamment de la loi « Informatique et Libertés ». Les administrateurs informatiques sont tenus à la confidentialité des informations qu'ils pourraient être amenés à connaître à cette occasion.

6. FILTRAGE ET RESTRICTIONS

Des moyens techniques de filtrage des accès à Internet restreignent les possibilités de navigation sur Internet. Les principes de Médecins du Monde ainsi que le cadre réglementaire guident les restrictions fixées. La mise en œuvre de ces filtres ne dégage pas l'utilisateur de ses responsabilités
La messagerie est soumise à des restrictions techniques qui portent sur les volumes des fichiers transmis ou sur les extensions de certains fichiers.
L'accès à Internet et à la messagerie sont soumis aux contrôles antivirus qui peuvent, par mesure de sécurité, restreindre l'accès à un site, supprimer des pièces jointes ou vider des messages de leur contenu.
Ces dispositions sont indispensables à la sécurité des accès externes. Médecins du Monde ne pourra être tenu pour responsable de la perte des données suite à ces contrôles ainsi que des conséquences qui s'en suivent.

7. DISPOSITIFS DE CONTROLE

7.1 Dispositifs spécifiques à la messagerie électronique

Les informations enregistrées dans les journaux pour chaque message électronique sont :

- émetteur du message ;
- destinataire du message ;
- date et heure de traitement du message.

➔ **La durée de conservation des journaux est de 90 jours.**
Médecins du Monde procède à la lecture de l'enveloppe de certains messages (date, heure, émetteur, destinataire, objet, etc.). Si l'objet du message n'est pas marqué comme étant un message à usage personnel, et en cas de non-respect par l'utilisateur des dispositions générales présentées au chapitre 4.1, le contenu du message pourra être consulté.

7.2 Dispositifs spécifiques à l'utilisation d'Internet

Les informations enregistrées dans les journaux pour chaque accès à Internet sont :

- adresse des sites consultés (URL).
- identifiant utilisé pour la connexion qui pourra aussi être conservé.
- type de flux (HTTP, FTP …).
- volume des données reçues et transmises.

➔ **La durée de conservation des journaux est de 30 jours.**

Médecins du Monde s'interdit toute utilisation de ces informations pour un contrôle des sites Internet consultés par les représentants du personnel et les représentants syndicaux dans le cadre des activités liées à leur mandat.

7.3 Dispositifs spécifiques à l'accès aux ressources partagées

Les informations enregistrées dans les journaux pour chaque accès aux ressources partagées (lecteurs réseaux) sont :

- date et heure de la connexion.
- identifiant utilisé pour la connexion.
- profil associé à la connexion (privilèges attribués).

➔**La durée de conservation des journaux est de trois mois maximum.**

Il pourra être procédé à la lecture du contenu des fichiers non personnels. Dans ce cas, Médecins du Monde pourra informer par écrit l'utilisateur dont les données ont été consultées.

7.4 Dispositifs spécifiques aux postes de travail

Les informations enregistrées dans les journaux au niveau des postes de travail sont :

- détail des connexions sur le poste de travail : identifiant des connexions réussies et refusées ;
- détail des « erreurs système » recensées sur les postes de travail ;
- détail des incidents recensés par les logiciels antipollution sur le poste de travail ;
- détail des incidents recensés par le pare-feu personnel, pour les postes de travail qui en sont munis : flux bloqués, non-conformités détectées, etc.

➔ **La durée de conservation des journaux est de trois mois maximum.**

Il pourra être procédé à la lecture du contenu des fichiers non personnels. Dans ce cas, Médecins du Monde pourra informer par écrit l'utilisateur dont les données ont été consultées.

7.5 Dispositifs spécifiques à l'accès distant aux SI

Les informations enregistrées dans les journaux pour chaque connexion aux Systèmes d'Information de Médecins du Monde depuis l'extérieur sont :

- date et heure de début et de fin de connexion.
- identifiant utilisé pour la connexion.

➔ **La durée de conservation des journaux est de six mois maximum.**

7.6 Dispositifs spécifiques aux applications à accès contrôlé

Les informations enregistrées dans les journaux au niveau des applications dépendent des exigences légales et réglementaires s'appliquant à chaque application.

Par défaut, les informations suivantes sont enregistrées :

- identification de l'utilisateur, et le cas échéant son profil d'accès.
- date et heure de la connexion.

➔**La durée de conservation des journaux est par défaut de trois mois.**

Pour les applications n'implémentant pas ces règles par défaut, le détail des informations enregistrées, leur finalité et la durée de conservation des journaux seront communiqués aux utilisateurs de l'application.

