CHARTE D'UTILISATION DU SYSTÈME D'INFORMATION ET DE COMMUNICATION

Préambule

SMATCH CONNECT met en œuvre un système d'information et de communication indispensable à la réalisation de ses missions. Ce système comprend notamment les équipements informatiques, les réseaux internes et externes, les outils collaboratifs, les moyens de télécommunication, les logiciels métiers, ainsi que les applications de gestion et de suivi de l'activité, dont le CRM actuellement utilisé.

Les utilisateurs accèdent à ces ressources et sont tenus d'en faire un usage conforme aux règles de sécurité, de confidentialité et de bonne conduite définies par la présente charte. Celle-ci vise à prévenir les risques liés à l'utilisation du système d'information, à protéger les données traitées, et à garantir la conformité aux obligations légales, notamment celles issues du Code du travail, du RGPD, de la loi Informatique et Libertés, ainsi que de la jurisprudence en vigueur.

La présente charte s'impose à tout utilisateur et constitue un document interne de référence. Elle est annexée au règlement intérieur lorsqu'il existe et communiquée individuellement à chaque salarié.

Article 1 – Champ d'application

1.1 Utilisateurs concernés

La présente charte s'applique à l'ensemble des personnes ayant accès au système d'information et de communication de SMATCH CONNECT, quel que soit leur statut : salariés, mandataires sociaux, intérimaires, stagiaires, prestataires, consultants externes, visiteurs autorisés.

Tout utilisateur permettant l'accès à un tiers doit s'assurer que celui-ci respecte les règles de la présente charte.

1.2 Définition du système d'information

Le système d'information et de communication comprend notamment : postes de travail (fixes et nomades), serveurs, réseaux, téléphonie, logiciels, CRM, outils collaboratifs, bases de données, documents électroniques, supports amovibles et tout matériel connecté au réseau.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés connecté au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'entreprise

L'utilisateur ne dispose que d'un droit d'usage, lequel s'éteint automatiquement à son départ.

1.3 Articulation avec d'autres dispositifs

La présente charte est, sans préjudice des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives, compatible avec l'organisation d'élections par voie électronique ou la mise en télétravail.

Article 2 – Accès, confidentialité et sécurité

2.1 Accès aux ressources

L'accès aux ressources informatiques est attribué individuellement et limité aux besoins professionnels. Le service informatique assure la maintenance, la supervision et la sécurité du système, dans le respect de l'article L1222-4 du Code du travail. Il est assujetti au devoir de réserve et est tenu de préserver la confidentialité des données qu'il est amené à connaître dans le cadre de leurs fonctions

2.2 Identifiants et mots de passe

Les identifiants et mots de passe sont strictement personnels. Ils permettent notamment de contrôler l'activité des utilisateurs mais aussi d'assurer la confidentialité et la sécurité des données.

L'utilisateur s'engage à ne jamais les communiquer, à respecter les règles de complexité, à activer l'authentification multi-facteur lorsque disponible. Lorsqu'ils sont choisis par l'utilisateur, il s'engage aussi à les modifier régulièrement.

2.3 Règles générales de sécurité

L'utilisateur doit notamment :

- Signaler tout dysfonctionnement, violation ou tentative de violation suspectée de son compte réseau,
- Verrouiller son poste,
- Ne pas installer de logiciels non autorisés,
- Ne pas modifier la configuration du matériel,
- Ne pas accéder à des données non destinées, respecter les règles de copie et d'exportation de données.
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur.
- Ne pas masquer sa véritable identité.
- Ne pas usurper l'identité d'autrui
- Ne pas copier, modifier, détruire les logiciels propriétés de l'entreprise.
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas.
- Toute copie de données sur un support externe est soumise à l'accord du supérieur hiérarchique

Les intervenants externes doivent contractuellement s'engager à respecter la présente charte.

2.4 Matériel informatique et équipements nomades

Les équipements nomades (tous les moyens techniques mobiles comme ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc.) doivent être protégés physiquement, chiffrés lorsque possible, verrouillés automatiquement, déclarés en cas de perte ou vol. Tout matériel prêté fait l'objet d'un registre de suivi.

L'utilisateur est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements.

Article 3 – Protection des ressources et des données

SMATCH CONNECT met en œuvre les moyens humains et techniques nécessaires pour assurer la sécurité du système d'information et de communication.

A ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs.

Il relève également de la responsabilité de l'entreprise de prévoir un plan de continuité du service.

