Charte informatique

PBM	Charte informatique	Signature	
Rédigé par	Mohamed BEKHEDDA DSI		
Approuvée par	Christophe Gomis		Date : 12/03/2024
Version	1.0		Nombre de pages :15

Préambule

PBM Groupe met en œuvre un système d'information et de communication (ci-après le « **SI** » ou « **Système d'Information »**) pour l'ensemble de ses entreprises et notamment pour «Nom_de_la_société». Ce SI est nécessaire au bon fonctionnement et à l'exercice de ses activités, comprenant notamment un réseau informatique, un système de communications numériques par e-mails, messagerie instantanée et téléphonie, ainsi que des outils mobiles, qui favorisent l'accès à l'information, au transfert de données et améliorent ainsi la communication.

Un usage non maîtrisé du SI et/ou du matériel expose l'entreprise à un certain nombre de difficultés d'ordre technique (incluant notamment la saturation de la bande passante et des capacités de stockage, l'augmentation des risques de virus informatiques, les risques de divulgation d'informations confidentielles, de cyber-attaques) et juridique puisque tout usage du SI contraire à la réglementation en vigueur par les utilisateurs est susceptible d'engager la responsabilité de PBM Groupe ainsi que la leur.

Dans un but de promotion d'une utilisation loyale, responsable et sécurisée du SI, la présente charte a pour objet d'en fixer les conditions d'utilisation et d'informer les utilisateurs sur les moyens de contrôle et de surveillance mis en œuvre par l'entreprise afin d'assurer l'efficacité ainsi que la sécurité du SI (ci-après, la « **Charte** »).

I. CHAMP D'APPLICATION

A. Utilisateurs

Sauf mention ou stipulation contraire, la Charte s'applique à l'ensemble des utilisateurs (ci-après les « **Utilisateurs** ») du SI, quel que soit leur statut, y compris : les mandataires sociaux, les salariés, les intérimaires, les stagiaires, les employés de sociétés prestataires de services et plus généralement toute personne autorisée à utiliser le SI.

De plus, la Charte s'applique aux Utilisateurs qui communiquent sur les réseaux sociaux à titre professionnel et/ou dès lors que la communication fait un lien direct ou indirect avec PBM Groupe, ses marques, ses produits et l'activité professionnelle du salarié. Ce sujet fait l'objet d'une annexe spécifique au présent document.

B. Le Système d'Information de PBM

D'une façon générale, le SI est composé de tous les outils informatiques et/ou de télécommunication et les services informatiques accessibles depuis le SI mis à la disposition des Utilisateurs.

Le SI est notamment constitué des éléments suivants :

- des ordinateurs et moyens de communication téléphonique, fixes ou mobiles, et tout autre matériel informatique : périphériques (dont clés USB ; disques durs externes), photocopieurs, tablettes, ;
- l'ensemble des logiciels, progiciels, bases de données et données;
- les infrastructures réseaux et de télécommunications ;
- la messagerie électronique, outils collaboratifs et l'intranet et/ou l'extranet
- la connectivité, permettant l'accès à internet;

- les services n'appartenant pas à l'entreprise et auxquels les Utilisateurs seraient susceptibles d'accéder via le système d'information. Mode SAAS (Software As A Service : Service Logiciel hébergé dans le cloud), cloud.

C. Le Service Informatique

Le Service Informatique a notamment pour mission de contrôler la sécurité, l'intégrité et l'usage loyal du SI, des accès et utilisations de l'ensemble du SI, des services tiers et de la connectivité Internet par les Utilisateurs. Il peut être externalisé et géré par un prestataire spécialisé.

Les membres du Service Informatique sont assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître. En cas de questions relatives à l'utilisation du SI et/ou des Services Internet, les utilisateurs sont invités à contacter le Service Informatique pour obtenir de plus amples informations.

D. Dépôt, communication et entrée en vigueur de la présente Charte

La Charte fait partie intégrante du Règlement Intérieur de l'entreprise du Groupe PBM et a été soumise à information et consultation préalable du CSE.
Un exemplaire peut être obtenu sur simple demande auprès de la Direction des Ressources Humaines. En outre, la Charte pourra le cas échéant, être mise à disposition en libre téléchargement par les Utilisateurs à partir de l'intranet de PBM.

Toute modification ultérieure ou tout retrait d'une ou plusieurs dispositions de la présente Charte serait, conformément au Code du travail, soumis à la même procédure, étant entendu que toute disposition de la présente Charte qui deviendrait contraire aux dispositions légales, règlementaires ou conventionnelles applicables à PBM, serait nulle de plein droit sans préjudice des autres dispositions qui garderont toute leur force et leur portée.

