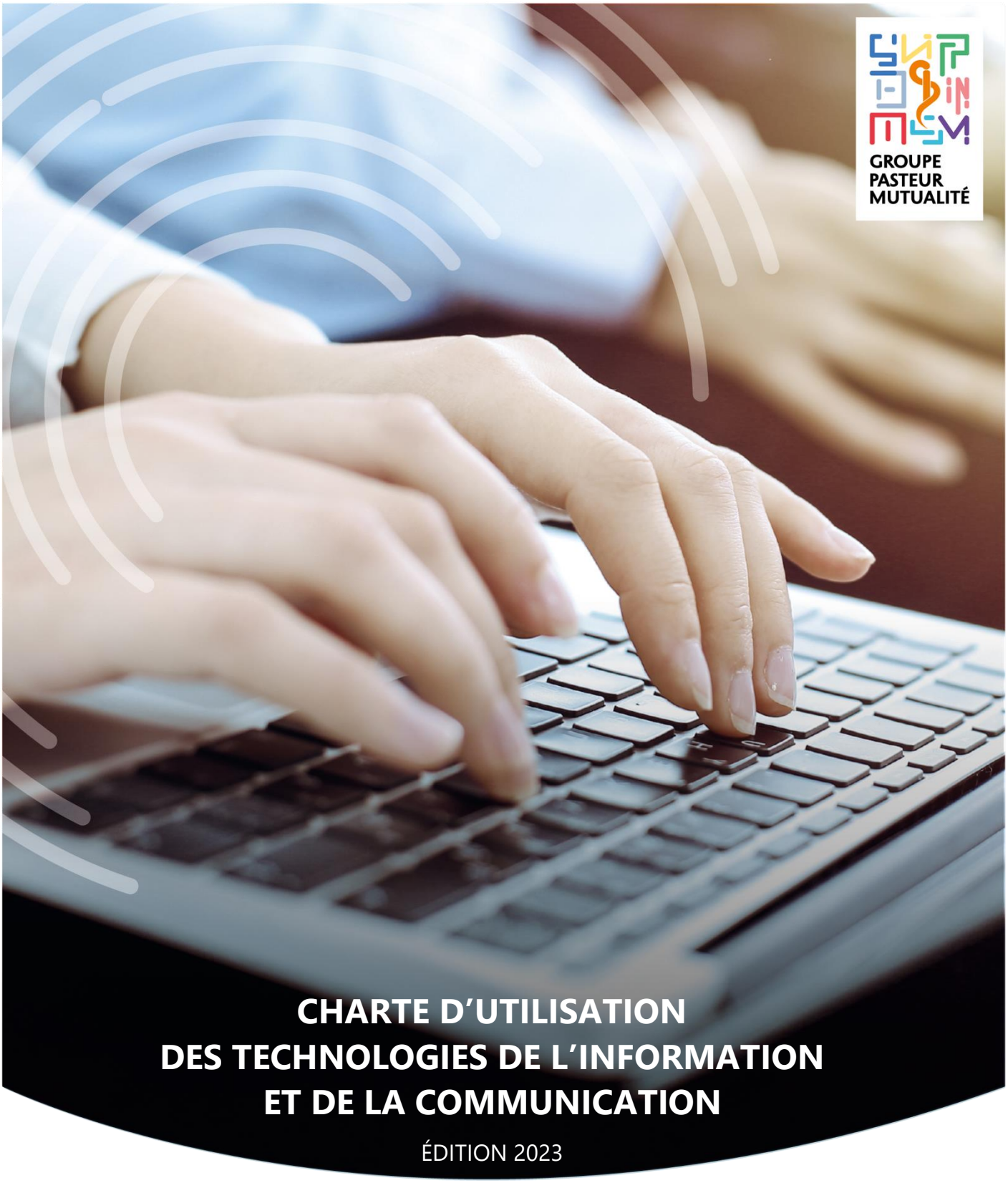

CHARTE D'UTILISATION DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

ÉDITION 2023

REDACTEUR : PALOMA GOUIN I RESPONSABLE SECURITE DES SYSTEMES D'INFORMATION GROUPE

DATE DE MISE EN VIGUEUR : 25 MAI 2023

Table des matières

Préambule

L'essor des réseaux d'information et de communication contribuent favorablement à l'exercice de l'activité professionnelle des utilisateurs de Groupe Pasteur Mutualité, à travers de nouveaux usages et réflexions : mobilité, consommation de données dans le nuage « cloud », protection des données personnelles et responsabilité numérique.

Il en importe néanmoins de souligner les risques liés au numérique et à la cybersécurité, inhérents à l'utilisation de ces ressources, dont l'impact serait majeur pour les entités de Groupe Pasteur Mutualité. L'anticipation et la protection des données d'entreprise sont alors essentielles et nécessitent, de fait, un encadrement de ces utilisations pour en réduire l'impact en cas de malveillance ou de mauvais usage de ces outils.

C'est dans ce contexte que la finalité principale, identifiée par la charte d'utilisation des technologies de l'information et de communication, est de contribuer à la préservation du patrimoine informationnel de Groupe Pasteur Mutualité et fait de l'utilisateur un acteur responsable, au cœur de la réalisation de cet objectif.

Aussi, la présente charte visera trois piliers fondamentaux :

- sensibiliser l'ensemble des parties prenantes aux risques liés au numérique et à la cybersécurité ainsi qu'aux principales mesures mises en œuvre pour s'en protéger ;
- informer les utilisateurs de leurs droits et obligations dans le cadre d'une utilisation professionnelle des outils de communication et d'information de l'entreprise ;
- porter à la connaissance de chacun, dans un esprit de loyauté et de transparence, les moyens utilisés pour assurer la sécurité, le contrôle de l'accès, l'utilisation des ressources des systèmes d'information, mais plus généralement, de préserver les intérêts légitimes de l'organisation.

Les manquements aux règles qui seront présentées par la suite, pourront être sanctionnés dans les conditions prévues, à cet effet, par le règlement intérieur.

1. Définitions

On désignera sous le terme **GPM**, toute entité de Groupe Pasteur Mutualité affiliée ou non au GIE GPM et incluse dans le champ d'application de la politique de sécurité des systèmes d'information.

