Charte d'utilisation des moyens informatiques et des outils numériques

[Modèle pour une entreprise de 20 salariés · à jour au 8 octobre 2026 : ligne à supprimer]

[Raison sociale], [forme juridique], [adresse du siège]

Version [1.0] du [date]

[Le cas échéant : avis du comité social et économique du [date] ·] communication à l'inspection du travail et diffusion au personnel le [date] · entrée en vigueur le [date, au moins un mois après ces formalités]

À lire avant d'utiliser ce modèle (page à supprimer)

Nous avons rédigé ce modèle chez KERIONIS, prestataire informatique à Crevin, en Ille-et-Vilaine. Il vise une entreprise fictive de 20 salariés : bureaux, postes Windows, Microsoft 365, quelques ordinateurs portables, télétravail partiel, smartphones professionnels et personnels, Wi-Fi invités, imprimante multifonction et prestataire d'infogérance. Il s'appuie notamment sur le Code du travail, le Code pénal, le RGPD, le règlement européen sur l'intelligence artificielle et les recommandations de la CNIL, de l'ANSSI et de Cybermalveillance.gouv.fr, dans leur état au 8 octobre 2026. Vous pouvez le reprendre et l'adapter librement.

L'adapter à votre entreprise. Remplacez le logo de la couverture par celui de votre entreprise, puis tout ce qui figure entre crochets et surligné. Supprimez les règles qui ne correspondent à aucun outil que vous utilisez et tranchez les options signalées (appareils personnels, filtrage des connexions sécurisées, campagnes d'hameçonnage simulé). Une charte ne vaut que si elle décrit ce que le système fait vraiment : les contrôles annoncés à l'article 20 et à l'annexe D doivent correspondre exactement aux outils en place. Votre prestataire informatique peut vous aider à les relever.

L'adopter dans les formes. Une charte qui fixe des règles et annonce des sanctions contient des « obligations générales et permanentes » en matière de discipline, au sens du Code du travail. Selon la lettre de l'article L1321-5, elle est alors soumise aux règles du règlement intérieur, même dans une entreprise de moins de 50 salariés qui

n'en a pas ; aucune décision publiée n'a encore tranché ce cas ; par prudence, suivez la procédure de l'article L1321-4 :

- avis préalable du comité social et économique, s'il existe (à partir de 11 salariés) ;
- diffusion au personnel par tout moyen (affichage, intranet, remise individuelle) ;
- communication à l'inspection du travail, en deux exemplaires, avec l'avis du CSE, en même temps que la diffusion ;
- entrée en vigueur au moins un mois après ces formalités ; toute modification suit le même chemin.

Le dépôt au greffe du conseil de prud'hommes n'est plus prévu par la loi depuis le 28 mai 2026, mais l'article R1321-2, qui l'organise, figure toujours comme en vigueur sur Légifrance. Par prudence, vous pouvez effectuer ce dépôt : tant que l'article R1321-3 n'est pas modifié, le délai d'un mois court à partir de la dernière des formalités de publicité et de dépôt. La voie la plus sûre, à faire valider par votre conseil, consiste à adopter un règlement intérieur, facultatif sous 50 salariés, et à y annexer la charte : une règle disciplinaire posée dans un document qui n'est ni un règlement intérieur ni une note de service régulièrement adoptée a déjà été jugée inopposable. À partir de 50 salariés, la charte constitue une adjonction au règlement intérieur, devenu obligatoire, et le CSE est en outre consulté sur les moyens de contrôle de l'activité. La signature individuelle de la charte n'est pas une condition de sa validité ; l'accusé de réception de l'annexe G sert de preuve que chacun en a eu connaissance.

Les documents qui restent à part. La charte ne remplace pas :

- la charte ou l'accord de télétravail (article L1222-9 du Code du travail, avec son propre avis du CSE) ;
- le contrat de sous-traitance avec votre prestataire informatique (article 28 du RGPD) ;
- le registre des traitements et le registre interne des violations de données, qui recense toutes les violations, même celles qui ne sont pas notifiées à la CNIL ;
- l'analyse d'impact relative à la protection des données si un dispositif surveille l'activité de façon constante, ou si vous utilisez un outil de filtrage de la navigation (serveur mandataire filtrant), a fortiori s'il examine le contenu des connexions sécurisées : la CNIL la conseille dans ce cas et recommande d'y associer le CSE, même quand ce n'est pas obligatoire ;
- l'information propre à la vidéosurveillance ou à la géolocalisation, si vous en utilisez ;
- l'information des visiteurs qui utilisent le Wi-Fi invités (la charte ne s'applique pas à eux).