II. VOS RESPONSABILITES

A. Règles générales

Les Utilisateurs s'engagent :

- à utiliser les moyens électroniques ou informatiques et les moyens de communication mis à leur disposition en conformité avec les règlementations applicables et notamment celles relatives à la protection de la propriété intellectuelle et des données à caractère personnel.
- à utiliser le SI et/ou les Services Internet pour leurs besoins professionnels dans les conditions plus amplement décrites à l'article III. de la Charte.

Tous les Utilisateurs s'engagent à respecter les règles et principes stipulés dans la Charte. Un manquement à ces règles et principes pourrait constituer une faute susceptible d'entraîner des sanctions disciplinaires et/ou des poursuites judiciaires, comme plus amplement décrit à l'article V de la Charte.

B. Mise à disposition et restitution du SI et des Services Internet

Le SI et les Services Internet sont mis à disposition des utilisateurs pour toute la durée de la relation de travail et restent l'entière propriété de l'entreprise. A cet effet, l'Utilisateur s'engage à maintenir tous les éléments constituant le SI et/ou les Services Internet (ordinateurs, téléphones, équipements, logiciels,…) en bon état de fonctionnement et à les restituer sur simple demande à PBM ou à la date de son départ

Il est précisé que l'accès et l'utilisation du SI et des Services Internet de l'entreprise sont interdits via un appareil personnel, sauf cas exceptionnel expressément autorisé.

1. Protection du SI

Les logiciels ou progiciels qui sont utilisés au sein de l'entreprise sont tous protégés par des droits de propriété intellectuelle. A ce titre, chaque utilisateur s'engage à respecter strictement lesdits droits et toutes les conditions d'utilisation qui lui seront communiquées.

Les Utilisateurs s'engagent à ne pas utiliser sur le SI, des logiciels ou progiciels externes à PBM Groupe quelle qu'en soit l'origine ou la nature, professionnelle ou privée. En effet, un contrat doit être établi avant toute acquisition de logiciels édités par des tiers ou toute acquisition de base de données, que ces derniers soient gratuits ou payants. Les Utilisateurs sont invités à contacter la direction du Service Informatique. A défaut d'accord écrit de sa part, son refus sera présumé.

Pour des raisons de sécurité, l'entreprise se réserve la faculté, à tout instant et sans préavis, de procéder ou de faire procéder, par tout tiers de son choix, aux contrôles nécessaires pour s'assurer du respect des présentes prescriptions.

2. SI et temps de travail

L'évolution de la technologie et des moyens modernes de communication permettent de mettre à la disposition des Utilisateurs un SI performant, nomade et accessible à partir de nombreux endroits différents. Ces nouveaux modes de communication rendus accessibles par le biais de ce SI, ne doivent pas entraîner de dérives. L'entreprise fait appel à l'autonomie et la responsabilité de chaque Utilisateur pour que l'utilisation professionnelle de ces outils s'inscrive dans le cadre de la durée légale du travail et notamment des durées maximales de travail et repos obligatoires.

Cette Charte s'applique que le SI soit utilisé dans les locaux de l'entreprise, lors de déplacements professionnels ou pour les Utilisateurs en « home Office ».

3. Gestion des départs des collaborateurs

Lors de son départ de l'entreprise, l'utilisateur doit remettre, à son manager et en bon état de fonctionnement, l'ensemble des moyens informatiques et de communication électronique mis à sa disposition dans le cadre de ses fonctions (ordinateur, périphériques, mobiles, supports de stockages …).
Le manager est responsable de cette restitution auprès du service Informatique.

Les codes d'accès aux SI et à la messagerie seront supprimés au départ du collaborateur.

C. Confidentialité

1. Confidentialité des identifiants et mots de passe

Pour l'accès à certains éléments du SI (ouverture de session, messagerie électronique, certaines applications), tout Utilisateur est doté d'un identifiant et d'un mot de passe qui lui sont personnels et doivent être gardés confidentiels.

Le mot de passe doit être mémorisé par l'Utilisateur **et ne pas être conservé par écrit ou dans un fichier**. Il peut également être stocké dans un gestionnaire de mots de passes fourni par le groupe PBM ou validé par ce dernier. Il ne doit pas être transmis à des tiers ni être aisément accessible. Il est interdit de l'utiliser hors du cadre professionnel de l'entreprise. Toute connexion effectuée en utilisant son identifiant et son mot de passe sera réputée avoir été effectuée par l'Utilisateur. Le mot de passe doit être saisi par l'Utilisateur à chaque ouverture de session et ne pas être conservé en mémoire dans le SI. Le mot de passe choisi par l'Utilisateur doit respecter un certain degré de complexité et être modifié régulièrement. Des consignes de sécurité complémentaires sont élaborées par le Service Informatique afin de recommander les bonnes pratiques en la matière.