On désignera sous le terme **utilisateur**, toute personne intervenant à titre permanent ou temporaire et disposant d'un accès, local ou à distance, aux ressources des systèmes d'information de GPM. La présente charte s'impose à tous les utilisateurs quels que soient leur statut ou le lieu d'exercice de leurs fonctions au sein de GPM (salarié, alternant, stagiaire, vacataire, prestataire, consultant…).

On désignera sous le terme **compte**, le moyen d'accès (nom d'utilisateur, mot de passe et autre facteur) qui permet à un utilisateur de se connecter aux services et aux ressources informatiques.

Les **ressources d'information et de communication** sont l'information et ses différents moyens de stockage, d'accès ou d'utilisation, parmi lesquels :

- les données et les informations, quels que soient leur nature et leurs supports de stockage ;
- les systèmes informatiques locaux, distants, bureautiques, de messagerie… ;
- les réseaux de communication ;
- les connexions, l'utilisation d'Internet et de l'Intranet ;
- la téléphonie ;
- les dispositifs de sécurité (pare-feu, antivirus, proxy…) ;
- les matériels, logiciels, applications et tout processus de traitement des données (automatisés ou non) ;
- les procédures de création, modification, suppression et d'échange d'informations.

Le terme **DPO** signifie Data Protection Officer soit Délégué à la Protection des Données.

Le terme **CSE** signifie Comité Social et Économique soit l'instance de représentation du personnel dans l'entreprise.

On désignera sous le terme **WIFI**, l'ensemble de protocoles de communications sans fil régi par les normes du groupe IEEE 802.11. Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, modem Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.

2. Champ d'application de la charte

La présente charte constitue une adjonction au règlement intérieur, diffusée à l'ensemble du personnel de GPM, qui produit, à ce titre, les mêmes effets.

Toute personne utilisant les ressources d'information et de communication de GPM est soumise aux règles de cette présente charte et consent à l'utilisation des moyens nécessaires à la sécurisation des données de l'entreprise. Ce cadre est également complété par la Politique de Sécurité des Systèmes d'Information.

Tout utilisateur faisant intervenir des personnes extérieures à GPM tels que des prestataires, des sous-traitants, des sociétés d'intérimaires, etc., se doit de faire respecter la présente charte, en exigeant un engagement contractuel pour toute intervention externe.

L'utilisation des ressources d'information, de communication dans l'entreprise est réservée à un usage professionnel, sauf exception pour répondre à une situation d'urgence. Ainsi, l'usage à titre privé de ces outils sera toléré de façon limitée, à condition de ne pas perturber l'accomplissement de la mission de l'utilisateur et de ne pas porter atteinte à l'image des entités de Groupe Pasteur Mutualité, ainsi qu'au bon fonctionnement des systèmes d'information.

La date d'entrée en vigueur de la charte d'utilisation des technologies de l'information et de communication est fixée au 25/05/2023 après consultation et avis du Comité Social et Économique. La présente est disponible dans sa dernière version numérique sur Tot'm. Elle fait l'objet d'un affichage au 4ième étage au sein du siège de Groupe Pasteur Mutualité (1 boulevard Pasteur 75015 Paris), et est systématiquement remis par la direction des ressources humaines à tout nouveau collaborateur. Tout changement significatif sera notifié à l'ensemble des utilisateurs qui s'engagent à en prendre connaissance et à le respecter.

3. Dispositions générales

Les entités de Groupe Pasteur Mutualité s'engagent à :

- mettre en place les systèmes et les outils permettant de garantir la sécurité globale du système d'information (données, réseaux, applications, postes de travail), afin d'éviter tout risque de destruction, d'altération et d'atteinte à la confidentialité ou à la disponibilité ;
- de suivre les préconisations en matière de sécurité des systèmes d'information ;
- s'assurer du respect des procédures adaptées aux contraintes de la sécurité des ressources d'information et de communication, avec l'attribution des accès protégés aux nouveaux arrivants, la suppression des droits des sortants, une gestion des mots de passe adéquate.

Chaque utilisateur est responsable des ressources qu'il utilise et doit en assurer, à son niveau, la protection afin qu'elles demeurent disponibles, fiables et intègres.

Chaque utilisateur doit savoir que l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi et de la réglementation applicables. Notamment, des recommandations de la Commission Nationale Informatique et Libertés (CNIL) et de la sécurité de l'entreprise. Et que d'autre part, sa négligence ou la mauvaise utilisation des ressources pourrait faire courir des risques à l'entreprise. L'accès aux ressources d'information et de communication de GPM est réservé aux utilisateurs de GPM ou à ses sous-traitants, qui doivent impérativement respecter les mêmes règles.

Toute installation ou modification (équipement, logiciel, données de configuration...) doit se faire dans le respect des procédures de l'entreprise.

4. Sécurité des ressources d'information et de communication

La protection du système d'information de Groupe Pasteur Mutualité vise avant tout à assurer sa disponibilité, son intégrité, sa confidentialité et sa traçabilité. Bien que des moyens organisationnelles et techniques soient mis en œuvre, ils ne constituent qu'un premier niveau de protection. Chaque collaborateur a un devoir individuel essentiel à jouer.

a. Conditions d'accès aux ressources

L'usage des moyens fournis aux utilisateurs de GPM s'effectue à partir de comptes nominatifs dont l'utilisation est soumise à une authentification. Tout possesseur d'un compte est responsable de l'utilisation de son identification d'utilisateur. Les moyens d'authentification (application mobile, code à usage unique, mot de passe, badge, ...) sont personnels, confidentiels et incessibles. L'utilisateur est responsable de toute connexion aux ressources d'information et de communication effectuée à l'aide de son identifiant, de ses mots de passe, ainsi que l'utilisation des données obtenues à partir des ressources d'information et de communication. A cet égard, il appartient à l'utilisateur d'utiliser tous les moyens mis à sa disposition par l'entreprise pour préserver la sécurité des systèmes d'information et des données qu'il contient.

L'utilisateur s'interdit l'utilisation de l'identifiant et du mot de passe d'un autre utilisateur. En cas d'absence de l'utilisateur, et pour des raisons de continuité de service, des possibilités de transfert de courrier électronique sont offertes sur une autre boîte aux lettres électronique de GPM et encadrée par une demande auprès de la direction des ressources humaines.