Ce qu'il ne faut pas y ajouter. Pas de clause de remboursement du matériel perdu ou cassé : sauf faute lourde, la responsabilité pécuniaire d'un salarié envers son employeur ne peut pas être engagée. Pas d'amende ni de retenue sur salaire, pas de clause de neutralité générale, pas d'interdiction générale de s'exprimer sur son travail.

Ce document n'est pas un avis juridique. Faites relire votre version par votre conseil avant de l'adopter, et revoyez-la à chaque changement d'outil ou de réglementation, par exemple à la promulgation de la loi française de transposition de la directive NIS2, qui n'avait pas eu lieu au 8 octobre 2026.

Modèle proposé gratuitement par KERIONIS, Crevin (Ille-et-Vilaine) · 06 77 40 79 55 · contact@kerionis.fr · https://www.kerionis.fr/charte-informatique-entreprise

Sommaire

Préambule

1. Objet de la charte · 2. Champ d'application · 3. Définitions · 4. Principes généraux et usage personnel

5. Comptes, mots de passe et authentification · 6. Poste de travail et logiciels · 7. Messagerie électronique

8. Virements, coordonnées bancaires et fraude au président · 9. Internet et téléchargements · 10. Stockage, partage et sauvegarde des données

11. Données personnelles et informations confidentielles · 12. Intelligence artificielle · 13. Réseaux sociaux et expression en ligne

14. Matériel nomade et déplacements · 15. Télétravail · 16. Smartphones, tablettes et appareils personnels · 17. Réseau, Wi-Fi, objets connectés et imprimantes

18. Support informatique et prestataire · 19. Incidents de sécurité : signaler et réagir · 20. Administration du système d'information et contrôles

21. Absence et départ de l'utilisateur · 22. Droit à la déconnexion · 23. Logiciels, licences et propriété intellectuelle

24. Responsabilités et sanctions · 25. Signalements protégés et représentants du personnel · 26. Entrée en vigueur, diffusion et mise à jour

Annexes : A. Contacts utiles · B. Fiche réflexe en cas d'incident · C. Outils autorisés et sauvegardes · D. Information des utilisateurs sur les traitements de données · E. Rappels légaux · F. Engagements des administrateurs · G. Accusé de réception

Préambule

[Raison sociale] met à la disposition de son personnel des moyens informatiques et des outils numériques indispensables à son activité. Leur bon usage protège l'entreprise, ses clients, ses partenaires et ses salariés eux-mêmes : une erreur, un mot de passe partagé ou un message frauduleux suffit à bloquer l'activité ou à exposer des données.

La présente charte fixe les règles d'utilisation de ces moyens. Elle informe aussi chacun des contrôles mis en place pour assurer la sécurité du système d'information, de leurs limites et des droits dont il dispose. Elle comporte des obligations générales et permanentes en matière de discipline : à ce titre, elle a été [le cas échéant : soumise à l'avis du comité social et économique le [date],] communiquée à l'inspection du travail et portée à la connaissance du personnel le [date] par [affichage et publication sur l'intranet]. Elle entre en vigueur le [date]. [Si l'entreprise dispose d'un règlement intérieur : elle y est annexée et en fait partie.]

Les règles écrites au présent (« l'utilisateur verrouille sa session », « il est interdit de ») s'imposent à tous. Les phrases introduites par « il est recommandé » ou « de préférence » sont des recommandations. La charte est rédigée en français et tenue à la disposition de chacun sur [emplacement : intranet, dossier partagé].

Article 1. Objet de la charte

La charte a pour objet de définir les conditions d'utilisation des moyens informatiques et des outils numériques de l'entreprise, de préserver la sécurité et la disponibilité du système d'information, de protéger les données de l'entreprise et les données personnelles qu'elle traite, et d'informer les utilisateurs des contrôles qui peuvent être effectués et des garanties qui les encadrent.

Elle ne remplace ni le contrat de travail, ni la charte ou l'accord de télétravail, ni les documents d'information propres à d'autres dispositifs éventuels (vidéosurveillance, géolocalisation des véhicules), auxquels elle renvoie.

Article 2. Champ d'application

Personnes concernées. La charte s'applique à toute personne qui utilise les moyens informatiques de l'entreprise : salariés quel que soit leur contrat, apprentis, stagiaires, intérimaires, et toute personne autorisée à y accéder. Les prestataires extérieurs, dont le prestataire informatique, et leurs intervenants y sont tenus par une clause de leur contrat [à vérifier dans les contrats en place].