Les Utilisateurs ne sont pas autorisés à utiliser les comptes informatiques d'autres Utilisateurs sans leur accord ni à tenter de masquer leur véritable identité. Le non-respect de ces règles est susceptible d'engager la responsabilité de l'Utilisateur, notamment lorsqu'il a communiqué ses identifiant et mot de passe à un tiers.

2. Protection des informations confidentielles

Il est demandé à l'Utilisateur :

- D'informer le Service informatique, dans les plus brefs délais et par tous les moyens, de la perte ou du vol d'un élément du SI ;
- De veiller à respecter la confidentialité des informations et des données contenues dans le SI et d'alerter le Service Informatique dans les plus brefs délais et par tous moyens en cas de menace pour l'intégrité du système ou des données Conservées ;
- En cas d'absence, même temporaire, de verrouiller l'accès au matériel qui lui est confié, dès lors que celui-ci contient des informations à caractère professionnel ;
- De veiller au respect de la confidentialité des informations en sa possession et à la réglementation applicable en matière de protection de la vie privée et du secret des correspondances.

En effet, dans le cadre de ses activités professionnelles, chaque Utilisateur est amené à accéder à des informations confidentielles, entendues comme tous documents, données et informations, de quelque nature que ce soit, notamment commerciale, financière, stratégique, technique, à caractère personnel ou autres, communiquées par écrit ou par oral, pour lesquelles il est indiqué qu'elles ont un caractère confidentiel ou qui doivent être raisonnablement considérées comme telle par l'Utilisateur qui les reçoit compte tenu de leur nature.

Tous les e-mails envoyés par les sociétés du groupe et toutes les informations transmises via Internet comportent la clause de confidentialité.

Chaque Utilisateur a été informé que toute violation du présent engagement l'expose notamment à des actions et sanctions disciplinaires et pénales conformément aux dispositions légales en vigueur.

3. Communication sur les réseaux sociaux

Sauf accord écrit de la direction ou du service communication, il n'est pas autorisé de communiquer sur les réseaux sociaux au nom du Groupe PBM et ses entreprises, ou sur des sujets concernant le Groupe PBM et ses entreprises.

D. Données à caractère personnel

Si les Utilisateurs sont amenés à accéder à des données à caractère personnel, ils reconnaissent la confidentialité desdites données et s'engagent par conséquent, conformément au Règlement Général sur la Protection des Données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin de protéger la confidentialité des informations auxquelles ils ont accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à les recevoir.

Ils s'engagent en particulier à :
- ne pas utiliser les données auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir la communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de leurs fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- s'assurer, dans la limite de leurs attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de leurs fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données ;
- et, d'une manière générale, respecter l'ensemble des règles et principes concernant les Données Personnelles de l'entreprise

III. UTILISATION COURANTE & PROFESSIONNELLE DU SI ET DES SERVICES INTERNET

A. Dispositions générales

L'entreprise fournit un accès au SI et aux Services Internet pour des besoins uniquement professionnels et légitimes, de manière générale et dans les conditions plus amplement définies ci-dessous :

B. Règles spécifiques à l'utilisation d'Internet

Dans le cadre de leurs activités, les Utilisateurs peuvent avoir accès à Internet pour un usage professionnel. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le Service Informatique.

En tout état de cause, sont interdit(e)s :

- La consultation de sites Internet, le téléchargement et/ou la recherche d'informations dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou au respect des droits des personnes (contenu raciste, diffamatoire, pornographique, discriminatoire notamment au regard de la race, l'origine nationale, le sexe, la religion, les opinions politiques, les origines sociales, l'âge, la santé ou le handicap) et de la vie privée ;
- La connexion à des sites Internet et/ou le téléchargement de jeux en ligne, loteries en ligne ;
- L'accès à des sites de téléchargement illicite de logiciels et d'œuvres protégés par le droit de la propriété intellectuelle ;
- Le téléchargement ou l'exécution à distance de logiciels, ou œuvres, mêmes licites.

Concernant l'utilisation des médias sociaux, que ce soit à partir du SI ou des Services Internet ou d'un matériel personnel, l'Utilisateur s'engage à respecte les principes énoncés dans le guide d'utilisation des Réseaux Sociaux figurant en Annexe.