Par défaut, tout transfert automatique des courriels est interdit.

b. Règles de sécurité à respecter

Tout utilisateur témoin ou victime d'un incident de sécurité doit en référer immédiatement au support informatique (monsupport@gpm.fr), au RSSI (rssi@gpm.fr) ou à l'aide du dispositif d'alerte, accessible depuis Tot'm. Les entités de Groupe Pasteur Mutualité peuvent être soumises à une obligation de notification de ces incidents au regard de la règlementation en vigueur (autorité de régulation, DPO, personnes concernées, ...).

Le 26 mai 2020, l'utilisation du téléphone portable personnel a fait l'objet d'un avis positif par les membres du CSE. De ce fait, l'installation d'une application mobile est autorisée afin de recevoir un code de sécurité dans le cadre des nouvelles modalités de connexion distante.

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- ne pas masquer sa véritable identité et ne pas usurper l'identité d'autrui ;
- ne pas modifier le paramétrage du poste de travail et ne pas installer de logiciels sans autorisation préalable ;
- ne pas copier, modifier, détruire les logiciels propriétés des entités de Groupe Pasteur Mutualité ;
- ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas ;

- ne pas copier de données professionnelles sur un support externe non fourni par GPM ou toute autre solution de stockage en ligne, excepté les solutions d'entreprise prévues à cet effet (outil collaboratif Microsoft 365 et la plateforme d'échanges sécurisés, également nommée Oodrive) ;
- ne pas transmettre de données sensibles, notamment les médicales par courriel ou solliciter un adhérent pour recevoir ces dites données par voie électronique non sécurisée ;
- ne pas envoyer d'informations professionnelles sur une messagerie personnelle ;
- verrouiller son poste de travail dès qu'on s'en éloigne :
    - Windows : Touches Windows+L
    - Mac : Touches Control+Cmd+Q
- ne jamais mener d'actions engageant la responsabilité juridique ou financière des entités de GPM en répondant par exemple à un courriel dont l'authenticité n'est pas vérifiée ;
- appliquer les mesures de sécurité demandées par l'entreprise avant tout import de données d'origine extérieure ;
- utiliser des mots de passe qui respectent les bonnes pratiques en vigueur (cf. § 4.c) ;
- utiliser les moyens mis à sa disposition pour chiffrer les informations de l'entité ;
- ne transmettre en aucun cas à des tiers les moyens d'authentification qui lui sont fournis par l'entité, lesquels doivent rester personnels et confidentiels ;
- ne pas brancher, téléphone, ordinateur portable de l'entreprise sur des bornes de recharge USB publiques.

c. Règles de sécurité des mots de passe

Les comptes utilisateurs et à privilèges disposent de règles de construction différenciées et établies selon les critères suivants :

- Compte utilisateur :
    - 12 caractères respectant les modalités suivantes :
        - majuscule, minuscule, chiffre et caractères spéciaux, et une fréquence de renouvellement établie à 180 jours.

- Compte à privilèges :
    - 15 caractères respectant les modalités suivantes :
        - historisation des 24 derniers mots de passe et une fréquence de renouvellement établie de 30 à 360 jours.

Pour vous aider, deux méthodes vous sont présentées pour construire un mot de passe :

- La méthode phonétique :
    - «J'ai acheté huit cd pour cent euros cet après-midi !» deviendra ght8CD%€7am!.
- La méthode des premières lettres :
    - la citation «un tien vaut mieux que deux tu l'auras» donnera 1tvmQ2tl'A#1.

Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle…) ne doivent jamais être réutilisés pour d'autres services. L'utilisateur ne doit pas conserver les mots de passe dans des fichiers ou sur des post-it. Il n'est pas conseillé de préenregistrer ses mots de passe dans des navigateurs et notamment depuis un ordinateur public ou partagé. En cas de doute sur l'intégrité ou la confidentialité de l'un de ces mots de passe, celui-ci doit être modifié dans les plus brefs délais. L'utilisateur doit veiller à ne pas laisser accessible les ressources de l'entreprise et doit verrouiller ou déconnecter son équipement en cas d'absence à son poste de travail, même temporaire.

5. Respect des obligations légales

Compte tenu des risques liés à l'utilisation des ressources d'information et de communication, l'utilisateur est soumis à des obligations particulières afin de protéger les biens informationnels et l'image de Groupe Pasteur Mutualité.

L'utilisateur est soumis au bon respect des dispositions légales ou réglementaires applicables en l'espèce et qui sanctionnent notamment :

- le non-respect des bonnes mœurs ;
- la diffusion de propos à caractère diffamatoire ou raciste ;
- le piratage ou la fraude informatique ;
- le non-respect du droit d'auteur ;
- le non-respect des dispositions de la loi « informatique et libertés » ;
- ...

Tout utilisateur ne respectant pas les règles et obligations définies dans la présente charte est passible d'une sanction disciplinaire (selon les modalités prévues par le règlement intérieur) et / ou pénale en cas de circonstances le justifiant.

6. Utilisation des postes de travail et des équipements mobiles

Groupe Pasteur Mutualité peut mettre à la disposition de l'utilisateur des ressources (postes de travail, serveurs, tablettes, téléphones, smartphones, imprimantes ...) pour exercer son activité professionnelle. Ainsi tout utilisateur est responsable de l'usage raisonnable des ressources informatiques et du réseau, auxquels il a accès et contribue à le sécuriser. A ce titre, l'utilisateur s'engage à prendre soin du matériel, des installations informatiques mis à sa disposition, également durant ces déplacements et lors du temps de charge des batteries afin d'augmenter le plus possible le cycle de vie des équipements.