Moyens concernés. Elle couvre notamment les postes fixes et portables, les smartphones et tablettes fournis, les comptes et services en ligne (Microsoft 365, messagerie, Teams, OneDrive, SharePoint, logiciels métier, gestionnaire de mots de passe, VPN), le réseau filaire et Wi-Fi, les imprimantes et la téléphonie, ainsi que les appareils personnels lorsqu'ils sont autorisés à accéder aux données de l'entreprise.

Lieux et moments. Elle s'applique dans les locaux, en télétravail et en déplacement, dès lors que les moyens de l'entreprise sont utilisés.

Article 3. Définitions

- **Utilisateur** : toute personne visée à l'article 2.
- **Moyens informatiques** : les matériels, logiciels, comptes, services et réseaux visés à l'article 2.
- **Données de l'entreprise** : toute information, quel qu'en soit le support, détenue ou traitée par l'entreprise dans le cadre de son activité.
- **Données personnelles** : toute information relative à une personne physique identifiée ou identifiable, au sens du RGPD (clients, salariés, candidats, fournisseurs, prospects).
- **Référent informatique** : [nom et fonction], désigné par la direction pour relayer les règles de la charte, recevoir les signalements et les demandes des utilisateurs, et faire le lien avec le prestataire.
- **Prestataire** : [nom du prestataire informatique], chargé de l'administration et du support du système d'information, sous-traitant au sens de l'article 28 du RGPD.
- **Administrateur** : toute personne qui dispose de droits étendus sur le système d'information pour en assurer le fonctionnement et la sécurité.

Article 4. Principes généraux et usage personnel

Les moyens informatiques sont mis à disposition pour l'activité professionnelle. Chaque utilisateur en fait un usage loyal, conforme à ses missions, à la présente charte et aux lois en vigueur. Il est responsable de l'usage fait avec ses identifiants.

Un usage personnel ponctuel et raisonnable est toléré, en particulier de la connexion à internet et d'une messagerie personnelle consultée dans le navigateur (webmail), à condition de ne pas nuire à l'activité, à la sécurité du système ni à la bonne marche de l'entreprise, et de respecter les interdits de la charte. Les éléments personnels conservés sur les moyens de l'entreprise sont identifiés par la mention « Personnel » ou « Privé » dans l'objet du message ou dans le nom du fichier ou du dossier ; un classement dans « Mes documents » ou dans un dossier à ses initiales ne suffit pas. Tout élément qui n'est pas ainsi identifié est présumé professionnel. L'utilisateur ne stocke pas de volumes importants de fichiers personnels (photos, vidéos, musique) sur les moyens de l'entreprise.

Il est interdit d'utiliser les moyens de l'entreprise pour harceler, menacer, injurier, diffamer ou discriminer quiconque, pour tenir des propos ou adresser des contenus sexistes, pour consulter, conserver ou diffuser des contenus illicites, pour exercer une activité commerciale personnelle ou pour dénigrer l'entreprise par des propos injurieux, diffamatoires ou excessifs. Le harcèlement moral et le harcèlement sexuel sont interdits par le Code du travail et punis par le Code pénal, le harcèlement sexuel commis au moyen d'un outil numérique étant puni plus sévèrement (annexe E). Les contacts utiles en cas de harcèlement figurent en annexe A.

Article 5. Comptes, mots de passe et authentification

Chaque utilisateur dispose d'un compte nominatif. Il ne se connecte jamais avec le compte d'un collègue et ne laisse personne utiliser le sien. Une adresse commune (par exemple « accueil » ou « contact ») n'existe qu'avec l'accord de la direction, de préférence sous forme de boîte partagée, que chacun ouvre avec son propre compte, sans mot de passe commun ; ses accès sont tracés. Les droits d'accès de chacun sont limités aux besoins de son poste ; ils sont revus à chaque changement de fonction et au moins une fois par an.