C. Règles spécifiques à l'utilisation de la messagerie électronique

Chaque Utilisateur dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique qui lui est attribuée par le Service Informatique.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spams, les contrôles réalisés sont automatiques.

Une signature électronique ainsi que le format du corps du mail sont automatiquement appliqués lors de la création d'un nouveau message. Ils ne doivent en aucun cas être remplacés.

Il est par ailleurs précisé qu'il est strictement interdit :
- d'envoyer des e-mails aux médias, sans mandat exprès et préalable ;
- d'envoyer des e-mails chainés et/de télécharger des logiciels de messagerie en ligne ou de discussion groupée.

Pour des raisons techniques, le nombre et le type des pièces jointes peuvent être limités par le Service Informatique pour éviter l'engorgement du système de messagerie. L'utilisateur doit donc s'assurer qu'il envoie des pièces avec une taille minimale et doit privilégier l'utilisation de systèmes alternatifs d'envoi validés par PBM Groupe, par exemple : lien hypertexte vers un stockage en ligne, SharePoint ou OneDrive. En cas d'envoi particulièrement volumineux, il est nécessaire d'en informer au préalable le Service Informatique afin que ce dernier prenne les dispositions nécessaires.

D. Règles spécifiques à l'utilisation des réseau Wifi

- **Au sein de PBM Groupe** :
  2 types de réseaux Wifi sont mis à disposition des utilisateurs.
  - **Wifi Privé** : **Exclusivement** réservé pour les utilisateurs du groupes PBM ayant besoin d'accéder au SI. Le mot de passe wifi ne doit être communiqué à personne. Les smartphones ne doivent pas être connectés sur ce réseau.

  - **Wifi Public** : réservé pour des visiteurs (Fournisseurs, clients, intervenants), ou pour connecter les smartphones des utilisateurs. Cet accès est limité et ne donne l'accès qu'à Internet.

- **A l'extérieur de PBM Groupe**:
  Pour les utilisateurs nomades disposant d'un PC portables, il est recommandé d'utiliser **le partage de connexion de son smartphone** si cela est possible. Dans le cas contraire, si l'utilisateur doit se connecter à un réseau Wifi public (Hôtel, Train, Aéroport, etc…), il doit **systématiquement lancer sa connexion VPN** même pour de la simple consultation internet.

E. Règles spécifiques à la téléphonie

Dans le cadre de leurs activités, les Utilisateurs peuvent avoir accès au système de téléphonie fixe de l'entreprise et, dans certains cas, d'un téléphone et d'une ligne téléphonique mobile.

Les appels téléphoniques à caractère personnel des Utilisateurs sont tolérés, dans la limite d'une utilisation raisonnable, à condition de ne pas perturber le fonctionnement de l'entreprise et de respecter les principes posés dans la présente Charte et notamment de ne pas se livrer *via* le téléphone mis à leur disposition, à une activité susceptible de causer à l'entreprise un quelconque préjudice et/ou de porter atteinte à son image et sa réputation.

L'Utilisateur est répertorié dans le SI avec mention de son numéro de téléphone fixe professionnel, et, le cas échéant, de son numéro de mobile professionnel. Le traçage des communications peut être effectué dans le respect « des recommandations de la CNIL ».

F. Connexion de dispositifs externes au SI

L'entreprise met à disposition des Utilisateurs un système de connexion à distance, permettant dans certains cas l'accès aux applications utilisables uniquement sur le réseau interne de l'entreprise. Ce système bénéficie d'une politique de sécurité destinée à protéger l'entreprise contre les actions malveillantes pouvant lui porter préjudice. Lorsqu'il utilise une telle connexion, l'utilisateur doit se conformer strictement aux mêmes règles que celles auxquelles il est soumis lorsqu'il accède aux systèmes informatiques depuis les locaux de l'entreprise.

L'Utilisateur s'engage à informer l'entreprise dans les plus brefs délais et par tous moyens, de la perte ou du vol de son matériel personnel.

