DOCUMENT 01

Charte informatique

Règles d'usage du système d'information, des outils numériques et des données de l'entreprise.

Entreprise		Date		Version	

Avant diffusion — à faire par le dirigeant
• Si vous avez un règlement intérieur (obligatoire à partir de 50 salariés), annexez-y la charte. • Si un CSE existe, informez-le et consultez-le. • Informez individuellement chaque salarié (signature ou remise contre émargement). • Précisez ce qui est journalisé ou contrôlé (transparence exigée par la CNIL). • Supprimez les articles qui ne s'appliquent pas à votre entreprise.

Préambule et champ d'application

La présente charte définit les règles d'utilisation des ressources informatiques de **[Nom de l'entreprise]** (ordinateurs, smartphones, messagerie, réseau, logiciels, services en ligne, données) par toute personne y accédant : salariés, stagiaires, alternants, intérimaires et prestataires. Elle vise à protéger les données de l'entreprise, de ses clients et de ses salariés, ainsi que la continuité de l'activité. Elle s'ajoute aux obligations légales et au règlement intérieur.

Article 1 — Accès et mots de passe

- Chaque utilisateur dispose d'un **compte personnel et nominatif**. Il ne le prête ni ne le partage, y compris avec un collègue ou la direction.
- Les mots de passe comptent **au moins 12 caractères** (ou une phrase de passe), sont uniques pour chaque service et conservés dans le **gestionnaire de mots de passe** fourni par l'entreprise. Ils ne sont ni écrits sur papier ni envoyés par message.
- L'**authentification multifacteur** est obligatoire dès qu'elle est disponible (messagerie, VPN, outils métier, administration).
- Tout poste laissé sans surveillance est **verrouillé** (Windows+L / Ctrl+Cmd+Q) ; le verrouillage automatique ne doit pas être désactivé.

Article 2 — Postes de travail et matériel

- Le matériel fourni est destiné à un usage professionnel. Il est tenu à jour : **les mises à jour ne sont pas repoussées** au-delà de quelques jours.
- L'antivirus/EDR et le chiffrement du disque ne peuvent être ni désactivés ni contournés. Aucun logiciel n'est installé sans validation du référent informatique.
- Les supports amovibles (clés USB, disques externes) d'origine inconnue ne sont jamais branchés. Les données sensibles ne sont copiées que sur des supports chiffrés fournis par l'entreprise.
- **La perte ou le vol** d'un équipement est signalé immédiatement au référent, de jour comme de nuit.

Article 3 — Messagerie et Internet

- La messagerie professionnelle est réservée à l'activité de l'entreprise ; un usage personnel occasionnel et raisonnable est toléré s'il ne gêne pas le travail et n'expose pas l'entreprise.
- **Vigilance face au phishing** : vérifier l'expéditeur, ne pas cliquer dans l'urgence, ne pas ouvrir de pièce jointe inattendue, ne jamais communiquer un mot de passe ou un code. En cas de doute : ne rien faire et **signaler au référent**.

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

- Toute demande inhabituelle de virement ou de modification de coordonnées bancaires est **confirmée par un second canal** (appel à un numéro connu) avant exécution.
- Les messages personnels doivent être identifiés comme tels (objet « Personnel » ou dossier dédié) pour bénéficier du secret des correspondances.

Article 4 — Protection des données

- Les données sont classées en trois niveaux : **Public**, **Interne**, **Confidentiel** (données clients, RH, financières, secrets d'affaires). Les données confidentielles ne sont partagées qu'avec les personnes qui doivent en connaître.
- Les fichiers professionnels sont enregistrés **uniquement dans les espaces autorisés** (serveur, cloud de l'entreprise). Les services de stockage ou de transfert personnels (messagerie perso, cloud perso) sont interdits pour des données professionnelles.
- Les données personnelles sont traitées dans le respect du RGPD et du registre des traitements. Toute nouvelle utilisation de données personnelles est signalée au référent RGPD avant sa mise en œuvre.
- Les documents papier confidentiels sont rangés sous clé et détruits (broyeur) lorsqu'ils ne sont plus utiles.

Article 5 — Télétravail et déplacements

- Hors des locaux, on utilise de préférence le matériel de l'entreprise et la connexion sécurisée (VPN ou accès protégé) pour accéder aux ressources internes.
- Les Wi-Fi publics (gares, hôtels, cafés) ne sont pas utilisés sans VPN. Les écrans sont protégés des regards et les conversations confidentielles tenues à l'abri des oreilles.
- Le Wi-Fi du domicile est protégé (mot de passe robuste, chiffrement WPA2/WPA3, box à jour).

Article 6 — Équipements personnels (BYOD)

- L'usage d'un équipement personnel pour accéder à des données de l'entreprise n'est autorisé que si le référent l'a validé et si l'appareil est à jour, protégé par code et chiffré. L'entreprise peut effacer à distance ses seules données professionnelles.

Article 7 — Réseaux sociaux et intelligence artificielle générative

- Sur les réseaux sociaux, chacun s'abstient de divulguer des informations confidentielles et précise, si nécessaire, qu'il s'exprime à titre personnel.
- Il est **interdit de saisir dans un outil d'IA générative non validé** par l'entreprise des données clients, personnelles, financières, des codes sources ou tout élément confidentiel. Les résultats produits par une IA sont relus et vérifiés avant tout usage.

Article 8 — Signalement des incidents

- Tout incident ou doute (message suspect, comportement anormal d'un poste, perte d'équipement, erreur d'envoi de données, clic sur un lien douteux) est signalé **sans délai** à **[Nom du référent]** ([téléphone / e-mail]).
- Un signalement fait de bonne foi et rapidement ne donne lieu à **aucune sanction** : mieux vaut dix fausses alertes qu'un incident découvert trop tard.

Article 9 — Arrivée, changement de poste et départ

- Les droits d'accès sont attribués selon le poste et ajustés à chaque changement de fonction. À son départ, l'utilisateur restitue tout le matériel, les accès sont **désactivés le dernier jour** et les données professionnelles sont transmises à son responsable.

Article 10 — Contrôles et transparence

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

- L'entreprise peut mettre en place des mesures de sécurité et de journalisation (traces de connexion, filtrage Internet, antivirus) strictement proportionnées à l'objectif de sécurité et conformes à la loi. Les salariés en sont informés : **[préciser : journalisation des connexions, durée de conservation, finalité]**.
- Aucun dispositif de surveillance permanente et individualisée de l'activité n'est mis en œuvre. Les fichiers et messages clairement identifiés comme personnels ne sont consultés qu'en présence de leur propriétaire ou après l'avoir dûment appelé, sauf risque ou événement particulier.

Article 11 — Sanctions et entrée en vigueur

- Le non-respect de la présente charte peut constituer une faute et entraîner des sanctions disciplinaires dans le respect de la procédure légale. Elle entre en vigueur le **[date]** et peut être modifiée après information (et consultation le cas échéant) des représentants du personnel.

Engagement de l'utilisateur

Je reconnais avoir lu la charte informatique de **[Nom de l'entreprise]**, en avoir reçu un exemplaire et m'engage à la respecter.

Nom et prénom		**Fonction**	
Date		**Signature**	

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.