L'utilisateur ne communique à personne son mot de passe ni ses codes de double authentification, et ne laisse personne utiliser sa clé de sécurité ni son application d'authentification, pas même à son responsable hiérarchique ou au support informatique ; le support ne les demande jamais. Il respecte les règles suivantes, issues des recommandations de la CNIL et de l'ANSSI :

- un mot de passe compte au moins 12 caractères mêlant majuscules, minuscules, chiffres et caractères spéciaux, ou au moins 14 caractères mêlant majuscules, minuscules et chiffres, ou une phrase de passe d'au moins 7 mots, sauf règle plus forte imposée par le système ; le code PIN lié à un appareil (Windows Hello, smartphone) suit les règles fixées par le prestataire ;
- le mot de passe maître du gestionnaire de mots de passe et ceux des comptes d'administration comptent au moins 15 caractères ;
- chaque service a son propre mot de passe, et un mot de passe professionnel n'est jamais utilisé pour un compte personnel ;
- un mot de passe ne contient ni nom, ni prénom, ni date de naissance, ni information visible sur les réseaux sociaux, ni suite évidente (123456, azerty) ;
- les mots de passe sont conservés uniquement dans le gestionnaire de mots de passe fourni par l'entreprise (annexe C), jamais sur un papier, dans un fichier, un tableur, un courriel envoyé à soi-même ou le navigateur ; le mot de passe de session et le mot de passe maître, qui ne peuvent pas figurer dans le gestionnaire, sont mémorisés ;
- un mot de passe provisoire remis par l'administrateur est changé dès la première connexion.

Les mots de passe des comptes utilisateurs n'ont pas à être changés périodiquement si ces règles sont respectées. Ils sont changés immédiatement en cas de doute : saisie sur un faux site, mot de passe vu par un tiers, utilisation sur un poste douteux.

La double authentification est obligatoire sur la messagerie, sur les outils Microsoft 365, sur tout accès au système depuis l'extérieur et sur les comptes d'administration. L'entreprise fournit le moyen d'authentification ([application sur le smartphone professionnel, clé de sécurité]). L'utilisateur qui accepte d'installer l'application d'authentification sur son téléphone personnel le fait de son plein gré ; s'il ne le souhaite pas ou n'en possède pas, un autre moyen lui est remis. Le code reçu par SMS, que l'ANSSI déconseille, n'est utilisé qu'en dernier recours. Une notification qui demande d'approuver une connexion alors que l'utilisateur n'est pas en train de se connecter est refusée et signalée sans attendre au référent et au prestataire : son mot de passe est probablement connu d'un tiers.

Les utilisateurs ne disposent pas des droits d'administrateur sur leur poste. Si une opération l'exige, seul le prestataire peut accorder ces droits, ponctuellement et pour une durée limitée. Les comptes d'administration sont nominatifs, jamais partagés, distincts des comptes de travail quotidien, et ne servent jamais à lire des courriels ni à naviguer sur internet.

Article 6. Poste de travail et logiciels

L'utilisateur verrouille sa session chaque fois qu'il quitte son poste, même quelques minutes. Le verrouillage automatique, réglé par le prestataire, intervient après [5] minutes d'inactivité.

L'utilisateur n'installe, ne copie, ne modifie ni ne supprime aucun logiciel, aucune extension de navigateur et aucun réglage de sécurité ou du système sans l'accord du prestataire : tout besoin lui est adressé. Il ne désactive jamais les protections du poste (antivirus, pare-feu, VPN, chiffrement du disque, logiciel de gestion à distance installé par le prestataire) et ne modifie pas leur configuration. Il laisse les mises à jour s'installer et redémarre son poste quand le système ou le prestataire le demande, sans le repousser indéfiniment. Il ignore toute fenêtre ou publicité qui propose une « mise à jour » en dehors de ces canaux.

L'utilisateur ne branche jamais sur son poste une clé USB, un disque ou tout autre périphérique trouvé, offert ou d'origine inconnue, ni ses supports personnels, et ne laisse pas un tiers y brancher son équipement, même pour recharger un téléphone. Seuls les supports amovibles fournis par l'entreprise sont utilisés ; un support connecté au poste professionnel est présumé utilisé à des fins professionnelles. Copier des données de l'entreprise sur un support amovible suppose l'accord du responsable hiérarchique et un support chiffré.

L'utilisateur ne laisse visible aucun document confidentiel ni aucun écran lisible par des visiteurs, à l'accueil comme en salle de réunion. Il n'utilise pas pour le travail un appareil dont le système n'est plus mis à jour par l'éditeur.

Article 7. Messagerie électronique

La messagerie professionnelle est destinée à l'activité professionnelle. Il est interdit de créer une règle de transfert automatique vers une messagerie personnelle ou externe, et de transférer manuellement des messages professionnels vers une adresse personnelle. La messagerie personnelle n'est jamais utilisée pour le travail.