G. Règles en matière de cyberattaques

La pratique du phishing est désormais extrêmement répandue.
D'une manière générale, il est demandé aux Utilisateurs la plus grande vigilance et de:

- **Ne jamais ouvrir un fichier en pièce jointe d'un mail provenant de personnes inconnues ou inattendues et refuser toute sollicitation ;**
- **Se méfier lors d'échange d'informations sensibles par email, comme la validation d'un virement bancaire ou un changement de RIB…, vérifier systématiquement et rigoureusement si la source correspond bien à l'adresse d'une personne connue ;**
- **Ne pas répondre à des sollicitations inattendues de soi-disant dirigeants de l'entreprise même si le profil semble correspondre à celui de la personne connue, ces attaques dites « Attaques au Président » : se font par SMS ou autre messagerie (telle que Whatsapp…) avec des sujets comme « ultra confidentiel » ;**
- **Alerter immédiatement le Service Informatique en cas de doute,**

H. Impact environnemental

L'attention des Utilisateurs est attirée sur l'impact de nos activités sur l'environnement. En effet, notamment, la conservation déraisonnable de données et l'envoi de messages électroniques lourds. Aussi, vous êtes invités à procéder régulièrement à la suppression de vos messages non essentiels et à éviter au maximum l'envoi de pièces jointes en privilégiant le partage de document au travers des espaces collaboratifs (Teams).

IV. CONTROLES ET PROCÉDURES APPLICABLES

A. Contrôle du SI

Les Utilisateurs sont informés que l'entreprise a mis en place des dispositifs d'analyse et de contrôle du SI et des Services Internet (notamment messagerie électronique, accès à Internet et appels téléphoniques) notamment pour des raisons de maintenance et de gestion technique, pour assurer la sécurité du SI et pour se prémunir contre toute utilisation non conforme du SI et des Services Internet.

Ces dispositifs d'analyse et de contrôle impliquent l'enregistrement et l'archivage, des données suivantes dont la durée de conservation respectera les directives de la CNIL et ne seront pas disproportionnés.

- Celles relatives à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers. Ces enregistrements pourront être conservés en lieu sûr, sous format électronique.

- Celles relatives aux connexions entrantes et sortantes au réseau interne, à la messagerie (nombre d'envoi de messages, de messages reçus, fréquence, contenu des messages professionnels) et à Internet (durée de connexion et sites les plus visités) afin de détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités telles que la consultation de sites web ou le téléchargement de fichiers.

- Celles relatives aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles ainsi que celles relatives aux messages instantanés pour surveiller le volume d'activité, détecter des dysfonctionnements.

En cas de dysfonctionnement constaté par le Service Informatique dans le cadre de ce dispositif de contrôle général, il peut être procédé à un **contrôle ciblé et à une vérification de toute opération effectuée par un ou plusieurs Utilisateurs.**

B. Organisation en cas d'absence

Pour des besoins d'organisation interne, l'Utilisateur est informé qu'en son absence, il doit communiquer l'ensemble des mots de passe ayant servi à protéger des documents professionnels.

En cas de départ de l'entreprise avec dispense d'activité ou en cas d'absence prolongée d'un utilisateur, et dans la mesure où l'accès aux données accessibles via son mot de passe et son profil seraient nécessaires à la bonne marche de l'activité le Service informatique pourra unilatéralement réinitialiser le mot de passe de l'utilisateur et accéder aux données accessibles via le profil de l'utilisateur. La direction du Services informatique sera seule

habilitée à procéder ou à faire procéder à la réinitialisation des mots de passe d'un utilisateur.

V. SANCTIONS

Le manquement aux règles et mesures de sécurité de la présente Charte et de ses annexes est susceptible d'engager la responsabilité de l'Utilisateur et d'entraîner à son encontre une sanction disciplinaire pouvant aller jusqu'au licenciement.

En cas de non-respect par l'Utilisateur des droits des tiers ou des règles légales et réglementaires en vigueur, L'entreprise pourra appeler celui-ci en garantie, conformément à la législation et dans le respect des procédures applicables suite à toute procédure civile engagée à son encontre. En outre, la responsabilité pénale de l'Utilisateur pourra être engagée directement et, en cas de condamnation par les juridictions compétentes, l'Utilisateur pourra être amené à réparer tout préjudice causé à un tiers.

Annexe 1 : Guide d'utilisation des Médias Sociaux

1. Préambule

Les réseaux sociaux **externes** (type LinkedIn, Facebook, Twitter, Instagram etc.) (ci-après, les « Réseaux Sociaux ») représentent pour chacun d'entre nous une opportunité d'échanges avec ses collègues et ses contacts extérieurs à l'entreprise. Toutefois, il est primordial d'être vigilant dans l'utilisation faite de ces Réseaux Sociaux, notamment lorsqu'il est fait référence à L'entreprise (groupe et filiales), à ses dirigeants, à ses marques et à ses produits. En effet, l'utilisation des Réseaux Sociaux par les collaborateurs peut engendrer des risques potentiellement graves pour l'entreprise et sa réputation, susceptibles d'engager leur responsabilité personnelle ou celle des dirigeants de l'entreprise. Ces risques peuvent prendre la forme de « fuites » d'informations sensibles, d'atteinte à l'image de personnes physiques, de PBM Groupe, et/ou de ses produits, de violation des droits de propriété intellectuelle de PBM Groupe et/ou de tiers, de menaces pour la sécurité des systèmes d'information de l'entreprise etc…