L'utilisateur s'interdit d'utiliser d'une manière qui pourrait mettre en danger les données que contient un équipement ainsi que les systèmes d'information de l'entreprise. Il est garant de la sécurité des équipements qui lui sont confiés et ne doit pas contourner la politique de sécurité mise en place sur ces derniers. En cas de perte ou de vol, l'utilisateur doit avertir dans les plus brefs délais le support informatique (monsupport@gpm.fr) et le délégué à la protection des données (dpo@gpm.fr). Afin qu'il soit procédé, si possible, à un blocage ou effacement à distance des données présentes sur le matériel, ainsi qu'à une évaluation de l'impact lié à la perte des données concernées et à l'inscription aux registres des incidents. Toute déclaration volontairement fausse est passible de sanctions disciplinaires et/ou de poursuites pénales. A des fins de précaution, certaines configurations peuvent être verrouillées par l'entreprise. L'utilisateur ne doit pas apporter de perturbations au fonctionnement des ressources et il s'interdit notamment :

- de modifier ces standards ;
- d'installer des logiciels qui n'auraient pas été approuvés formellement par l'Informatique ;
- d'ajouter ou de supprimer des équipements, matériels ou logiciels ou de modifier les données nécessaires à leur fonctionnement ;
- d'introduire des logiciels ou contenus malveillants (virus, cheval de Troie, bombe logique, etc.), à caractère pornographique, raciste ou contraire aux bonnes mœurs ainsi que tout autre fichier prohibé par la loi ;
- d'empêcher le bon fonctionnement ou la mise à jour du logiciel antivirus.

Toute demande d'ajout de matériel, logiciel, progiciel, etc., liée aux nécessités du service, d'une mission temporaire ou définitive, doit faire l'objet d'une demande auprès du support informatique. Il est rappelé que les sessions de travail doivent être verrouillées quand les équipements ne sont pas utilisés et même lors d'une absence momentanée du bureau.

Enfin, aucun ordinateur, non confié par l'entreprise, ne doit être connecté au réseau local de l'entreprise sauf :

- à un réseau strictement dédié validé par le RSSI (exemple : réseau wifi invité) ;
- dérogation temporaire et formelle du RSSI soumise à signature d'un engagement de l'utilisateur de l'équipement non GPM.

a. Postes de travail

Dans le cadre de son activité métier, le collaborateur dispose d'un poste de travail, permettant le travail à distance. Il est de son devoir de suivre les bonnes pratiques et il convient également :

- de veiller à maintenir en bon état de fonctionnement le matériel et les logiciels mis à sa disposition ;
- sur son lieu de travail, d'être vigilant et se doter d'un système antivol si nécessaire et en cas de non-utilisation, le ranger dans un casier fermé ;
- dans un lieu public (gare, train, restaurant, aéroports, etc.), veiller à ce que personne d'autre ne puisse consulter l'écran de son ordinateur en utilisant le filtre de confidentialité ;
- lors de déplacements, ne pas laisser l'ordinateur portable dans un véhicule en stationnement ou sans surveillance ;
- en tout état de cause, éviter d'y conserver des documents confidentiels ;
- signaler tout dysfonctionnement ou anomalie sur le matériel.

Comme pour les postes fixes et dans les mêmes conditions, l'utilisateur est informé que des contrôles périodiques sont effectués pour vérifier la bonne application des règles définies.

b. Téléphonie

Groupe Pasteur Mutualité met à disposition des utilisateurs et pour l'exercice de leur activité professionnelle, des téléphones mobiles. L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable. De manière générale, il est interdit d'appeler des numéros surtaxés, d'appeler les numéros à l'étranger ou à destination des DOM TOM sauf si des nécessités de services le justifient. Les SMS envoyés ou reçus sont présumés avoir un caractère professionnel, sauf s'ils ont été identifiés comme étant personnels.

Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. GPM vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs. L'entreprise s'interdit d'accéder à l'intégralité des numéros appelés. Toutefois, en cas d'utilisation manifestement anormale, l'Informatique, sur demande validée par la direction des ressources humaines, se réserve le droit d'accéder aux numéros complets des relevés individuels. En accord avec les dispositions réglementaires en vigueur, GPM se réserve la possibilité d'assurer un suivi, un contrôle et un enregistrement des communications téléphoniques à des fins d'amélioration de la qualité du service et de formation des utilisateurs.

c. Smartphones et tablettes

Pour réduire tout effet de bord, lors de l'utilisation des services en ligne GPM et notamment pour les tablettes, il est fortement déconseillé que l'utilisateur fasse une mise à jour d'OS, sans la validation de l'Informatique. Pour un usage en télétravail, il est demandé :

- de ne pas laisser les terminaux mobiles continuellement branchés sur chargeur ou au poste de travail (risque de dégradation anticipée de la batterie) ;
- d'éviter de les décharger complètement et de les laisser longtemps dans cet état (risque de perte de configuration).

En complément des aspects liés strictement à la « téléphonie », il est formellement interdit d'effectuer des achats susceptibles d'être facturés à GPM. L'utilisateur doit être extrêmement vigilant dans le cadre d'une utilisation privée de ces équipements et notamment dans le cadre des règles de confidentialité des applications utilisées.

L'utilisateur s'engage à :

- ne pas partager ses données de contacts ;
- ne pas tenter de pirater, modifier la configuration de ses équipements.

d. Autres terminaux mobiles, nomades ou dispositif de stockage

L'utilisation des terminaux mobiles personnels sur le lieu du travail est soumise aux restrictions suivantes :

- ne pas se connecter au système d'information de l'entreprise (par Wifi, par USB, Bluetooth…), hors réseau sans-fil mis à disposition par l'Informatique ;
- ne pas utiliser l'espace de stockage de ces appareils pour transporter des documents de travail ;
- ne pas recharger son smartphone en le connectant à une prise USB d'un ordinateur non géré par la structure ou mise à disposition dans un lieu public ;
- tout périphérique de stockage ou disques externes doit faire l'objet d'un scan par les solutions de sécurité (antivirus ou autre) à chaque utilisation par le collaborateur ;
- si ces périphériques contiennent des données sensibles, elles doivent être chiffrées avec les logiciels validés par l'informatique.

L'utilisation de support de stockage, pour transporter des données sensibles, stratégiques ou contenant des données à caractère personnel, est conditionné au chiffrement des données validé par l'Informatique et doit être limitée au profit de l'utilisation de la plateforme d'échanges sécurisés. L'usage dans le cadre professionnel des appareils photo, vidéo et de l'enregistreur sonore intégrés aux appareils mobiles personnels ou professionnels est interdit. A l'exception de la vente à distance et dans le cadre d'une autorisation expresse de la hiérarchie et/ou de la Direction de la communication et avec accord écrit des personnes concernées.