7.7 Dispositifs spécifiques à la téléphonie fixe

Les informations enregistrées dans les journaux au niveau des infrastructures téléphoniques internes (autocommutateur téléphonique, téléphonie sur IP) ou transmises par l'opérateur auprès duquel Médecins du Monde est cliente sont :

- numéro de téléphone appelé [3], service utilisé, opérateur appelé, destination de l'appel (appel local, départemental, national, international, numéro surtaxé).
- durée, date et heure de début et de fin de l'appel, éléments de facturation (nombre de taxes, volume et nature des données échangées à l'exclusion du contenu de celles-ci et coût du service utilisé).

➔ **La durée de conservation est d'un an maximum courant à la date de l'exigibilité des sommes dues en paiement des prestations de services téléphoniques.**

La liste détaillée des communications établies à partir d'un poste particulier peut être éditée. Une telle liste ne peut être fournie que sur demande explicite et motivée (utilisation manifestement anormale du téléphone) du responsable hiérarchique ou du contrôle de gestion en cas de dépenses anormales, de structure ou de mission de l'intéressé. Ce dernier devra pouvoir avoir accès à cette liste et fournir ses explications à son responsable.

Médecins du Monde s'interdit tout usage des informations issues de l'utilisation des services de téléphonie pour un contrôle des appels émis et reçus par les représentants du personnel et les représentants syndicaux dans le cadre de leur mandat.

7.8 Accès aux postes de travail, aux fichiers, et à la messagerie de l'utilisateur

Absence de l'utilisateur

En cas de refus ou d'incapacité d'un utilisateur à communiquer des informations nécessaires à la poursuite de l'activité de Médecins du Monde, et si ces informations ne sont pas accessibles par d'autres moyens, ses responsables hiérarchiques, de structure ou de mission peuvent demander au support informatique de proximité l'accès aux ressources nécessaires à la poursuite de l'activité de Médecins du Monde. **Ces demandes à caractère exceptionnel doivent être argumentées et formalisées par le demandeur auprès de la Direction des Ressources Humaines qui transmettra la demande au Service Informatique après consultation des Délégués du personnel. Dans le cadre d'un poste des RH la demande doit être faite auprès de la Direction Générale.**

Dans ce cas, Médecins du Monde s'interdit d'accéder aux informations à usage personnel de l'utilisateur, telles que définies aux présentes

Départ de l'utilisateur

Lors du départ, quelle qu'en soit la cause, d'un utilisateur de Médecins du Monde, les modalités de fermeture de ses comptes sont les suivantes :

- le responsable hiérarchique, de structure ou de mission de l'utilisateur demande au support informatique de proximité la fermeture des comptes de l'utilisateur en indiquant la date souhaitée de fermeture (un délai indicatif a été défini dans la note de gestion des adresses de messageries, cf. annexe A) ;
- le responsable de l'utilisateur communique cette date de fermeture des comptes à l'utilisateur ;

le responsable hiérarchique, de structure ou de mission peut demander à l'utilisateur de lui communiquer avant son départ les informations en sa possession qui sont nécessaires à la poursuite de l'activité de Médecins du Monde. En cas de refus ou d'incapacité de l'utilisateur de communiquer ces informations, et à condition que ces informations ne puissent être accédées par d'autres moyens, le responsable hiérarchique, de structure ou de mission peut demander au support informatique de proximité la mise à disposition de ces informations après son départ.

[3] Les numéros appelés y sont tronqués de leurs quatre derniers chiffres.

Ces demandes à caractère exceptionnel doivent être argumentées et formalisées par le demandeur auprès de la Direction des Ressources Humaines qui transmettra la demande au Service Informatique après consultation des Délégués du personnel. Dans le cadre d'un poste des RH la demande doit être faite auprès de la Direction Générale.

Dans ce cas, Médecins du Monde s'interdit d'accéder aux informations à usage personnel de l'utilisateur, telles que définies dans le paragraphe. Il est cependant recommandé à l'utilisateur de supprimer ses informations personnelles avant la date de fermeture de ses comptes. Le compte sera désactivé et ensuite supprimé après récupération des documents et messages électroniques.

Accès aux informations à usage personnel

Médecins du Monde se réserve le droit d'autoriser l'accès aux informations à usage personnel en cas :

- de péril imminent menaçant les intérêts de Médecins du Monde et qualifiable d'état de nécessité ;
- de demandes qualifiées des autorités compétentes de la justice ou de la police et avec l'accord du Service Juridique du siège de Médecins du Monde.