Ces risques sont parfaitement évitables dès lors que chacun fait preuve de bon sens et s'engage à respecter un certain nombre de règles simples, énoncées dans le présent document. En cas de doute sur le bon comportement à tenir, chaque collaborateur doit prendre contact avec son manager afin de lui exposer la situation et prendre avec lui les décisions qui s'imposent. Le service communication est également à votre disposition pour vous aider à adopter le bon comportement face à une situation particulière. **Ce guide a pour objectif de décrire les bonnes pratiques permettant d'utiliser ces moyens de communication en toute sécurité (ci-après, le « Guide »).**

2. Eviter toute confusion entre vous et l'entreprise

Sur les Réseaux Sociaux, il est plus difficile d'identifier la limite entre vie personnelle et vie professionnelle. En communiquant des informations, en vous identifiant en tant que collaborateur de l'entreprise sur un réseau social (par exemple, en utilisant votre adresse électronique professionnelle), il existe un risque que vous-même et / ou vos propos soient associés à l'entreprise.

- Si vous utilisez les Réseaux Sociaux à titre personnel :

n'utilisez pas votre adresse professionnelle ni les noms ou les logos de l'entreprise, des sociétés de PBM groupe, et/ou de ses marques ;

si vous êtes amenés à vous exprimer à propos de l'entreprise et notamment de ses projets, méthodes, savoir-faire, technologies ou services, indiquez clairement que vous travaillez pour l'entreprise mais que vous vous exprimez en votre nom propre et non au nom et pour le compte de l'entreprise et que vos propos ne reflètent que votre opinion personnelle, en aucun cas celle de l'entreprise.

- Si vous utilisez les Réseaux Sociaux à titre professionnel :

l'utilisation des Réseaux Sociaux doit s'effectuer dans le respect du présent Guide, des principes éthiques de l'entreprise et de l'ensemble des réglementations en vigueur. Toute discussion ou publication sur ces Réseaux Sociaux doit être faite en conformité avec la Charte et le présent Guide. Vous n'êtes autorisé à vous exprimer au nom de l'entreprise

et/ou de ses filiales et/ou à ouvrir un compte sur les Réseaux Sociaux à titre professionnel qu'à condition d'avoir obtenu en raison de la nature de la fonction exercée au sein de l'entreprise, une autorisation préalable et écrite soit du Directeur Général, soit du service Communication. Seules les personnes habilitées à être les porte-paroles officiels de l'entreprise sont identifiées et formées pour cela.

3. Être responsable des propos tenus sur les Réseaux Sociaux

Vous êtes responsable des propos que vous tenez et des contenus que vous diffusez sur les Réseaux Sociaux. Vous pouvez donc faire l'objet de poursuites judiciaires si vous tenez des propos pouvant être de nature à porter atteinte à la dignité et à la personnalité notamment tous propos pouvant être considérés comme diffamatoires, injurieux, discriminatoires, racistes, incitatifs à la haine ou à la violence, négationnistes ou tout autre contenu susceptible de porter atteinte aux bonnes mœurs ou à l'ordre public ou portant atteinte à la vie privée d'un tiers ou si vous diffusez des contenus illicites. Vous vous engagez à ne pas poster de contenu et à ne pas divulguer d'informations susceptibles de nuire à l'intérêt et la réputation de l'entreprise ou de ses collaborateurs (notamment leur vie privée).

Vous devez garder à l'esprit que toute information diffusée, même dans un cadre privé restreint, via les Réseaux Sociaux peut tomber dans un espace public numérique qui échappe au contrôle de son émetteur et qu'il est très difficile de retirer des informations des Réseaux Sociaux après publication. Aussi, ayez à l'esprit que tout ce qui est publié sur les Réseaux Sociaux peut avoir un impact sur vous, vos collègues, vos contacts extérieurs ou sur l'entreprise.
En outre, les éléments publiés peuvent constituer des commencements de preuve à vous opposer dans le cadre de procédures judiciaires éventuelles.