7. Utilisation des outils numériques

a. Utilisation d'internet

L'accès à internet n'est autorisé qu'au travers des dispositifs de sécurité mis en place par GPM. Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable. D'une manière générale, il est rappelé que l'utilisateur s'engage à adopter un comportement vigilant et responsable dans l'environnement internet. L'utilisateur doit notamment utiliser les services internet dans le cadre strict des droits qui lui sont accordés, des accès qui lui sont autorisés, et dans le respect des principes et des règles propres aux divers sites concernés. Il est de la responsabilité pénale et éthique de l'entreprise d'interdire la consultation de tout site légalement prohibé notamment incitant à la haine raciale, révisionniste, pédophile ou contraire aux bonnes mœurs.
Si l'utilisateur est amené à consulter, à son insu, de tels éléments, il est tenu d'informer le RSSI (rssi@gpm.fr) dans les plus brefs délais. Si un utilisateur constate qu'un site est bloqué à tort, celui-ci doit contacter le support informatique à l'adresse monsupport@gpm.fr. Le téléchargement de fichiers est autorisé, dans la mesure où l'émetteur est identifié et reconnu et où cela n'affecte ni les règles de sécurité ni la performance des ressources. Le téléchargement doit être légal et conforme à la règlementation applicable. L'utilisateur est informé que l'entreprise met en œuvre des outils de filtrage et de contrôle permettant de détecter les téléchargements illégaux.

b. Utilisation des réseaux sociaux

Les espaces de discussion, les réseaux sociaux sont réservés à un usage exclusivement professionnel et doivent faire l'objet d'une autorisation de la hiérarchie de chaque utilisateur ainsi que répondre aux règles d'utilisation des ressources édictées dans la présente charte.

L'utilisateur est pleinement et seul responsable des propos et messages qu'il échange tant vis-à-vis de l'entreprise que des tiers, extérieurs à cette dernière. L'utilisateur doit notamment :

- faire preuve de la plus grande correction à l'égard de ses interlocuteurs ;
- ne pas en faire un usage abusif ;
- observer un devoir de réserve, se garder d'émettre toute opinion susceptible de porter préjudice à l'image de GPM.

Ces espaces et réseaux représentent une source d'espionnage industriel très importante. En conséquence, l'utilisateur s'engage à ne les utiliser que dans le respect des principes suivants :

- ne pas s'exprimer au nom de GPM ;
- respecter les règles édictées par la présente charte mais aussi d'éthique et de loyauté envers l'entreprise, ses collaborateurs, administrateurs, adhérents, clients, fournisseurs et partenaires ;
- ne communiquer que des informations dont la véracité, la précision, la réalité ont été vérifiées et en veillant à ce que cette communication ne viole pas les règles de confidentialité, ni les droits de l'entreprise ou de tiers ;
- ne pas diffuser des informations confidentielles sur l'entreprise, sauf autorisation formelle ;
- ne pas utiliser des données, y compris les photographies ou autres données personnelles relatives à des tiers ;
- veiller à la sécurité des documents publiés ;
- créer des profils distincts « professionnel » et « personnel » lors de l'utilisation des médias sociaux en veillant à utiliser des paramètres de confidentialité adéquats ;
- respecter strictement les conditions générales d'utilisation.

Il convient d'exclure la communication d'informations personnelles sur le profil professionnel. Les propos exprimés ou les données communiquées sur un profil personnel doivent respecter les principes de loyauté, courtoisie, respect des règles de confidentialité, des droits de propriété intellectuelle et de protection des données personnelles édictées par la présente charte.

Il est rappelé que les communications sur les réseaux sociaux peuvent être ouvertes au public et peuvent être contrôlées par l'entreprise (à l'exception du cadre des recrutements ou de l'évaluation du personnel).

GPM se réserve le droit de demander la suppression ou le retrait de tout contenu d'un utilisateur portant préjudice à l'entreprise, ses salariés, clients, fournisseurs ou partenaires. L'utilisateur s'oblige à répondre à la demande de suppression ou de retrait dès réception de la demande.

Tout contenu publié par un utilisateur sur un espace collaboratif par l'entreprise relève de la responsabilité du seul utilisateur. GPM ne saurait être tenu responsable d'un manquement de l'utilisateur aux règles énoncées dans la présente charte.

L'utilisateur, s'il a créé un espace de discussion personnel, devra s'abstenir de toute publication durant leur temps de travail. Ils devront également se garder de diffuser, soit sur leur espace de discussion, soit sur celui d'un tiers, des propos injurieux ou diffamatoires, portant atteinte à l'honneur et à la réputation de GPM, de ses collaborateurs ou de ses administrateurs.

8. Outils collaboratifs

Lorsque des outils sont mis à disposition de l'utilisateur dans le cadre de l'entreprise, celui-ci doit les utiliser à des fins professionnelles, et en faire un usage approprié conformément à la présente charte. Ces outils, sauf dispositions spécifiques de GPM, n'ont pas pour but de contrôler l'activité individuel courante de l'utilisateur conformément à la présente charte. L'utilisateur est individuellement responsable de ses publications et partages. Lors de la création d'une équipe ou d'une ressource dans un espace collaboratif, l'utilisateur en devient propriétaire et se doit de s'assurer d'une revue des droits périodique.

Les groupes à vocation politique, religieuse, philosophique, syndicale ou sexuelle ne sont pas autorisés. De manière plus générale, toute démarche à caractère prosélyte sera à proscrire.

L'utilisateur s'engage à :

- respecter la loi en vigueur ainsi que la présente charte ;
- ne pas intervenir de façon anonyme, ni utiliser de pseudonyme ou emprunter une quelconque identité fictive ;
- ne doit pas porter atteinte aux droits de tiers ni être susceptible par ses contributions de porter atteinte à l'image de GPM, de ses collaborateurs ou de ses administrateurs ;
- faire preuve de discernement et de prudence s'agissant des informations auxquelles il accède, qu'il transmet ou partage notamment sur la sensibilité des informations (stratégiques, restreinte, interne) et les personnes accédant au partage ;
- veiller à la modération des espaces qui lui sont ouverts ;
- ne pas tenter d'obtenir des droits ou privilèges qui ne lui ont pas été octroyés et signaler toute anomalie ;
- informer tous les participants, de son intention de vouloir enregistrer, une conversation téléphonique, un entretien, une réunion de travail… afin qu'ils aient la possibilité de pouvoir formellement s'y opposer.
- signaler un comportement contraire à la charte ou un abus, auprès du RSSI (rssi@gpm.fr).