L'accès à ces informations se fera dans le principe de proportionnalité et dans le respect des lois, en particulier dans le respect du secret des correspondances et de la vie privée.

Hormis ces cas, tout accès au contenu d'un fichier, d'un répertoire ou d'un message explicitement marqué comme à usage personnel devra être effectué en présence de l'utilisateur ou après l'avoir invité à être présent.

.8. BLOCAGE DES ACCES

Dans le cas d'utilisations illégales ou non autorisées ou remettant en cause le bon fonctionnement des Systèmes d'Information, la sécurité des Systèmes d'Information ou les intérêts de Médecins du Monde, le Service Informatique ou le support informatique de proximité pourra mettre en œuvre les actions de protection adaptées et/ou de correction nécessaires jusqu'au retour à la normale, et informer la hiérarchie.

Les habilitations de l'utilisateur aux ressources informatiques peuvent être modifiées ou retirées à tout moment par Médecins du Monde.

Par mesures techniques ou administratives, les accès à Internet et à la messagerie pourront être suspendus, restreints ou supprimés, individuellement ou collectivement quand cela sera nécessaire, notamment pour le maintien de la bonne marche ou de l'intégrité des Systèmes d'Information de Médecins du Monde.

Ces dispositions pourront être prises sans information préalable des utilisateurs. Comportement en cas d'incident.

.9. VOL OU PERTE D'UNE RESSOURCE

En cas de vol ou perte d'équipements informatiques (poste de travail, support amovible etc…) fournis par Médecins du Monde, l'utilisateur doit :

- informer son responsable hiérarchique, de structure ou de mission et le support informatique de proximité et leur communiquer :
  - les circonstances de la perte ou du vol, pour permettre à Médecins du Monde de décider de l'opportunité de porter plainte au nom de Médecins du Monde ; l'utilisateur ne doit pas porter plainte en son nom ; seule une personne habilitée peut porter plainte au nom de Médecins du Monde ;
  - l'inventaire des données qui étaient présentes sur le matériel avec leur niveau de sensibilité et leur niveau de protection au moment de la perte ou du vol ;
- le support informatique de proximité communiquera ces informations au Service Informatique du siège et au CIL au sein du Service Juridique du siège.

.10. INFECTION OU INTRUSION SUR LE POSTE DE TRAVAIL

En cas de suspicion ou de constatation d'événements pouvant porter atteinte à la sécurité des Systèmes d'Information de Médecins du Monde (par exemple, une intrusion ou une infection par un code malicieux sur le poste de travail ou sur des ressources informatiques), l'utilisateur ne doit pas tenter de résoudre lui-même l'incident.

L'utilisateur doit :

- isoler le matériel en le déconnectant de tout réseau et en particulier de celui Médecins du Monde ;
- prévenir le support informatique de proximité qui prendra les dispositions nécessaires pour confiner et traiter l'incident.

Une infection par un code malicieux (virus, vers, spywares, chevaux de Troie, bombes logiques, etc…) ou une intrusion sur le poste de travail peut se traduire par un comportement anormal du matériel ou des alertes des dispositifs de sécurité (logiciel antipollution, pare-feu personnel etc…).

Le CIL au sein du Service Juridique doit être informé par le Service Informatique de toute faille ayant mis en danger la protection des données personnelles de Médecins du Monde.

.11. DYSFONCTIONNEMENT DE L'EQUIPEMENT

En cas de dysfonctionnement du matériel ou de non-respect des exigences précitées, une reconfiguration du système pourra être décidée.

Le cas échéant :

- le support informatique de proximité réinitialisera l'équipement avec sa configuration initiale standard,
- le support informatique de proximité ne restaurera pas les données marquées «usage personnel» ; Médecins du Monde ne pourra être tenue pour responsable de la perte ou de l'altération des données marquées «usage personnel» ainsi que des conséquences qui s'en suivent.

ANNEXE A

Délais de suppression des adresses de messagerie après départ d'un utilisateur

Ces délais sont extraits de la note « Processus de création suppression d'adresses de messagerie v1.0 » de décembre 2013.

- pour les stagiaires, bénévoles : à la date de fin du contrat ;
- pour les salariés : 1 mois après la fin du contrat ;
- pour les responsables de missions, responsables de groupe, délégués régionaux, secrétaires régionaux et trésoriers régionaux : 3 mois à compter de l'enregistrement par le CA de la démission/fin du mandat de la personne ;
- pour les administrateurs : 12 mois à compter de la fin de leur mandat ;
- pour les membres du Bureau : 24 mois à compter de la fin de leur mandat ;
- pour les anciens présidents : 36 mois à compter de la fin de leur mandat.