4. Ne pas divulguer d'informations confidentielles

Vous ne devez en aucun cas communiquer d'informations confidentielles relatives à l'entreprise, ses projets, ses marques ou ses produits. Les informations confidentielles désignent tous les documents, données et informations, de quelque nature que ce soit, quelques soient leurs supports, notamment commerciale, financière, stratégique, technique, à caractère personnel ou autres, communiquées par écrit (sur un support tangible ou intangible) ou par oral, pour lesquels il est indiqué qu'elles ont un caractère confidentiel ou qui doivent être raisonnablement considérées comme telles par l'Utilisateur qui les reçoit compte tenu de leur nature (ci-après « Informations Confidentielles »).

Veillez également à vérifier les arrière-plans des photos ou vidéos que vous postez sur les Réseaux Sociaux afin de vous assurer qu'ils ne contiennent pas d'Informations Confidentielles ou sensibles ou tout autre élément dont la divulgation pourrait être préjudiciable pour l'entreprise.

Si vous n'êtes pas sûr de la nature d'une information, abstenez-vous de la publier et prenez conseil auprès de votre manager.

5. Être respectueux des droits de propriété intellectuelle/droit à l'image de tiers

Lorsque vous utilisez les Réseaux sociaux, veillez à respecter les droits de propriété intellectuelle des tiers et ceux de l'entreprise ainsi que le droit à l'image des personnes physiques.
Lorsque vous intervenez à titre professionnel sur les Réseaux Sociaux et que vous publiez des éléments susceptibles d'être protégés par des droits de propriété intellectuelle (photos, vidéos, marques, logos, musiques, dessins …), assurez-vous impérativement que vous

détenez les droits de reproduire ces éléments. Par ailleurs, vous devez veiller à respecter scrupuleusement le droit à l'image de personnes physiques : par exemple, vous ne devez pas publier de photos ou de vidéos d'évènements professionnels représentant des personnes physiques sans avoir obtenu l'accord préalable de l'ensemble de ces personnes ainsi que celui de l'entreprise.

6. Faites preuve de prudence et de bon sens

Avant de publier des informations sur les Réseaux Sociaux, faites preuve de prudence et renseignez-vous sur les contenus que vous partagez, les personnes qui en sont les destinataires et sur le bien-fondé de la diffusion de ces informations. Rappelez-vous qu'il n'y a pas de garantie sur l'identité des personnes participant aux Réseaux Sociaux et qu'il est possible d'usurper l'identité d'une autre personne sur les Réseaux Sociaux à des fins de malveillance. Les Réseaux Sociaux constituent l'une voies privilégiées de l'espionnage économique. Soyez également vigilant aux données à caractère personnel vous concernant que vous diffusez sur les Réseaux Sociaux. De telles informations peuvent être reprises et diffusées de manière plus large auprès de tiers.

7. Être responsables et constructifs

Pour une discussion constructive et propice à la liberté d'expression, évitez les provocations et les conflits. Restez respectueux, bienveillant et courtois, notamment vis-à-vis des consommateurs de nos produits, de vos collègues ou des personnes qui ont une sensibilité, des valeurs ou des coutumes différentes. Faites preuve de réserve et de proportion quant à vos opinions, croyances notamment religieuses, philosophiques, politiques. Assurez-vous que les informations que vous communiquez sont correctes, fiables et exactes. Chacun des commentaires postés sur les Réseaux Sociaux doit respecter les règles de bon sens et de politesse et doit être modéré et proportionné.

8. Devoir d'alerte

Les collaborateurs sont susceptibles d'être contactés à propos de l'entreprise via leurs réseaux sociaux personnels, sur des problématiques notamment de recrutement, de recueil d'avis sur l'entreprise ou sur les produits commercialisés. Le collaborateur doit remonter à son manager tout sujet, incident, information erronée sur l'entreprise ou ses services, propos diffamatoires (sans que cette liste soit exhaustive) afin que l'entreprise puisse, si besoin, mettre en œuvre la réaction adaptée.

Tout collaborateur ayant des questions sur le présent document, son interprétation ou son étendue, ou des difficultés dans une situation particulière, à discerner le comportement approprié, ne doit pas hésiter à en référer à son manager ou son référent RH

Annexe 2 : Guide d'utilisation du SI l'entreprise en mobilité

Les moyens informatiques et de communication électroniques dits « nomades » sont mis à disposition de l'utilisateur selon les besoins des fonctions et missions. On entend par « nomade » tous les moyens techniques (ordinateurs portables, téléphones mobiles, clé 4G, disques durs externes, …) qui peuvent être utilisés hors des murs de l'entreprise.
Lorsque ces matériels sont utilisés hors des murs de l'entreprise, l'utilisateur en assure la garde et la responsabilité. Il procède lui-même ou assiste l'entreprise selon les cas à toutes les démarches (dépôt de plainte pour vol, déclaration de perte, déclaration assurance, …) rendues nécessaires à la suite d'un incident de quelque nature que ce soit.