Dans le cas d'une consommation de services d'informatique dans le nuage « Cloud », l'utilisateur s'engage à respecter les conditions générales d'utilisation de cette plateforme qui régissent les interactions entre les utilisateurs et les différents groupes.

L'entreprise se réserve le droit de contrôler cet usage, dans les limites et selon les conditions prévues par la loi et conformément aux dispositions relatives au contrôle de la présente charte. Une attention particulière est apportée à l'enregistrement des réunions en ligne puisque l'utilisateur doit en formuler son souhait.

a. Utilisation de la messagerie électronique

L'adresse électronique octroyée par l'entreprise est strictement professionnelle. Elle ne doit donc pas être utilisée dans un autre contexte, et notamment diffusée sur des sites internet (messagerie instantanée et « chat », forums, blogs, etc.), sans rapport avec l'activité professionnelle. Il est essentiel de suivre les préconisations en matière d'échanges professionnels. De manière générale, il est essentiel de transférer tout courriel suspect à l'aide de la fonctionnalité « Report phishing » disponible depuis le client de messagerie ou d'utiliser l'adresse report@gpm.fr pour analyse.

L'utilisateur ne doit pas :

- affecter le trafic normal des messages professionnels par l'émission ou la réception de messages à caractère personnel ;
- ouvrir les fichiers joints ni cliquer sur les liens issus de messages électroniques douteux et non sollicités ;
- fournir des informations personnelles en particulier si les informations sont demandées dans un courrier électronique ou sur un site dont il n'a pas une confiance absolue ;
- utiliser la messagerie électronique professionnelle pour relayer des messages électroniques intempestifs (à titre d'exemple plus de 10 destinataires), sauf pour des raisons de services et/ou avec une autorisation formelle de la direction des ressources humaines ou de la communication ;
- envoyer des messages en chaîne (messages reçus individuellement dans le cadre d'une diffusion collective avec invitation à le renvoyer également collectivement) ;
- répondre ni faire suivre les courriers électroniques alarmistes de provenance douteuse qui sont souvent des tentatives d'escroquerie ;
- répondre à des demandes d'assistance de provenance douteuse (si la demande provient de l'adresse exacte d'un adhérent, d'un collaborateur ou d'un administrateur, il est possible d'informer par téléphone la personne concernée d'une usurpation de son identité et d'un probable piratage de sa messagerie) ;
- transférer automatiquement des messages électroniques vers une messagerie externe ;
- transférer des documents non publics vers une messagerie externe.

b. Stratégie de communication électronique

Le service informatique intègre en permanence la nécessité d'informer les utilisateurs de tout évènement susceptible de perturber ou interrompre le bon fonctionnement de l'environnement de travail, et de les informer de la reprise normale. Ces communications sont réalisées depuis la boite aux lettres : +production-dsi@gpm.fr

Font l'objet d'une communication :

- les arrêts planifiés (pour maintenance nécessitant l'arrêt des infrastructures ou des applicatifs) ;
- les arrêts sur incident lorsque le délai de reprise dépasse le niveau d'engagement ;
- les dégradations de performance (ralentissements, microcoupures, etc.).

Le service informatique communique par courriel pour les collaborateurs du siège et via un canal Teams pour les collaborateurs du réseau.

Pour les autres services, le canal de communication privilégié, reste le courriel, à travers l'utilisation des listes de distribution suivantes :

- +siege@gpm.fr : si la communication est à destination du siège
- +reseau@gpm.fr : si la communication est à destination du réseau commercial

c. Accès à distance

La présente charte s'applique pleinement en cas de connexion à distance.

Seules les solutions d'accès fournies par l'entreprise et explicitement dédiées à cet usage distant sont autorisées (connexion au réseau sécurisé de l'entreprise et authentification multi-facteur). En particulier, l'utilisateur s'oblige à une vigilance accrue et à un comportement responsable lié à la sensibilité de ses opérations. L'utilisateur se doit d'utiliser un poste à jour et bénéficiant de l'ensemble des composants de sécurité des systèmes d'information. Aucune opération sensible (ayant trait à des données bancaires ou de santé par exemple) ni impression ne doit être effectuée dans un lieu public (gare, restaurant, cybercafé, aéroport…).

Les équipements mis à disposition sont réservés à un usage strictement professionnel par l'utilisateur et doivent être sécurisés selon les modalités décrites préalablement. L'utilisateur ne doit pas entraver le fonctionnement des mises à jour de sécurité et des équipements de sécurité.

En cas de difficultés, relatives à ces éléments, l'utilisateur doit prendre contact avec le support informatique selon les procédures en vigueur.

9. Analyse et contrôle de l'utilisation

a. Droits et devoirs des administrateurs des réseaux et systèmes

La mise en place d'outils de sécurité par l'entreprise ne doit pas, toutefois, dispenser les utilisateurs d'une obligation de vigilance à cet égard. En effet, l'utilisateur a la charge, à son niveau, de contribuer à la sécurité générale et à celle de son entité. Toute tentative de violation des ressources mises à sa disposition doit être signalée dès qu'il en a connaissance, ainsi que toute situation anormale ou dysfonctionnement. Afin de conduire les actions correspondant à leurs missions (maintenance, configuration, évolution, supervision...), les administrateurs des réseaux et systèmes disposent de droits d'accès privilégiés au système d'information. Ces droits d'accès privilégiés peuvent présenter des risques spécifiques, car donnant la possibilité technique d'accéder à des informations confidentielles, d'altérer voire de supprimer des données, de modifier des droits d'accès au système d'information ou des mécanismes de protection, de réaliser des contrôles ne respectant pas le cadre légal et réglementaire. Chaque administrateur doit avoir conscience de ses responsabilités en matière de sécurité du système d'information, et des risques que présente une utilisation abusive des droits d'accès privilégiés qui lui sont confiés (cf. Annexe). Les administrateurs doivent également veiller à assurer le fonctionnement normal et la sécurité des outils informatiques et veiller à ce que les intérêts légitimes du système d'information soient préservés. Dans ce cadre, les administrateurs des systèmes informatiques et sécurité sont tenus à une responsabilité et à des obligations renforcées par rapport à celles des autres utilisateurs, notamment en matière de confidentialité et d'intégrité dans l'exercice de leur métier.

b. Moyens de contrôle interne

L'utilisateur est informé que les moyens fournis par l'entreprise peuvent être géolocalisables.