L'utilisateur est responsable des ressources confiées et doit protéger les données, effectuer les sauvegardes nécessaires, respecter les droits de propriété intellectuelle et ne pas utiliser les outils à des fin

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication s préjudiciables.

Article 4 – Accès à Internet

L'accès à Internet est autorisé dans le cadre professionnel.

Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le service informatique. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites, est interdite sauf autorisation expresse de la Direction.

Sont interdits : contenus illicites, violents, haineux, pornographiques, téléchargements non autorisés, activités portant atteinte à l'image de l'entreprise, leur responsabilité pénale pouvant être engagée.

Une utilisation personnelle est tolérée si elle est raisonnable, non illicite et ne nuit pas au travail ni à l'intérêt ou à la réputation de l'entreprise.

Article 5 – Messagerie électronique

5.1 Principes généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. La messagerie professionnelle doit donc être utilisée avec prudence notamment afin de ne pas engager la responsabilité civile ou pénale de l'entreprise et/ou de l'utilisateur.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer le service informatique des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

En cas d'envoi à une liste de diffusion, il est important de vérifier la liste des abonnés à celle-ci, l'existence d'archives accessibles par le public et les modalités d'abonnement.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel. Les messages doivent, dans ce cas, être cryptés, conformément aux recommandations du service informatique.

Les utilisateurs doivent veiller à mettre en place un répondeur automatique pour toutes absences supérieures à 3 jours.

5.2 Limites techniques

Le service informatique peut limiter la taille des pièces jointes, le nombre de destinataires, la durée de conservation des messages.

Les messages électroniques sont conservés pendant une durée limitée au-delà de laquelle, ils sont automatiquement archivés

5.3 Utilisation personnelle

Les messages personnels sont tolérés à condition de respecter la législation en vigueur et de respecter les principes posés dans la présente charte.

Messages reçus comme envoyés doivent être identifiés comme « PRIVÉ » et rangés dans un dossier dédié. À défaut, ils sont présumés professionnels.

5.4 Suppression du compte

En cas de départ, le compte est supprimé dans un délai raisonnable. Les messages professionnels peuvent être consultés pour assurer la continuité du service et la défense de la société dans le cadre d'un contentieux. Les messages personnels identifiés comme tels ne peuvent être consultés.

Article 6 – Réseaux sociaux

L'utilisateur doit respecter la loi, les CGU des plateformes et l'image de l'entreprise. Sont interdits : propos diffamatoires, discriminatoires, injurieux, incitant à la haine, portant atteinte à l'entreprise ou à ses clients.

Article 7 – Données personnelles

Les traitements mis en œuvre respectent le RGPD, la loi Informatique et Libertés et les recommandations CNIL. Les utilisateurs doivent respecter les droits des personnes (accès, rectification, opposition, effacement).

Quand leurs fonctions le nécessiteront (RH, consultants en recrutement, ...) les utilisateurs suivront le MOOC de la CNIL sur le RGPD

Article 8 – Contrôle des activités

8.1 Contrôles automatisés

Les logs peuvent être collectés pour assurer la sécurité, détecter les anomalies, prévenir les intrusions, garantir la conformité.

L'activité du système d'information et de communication est surveillées et sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications suppression de fichiers ;
- aux connexions entrantes et sortantes au réseau interne, à la messagerie et à internet, pour 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.

Il peut également être mis en place des filtrages des sites Internet, l'élimination des courriels non sollicités, un blocage de certains protocoles (peer to peer, messagerie instantanée).

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur. Ces traitements sont réalisés conformément au RGPD et portés à la connaissance des salariés.

8.2 Contrôles manuels

Les fichiers identifiés comme « PERSONNEL » ne peuvent être ouverts qu'en présence du salarié ou celui-ci dûment appelé, sauf risque grave. Les fichiers non identifiés comme personnels sont présumés professionnels.

Article 9 – Départ de l'utilisateur

L'utilisateur restitue l'ensemble du matériel.

Il doit préalablement effacer ses fichiers et données privées

Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ, dans les conditions ci-avant.

Les données professionnelles restent la propriété de l'entreprise.

Article 10 – Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication. De plus,tout manquement peut entraîner des sanctions disciplinaires proportionnées à la gravité des faits dans le respect des procédures prévues par la loi et le règlement intérieur.

Article 11 – Information des salariés

La charte est communiquée individuellement à chaque salarié et affichée publiquement en annexe du règlement intérieur.

Article 12 – Entrée en vigueur

La présente charte entre en vigueur à compter du 1er Mars 2025

Versailles, le 26/02/2025,
Maxime LACOUR
Président