L'utilisation de moyens informatiques et de communication électronique nomades impose à l'utilisateur un niveau de surveillance et de confidentialité renforcé.

Il doit notamment veiller à ce que des tiers non autorisés ne puissent accéder à ces moyens et éléments accessoires, les utiliser ou accéder à leurs contenus.
En cas d'incident avéré mais aussi en cas de doute, il doit immédiatement en aviser son manager et les Services Informatiques de l'entreprise.

- **Spécificité des téléphones portables professionnels**

L'entreprise a mis à votre disposition un téléphone portable afin de mener au mieux votre mission. Cet outil de travail est donc placé sous votre responsabilité et ne doit jamais être laissé dans un quelconque endroit où il pourrait être volé. Il vous est ainsi interdit, entre autres, de le laisser dans un véhicule, même bien dissimulé.

1. **Principes Généraux**

Ce téléphone portable vous est fourni pour des raisons strictement professionnelles. Son utilisation à des fins personnelles est tolérée, sans surcoûts ou surcharge de réseau pour l'entreprise.

De plus, il est rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel.

L'utilisateur est informé qu'un journal des communications, entrantes et/ou sortantes, est accessible par la Direction des Services Informatiques s'agissant tant de la téléphonie fixe que mobile. Les utilisateurs sont informés que les relevés de communication peuvent faire l'objet d'un contrôle.

Les applications mises en place sur les smartphones peuvent permettre aux utilisateurs de se géolocaliser.
Cependant, nous recommandons fortement de ne pas mettre en œuvre ces processus de géolocalisation et les utilisateurs sont informés qu'en cas de géolocalisation, l'entreprise pourra avoir accès à cette information.

2. Engagement de l'utilisateur

L'utilisateur s'engage en outre à :

- Prévenir sans délai en cas de perte, vol ou faille de sécurité ;
- Mettre en œuvre tous les moyens de sécurité prévus par les fonctionnalités du smartphone et qui sont demandées et notamment le code d'accès ;
- Se déconnecter de toutes applications après usage et ne pas rester connectés par défaut ;
- Être vigilants vis à vis des données contenues dans le smartphone.

La vigilance de l'utilisateur est attirée sur le fait qu'un SMS ou l'utilisation de messages instantanés tels que chat n'a pas la même portée qu'un courrier manuscrit ou électronique.

3. Utilisation personnelle du téléphone

Les surcoûts pour l'entreprise engendrés par l'utilisation de la téléphonie à des fins personnelles devront être remboursés par les utilisateurs concernés. Il s'agit tout particulièrement des appels à des numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique.

L'entreprise, à travers un logiciel de gestion de flotte mobile, pourra limiter et contraindre l'utilisation du téléphone.

Toutefois, seule la Direction de l'entreprise, pourra avoir accès aux numéros détaillés, permettant d'identifier les interlocuteurs d'un utilisateur, et seulement en cas de différend avec lui.

4. Guide pour un bon usage de l'utilisation du téléphone professionnel au volant

Vous vous engagez à :

1. Utiliser le téléphone professionnel au volant (dans le cadre de vos déplacements professionnels et domicile-travail) uniquement sous certaines conditions :
    - Je n'utilise que des dispositifs de téléphonie autorisés par la loi ;
    - Je ne passe que des appels urgents, j'en limite la durée au strict minimum et je remets les autres à plus tard ;
    - En cas d'appel entrant, j'avertis immédiatement mon interlocuteur que je suis au volant et j'écourte la conversation ;
    - Je ne manipule pas mon téléphone, par exemple, pour consulter mes mails ou messages, que lorsque je suis à l'arrêt à un endroit sécurisé (pas au feu rouge ou dans les files), conformément à la loi.

2. Si malgré nos recommandations, vous utilisez le téléphone comme GPS de navigation routière, voici les conditions à respecter :
    - Je désactive les autres fonctionnalités de mon téléphone, ce qui me permet de ne pas être distrait par d'éventuels messages et notifications entrants ;
    - J'utilise un support adapté ;
    - Je démarre la navigation avant de prendre la route ;
    - Je désactive la fonction GPS en fin de trajet.

3. Même quand je ne suis pas au volant, écourter une conversation téléphonique avec un collègue ou un proche si ce dernier est au volant.