Divers équipements réalisent un filtrage, notamment lors de la navigation web. Et seront rejetés automatiquement après détection :

- les virus et attaques logiques ;
- les demandes de connexions sur certains sites ;
- les escroqueries véhiculées par les systèmes de messagerie (spam, phishing, etc...) ;
- les connexions des utilisateurs non dûment autorisées à franchir une passerelle inter-réseaux.

c. Archivage

A des fins de contrôle de sécurité, l'ensemble des flux d'informations pourra être archivé pendant un an. Sont ainsi susceptibles d'être archivées les informations suivantes :

- l'ensemble des flux entrants ou sortants au niveau de nos équipements ;
- l'ensemble des fichiers journaux (qui contiennent notamment les tentatives de connexion, les comptes et sites accédés) et des fichiers systèmes ;
- l'ensemble des fichiers rapports constitués par les équipements de sécurité (pare-feu, sonde de détection d'intrusion, anti-virus, ...).

Toute diffusion d'information sur ces moyens, par des personnes non mandatées, est interdite tant à l'intérieur qu'à l'extérieur de GPM.

Le traitement des informations et les moyens associés, déclarés à la CNIL, peuvent être utilisés à des fins de contrôle, à partir des archives, des documents mis en quarantaine, et de l'état instantané du système d'information :

- sur demande des autorités (administratives, judiciaires ou de police..) ;
- en cas d'incidents divers (virus, intrusion, saturation des ressources, pannes) ;
- en cas d'acte de malveillance avéré ou constaté, ou de détournement des moyens ou des ressources d'information et de communication ;
- si nécessaire, à la demande du destinataire ou de l'émetteur.

d. Moyens de contrôle externe

Les utilisateurs sont informés que l'entreprise se réserve la possibilité d'effectuer des contrôles sur la teneur des informations déposées par les utilisateurs sur les forums internet par consultation de serveurs internet externes à l'entreprise et spécialisés dans des recherches de ce type. Ces contrôles peuvent être opérés de façon inopinée ou systématique en cas d'incident ou d'acte de malveillance.

10. Départ définitif d'un collaborateur ou absence longue durée

Chaque utilisateur doit veiller à ce que la continuité de service soit assurée. Les responsables doivent s'assurer que le support informatique est informé, dans le respect des procédures en vigueur, de tout changement de fonction ou départ d'un de ses utilisateurs (collaborateurs, intérimaires, prestataires…).

En cas d'absence pour maladie, la direction des ressources humaines se réserve la possibilité de procéder à la suspension des accès de l'utilisateur, si le cas le justifie.

En cas d'absence temporaire de l'utilisateur, pour quelle que cause que ce soit (congés, maladie, ou de continuité de service, …), l'entreprise pourra avoir accès, dans le respect de la présente charte, à ses données (fichiers) de travail présumé professionnelles aux seules fins d'assurer la continuité du service. Les données considérées comme personnelles n'auront pas vocation à être consultées.

Il peut être demandé ponctuellement au service informatique, en ayant préalablement contacté les ressources humaines, pour transmettre au responsable de l'utilisateur, le ou les messages électroniques à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur. Le RSSI doit être informé de la procédure et l'utilisateur doit disposer dès que possible de la liste des messages qui ont été transférés.

L'utilisateur, quittant l'entreprise ou partant en absence longue durée, doit mettre en œuvre :

- un message d'absence indiquant qui contacter ;
- une délégation d'accès à sa messagerie à son responsable ou à la personne désignée par ce dernier.

Pour des raisons de continuité de service, tout responsable pourra demander la mise en œuvre de ces diligences pour un membre de son service après validation formelle par l'utilisateur concerné ou à défaut par la direction de la conformité.

De plus, l'utilisateur, lors de son départ définitif, doit notamment :

- restituer, en bon état général de fonctionnement, l'ensemble des équipements informatiques et des moyens de connexion qui lui ont été remis dans le respect des procédures en vigueur ;
- détruire ses données privées (répertoire personnel, fichiers, dossiers et messages électroniques identifiés par lui comme « privé ») ;
- supprimer le compte Apple et remettre en état d'usine la tablette et ou le téléphone mobile.

Par ailleurs, les accès informatiques sont supprimés faisant suite à un départ définitif selon les règles précisées en annexe par le support informatique (les cas prévoyant une dispense de préavis sont également inclus).

Tout collaborateur quittant l'entreprise perd sa qualité d'utilisateur. Les données et messages liés à son compte informatique seront détruits. Toute autorisation d'accès prend fin lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifiée.

11. Confidentialité

a. Respect de la confidentialité

Le respect de la confidentialité est inhérent aux activités de GPM. L'utilisateur doit donc respecter son obligation de réserve et de confidentialité à l'égard des tiers. La sauvegarde des intérêts de GPM nécessite le respect par l'utilisateur d'une obligation générale et permanente de confidentialité, de discrétion et de secret professionnel à l'égard des ressources et informations dont il a connaissance à l'occasion de l'exercice de ses fonctions.

Le respect de cette obligation implique notamment que l'utilisateur veille à ce que les informations qu'il exploite ne puissent pas être consultées, modifiées ou reproduites par un tiers non autorisé.

L'attention de l'utilisateur est attirée sur les risques liés à la diffusion de contenus d'information sur internet, en particulier au sein des réseaux sociaux et sur les blogs. Il est donc interdit de diffuser à l'extérieur de l'entreprise et, plus particulièrement, sur internet, la moindre information confidentielle sur GPM, qu'elle soit ou non protégée par une obligation légale de secret ou une obligation contractuelle de confidentialité.

Les messages personnels ne doivent pas contenir d'informations « internes entreprise », sensibles, stratégiques, confidentielles ou être assimilables à des communications de l'entreprise (signature ou en-tête au nom de l'entreprise).

b. Obligation de discrétion

Compte tenu du secteur particulier dans lequel il exerce son activité professionnelle, l'utilisateur est tenu :

- à une obligation de discrétion ;
- à une obligation de probité ;
- au secret professionnel ;
- à la confidentialité la plus absolue sur les éléments, informations, documents auxquels il a accès dans le cadre de ses fonctions.

Ces obligations s'appliquent également dans l'usage des ressources.

Dans le cadre de ses obligations et, afin de se prémunir de tout risque vis-à-vis de tiers (tel que la fraude), il est interdit aux utilisateurs de reproduire et de communiquer sous quelque forme que ce soit à des personnes internes ou externes à l'entreprise, personnes physiques ou morales, non autorisées, toutes informations confidentielles ou sensibles notamment :

- les détails précis de son travail quotidien : dossiers traités, projets internes, éléments techniques concernant le système d'Information, éléments concernant l'organisation de l'entreprise (réflexions en cours sur des projets par exemple …), éléments chiffrés (budgets, délégations de signature, montants de contrats…) ou tout élément concernant la sécurité de l'entreprise ;
- la nature et l'objectif de ses déplacements professionnels ;
- les informations confidentielles sur le personnel (coordonnées, rémunération d'un tiers, état de santé, etc.) ;
- l'identité des sociétés tierces (clients, fournisseurs, partenaires…) avec lesquelles l'utilisateur est amené à travailler.

Ce devoir de discrétion s'applique à tous les échanges à l'extérieur de l'entreprise : messageries instantanées, réseaux sociaux, discussions sur internet, communications avec des clients ou partenaires de l'entreprise, publications de son CV par l'utilisateur à l'extérieur de l'entreprise.

A noter que des usurpations d'identité sont réalisées notamment par téléphone et par courriel afin de préparer des attaques informatique (exemple : rançongiciel) et/ou des escroqueries financières (exemple : arnaque au Président, fausse demande d'assistance).

L'utilisateur doit adopter les bons réflexes :

- ne pas divulguer d'informations (qui est le Directeur de… ; qui s'occupe de… ; quels sont vos projets pour l'année à venir ; etc.) sur notre organisation par téléphone ou par courriel à des interlocuteurs externes que l'on ne connait pas ou que l'on ne peut pas identifier formellement ;
- prendre les coordonnées de la personne et indiquer qu'elle sera, éventuellement, rappelée sans communiquer d'identité ;
- faire attention à l'émetteur (Par exemple www.whitehouse.gov est le site officiel de la Maison Blanche, tandis que www.whitehouse.com ne l'est pas) ;
- avertir votre responsable et le RSSI (rssi@gpm.fr) si vous recevez ce type d'appel / de courriel ou en cas de doute.
- l'utilisateur amené dans le cadre de ses fonctions à manipuler des fichiers ou à intervenir sur les ressources de l'entreprise doit s'abstenir de prendre connaissance de leur contenu en dehors du strict exercice de sa mission.

12. Droit à la déconnexion

Les possibilités de connexion à distance sont désormais multiples avec le développement des équipements mobiles (ordinateur portable, tablette ou smartphone, etc…) permettant de travailler dans les locaux de GPM ou sur son lieu de télétravail.

Ces évolutions présentent des avantages tant à titre professionnel que personnel. Groupe Pasteur Mutualité considère toutefois que la mise à disposition de ces outils doit s'accompagner d'une véritable vigilance de la part de l'entreprise et de la part de chaque utilisateur afin de s'assurer que l'équilibre entre la vie professionnelle et la vie privée est respecté.

Un accord sur le droit à la déconnexion du 24 mars 2017 est publié en ce sens par la direction des ressources humaines sur l'intranet, rubrique Accords.

13. Numérique Responsable

Parce que le numérique est un acteur majeur d'émissions de Gaz à Effet de Serre, d'épuisement des ressources et d'affaissement de la biodiversité, participant activement au changement climatique, Groupe Pasteur Mutualité s'engage à optimiser les outils numériques pour limiter leurs impacts et consommations, à développer des offres de services accessibles pour tous, inclusives et durables.

Parce que la transition vers un numérique responsable est indispensable pour assurer la résilience des organisations, GPM s'engage à rendre le numérique mesurable, transparent et lisible pour des pratiques numériques éthiques et responsables.

GPM s'engage à favoriser l'émergence de nouveaux comportements et valeurs.

14. Protection des données à caractère personnel

a. Droit d'accès du collaborateur

Groupe Pasteur Mutualité accorde la plus grande importance au respect de la vie privée de ses collaborateurs et s'engage à ce que la collecte et la conservation de leurs données se fassent en toute transparence et sécurité, conformément à la règlementation en matière de protection des données à caractère personnel.

GPM a nommé un DPO et rédigé une « Charte de protection des données à caractère personnel des collaborateurs », publiée sur l'intranet. Tout collaborateur peut exercer ces droits par demande auprès du DPO (dpo@gpm.fr).

b. Droit à l'image

Une autorisation d'enregistrement de l'image et la voix est fournie à tout nouvel arrivant, destinée à recueillir le consentement et les autorisations nécessaires dans le cadre d'utilisation de l'image. L'image d'une personne ainsi que les enregistrements vidéo et sonores qui se rapportent à elle, ne peuvent être utilisés ou diffusés sans son consentement écrit. Les photos, enregistrements vidéo ou sonores pris dans le cadre des activités ou dans ses locaux ne peuvent pas être utilisés à des fins personnelles, et sont interdits à la diffusion externe sans le consentement.

c. Engagement de confidentialité manipulation de données à caractère personnel

Le collaborateur en tant qu'acteur de la conformité à la règlementation en matière de protection des données à caractère personnel, est également tenu au respect de certaines obligations. La constitution de fichiers bureautiques intégrant des données à caractère personnel doit être réalisée conformément à la réglementation : elle doit être prévue par un traitement enregistré dans le registre du groupe sous le contrôle du DPO.