Avant d'ouvrir une pièce jointe ou de cliquer sur un lien, l'utilisateur vérifie que l'expéditeur est connu, que le message était attendu et que le lien correspond au sujet ; il place la souris sur le lien, sans cliquer, pour lire l'adresse réelle qui s'affiche. Un QR code reçu par courriel ou par courrier appelle la même prudence. Est suspect tout message qui présente une urgence, une menace, une offre trop belle, une pièce jointe inattendue, une facture pour un achat inconnu ou une demande d'identifiants. En cas de doute, l'utilisateur vérifie par un autre canal, en appelant un numéro déjà connu, jamais en répondant au message ni en utilisant les coordonnées qu'il contient. Il ne répond jamais par courriel à une demande de mot de passe, de code ou de coordonnées bancaires.

L'utilisateur signale un message suspect avec le bouton « Signaler » d'Outlook, puis en prévient le référent. S'il a cliqué, ouvert une pièce jointe ou saisi son mot de passe, il appelle immédiatement le prestataire et change son mot de passe depuis un autre appareil de confiance, selon ses indications ; il ne supprime pas le message, qui sert de preuve. Il ne relaie pas les messages en chaîne ni les fausses alertes.

Un message qui semble venir d'un fournisseur ou d'un client connu peut réellement partir de sa boîte, si elle a été piratée : une adresse d'expéditeur exacte ne prouve pas que le message est authentique. Seule la vérification par un autre canal fait foi.

Un fichier qui contient des informations confidentielles (article 11) ou des données personnelles sensibles ou nombreuses (liste de clients, bulletins de paie, pièces d'identité, coordonnées bancaires, données de santé) n'est jamais envoyé à l'extérieur en simple pièce jointe : il est partagé par un lien nominatif (article 10) ou protégé par un mot de passe selon la méthode indiquée en annexe C, ce mot de passe étant transmis par un autre moyen (téléphone, SMS), jamais dans le même courriel. Un envoi à de nombreux destinataires externes qui ne se connaissent pas se fait en copie cachée (Cci). Un courriel contenant des données personnelles envoyé au mauvais destinataire est un incident à signaler immédiatement (article 19).

Article 8. Virements, coordonnées bancaires et fraude au président

Aucun virement imprévu et aucune modification de coordonnées bancaires d'un fournisseur, d'un client ou d'un salarié ne sont exécutés sur la seule base d'un courriel, d'un SMS, d'un message ou d'un appel, quel que soit l'expéditeur apparent. Toute demande de ce type fait l'objet :

- d'un contre-appel au numéro habituel de l'interlocuteur (contrat, fiche fournisseur, factures antérieures), jamais au numéro indiqué dans la demande ;
- puis d'une validation par une seconde personne habilitée : [nom ou fonction].

Cette procédure s'applique sans exception, y compris lorsque la demande semble venir de la direction, qu'elle est présentée comme urgente ou confidentielle, ou qu'elle s'appuie sur une voix ou une vidéo convaincantes. Le contre-appel est noté dans [la fiche fournisseur ou le registre des virements] (date, numéro appelé, personne jointe). Un utilisateur qui applique la procédure et retarde ainsi un paiement ne peut pas se le voir reprocher.

L'utilisateur ne prend aucun engagement financier ou juridique pour l'entreprise en réponse à un message dont l'authenticité n'est pas vérifiée. Il ne valide jamais une opération bancaire qu'il n'a pas lancée, même « pour l'annuler ». En cas de doute ou de fraude, il prévient immédiatement la direction et la comptabilité, qui demandent à la banque la suspension ou le retour des fonds, et il conserve tous les éléments (messages, numéros, ordres de virement, factures).

Article 9. Internet et téléchargements

L'accès à internet est fourni pour l'activité professionnelle ; un usage personnel raisonnable est toléré dans les conditions de l'article 4. Sont interdits la consultation de contenus illicites, le téléchargement illégal, l'usage de logiciels piratés, de « cracks » ou de générateurs de clés, et le téléchargement de tout programme par l'utilisateur lui-même : un logiciel nécessaire est installé par le prestataire depuis le site officiel de l'éditeur.

Il est recommandé de se méfier des liens sponsorisés en tête des résultats de recherche, souvent utilisés pour diffuser de faux logiciels. Sur un formulaire en ligne, l'utilisateur ne donne que les informations strictement nécessaires. Il ne se connecte pas à ses comptes professionnels depuis un ordinateur public ou partagé (hôtel, salon, cybercafé) ; s'il y a été contraint, il prévient le prestataire et change ensuite, depuis un poste de confiance, les mots de passe saisis.

Une fenêtre affichée en plein écran, parfois sonore, qui affirme que l'ordinateur est infecté et donne un numéro à appeler est une arnaque au faux support technique. L'utilisateur n'appelle pas, ne donne aucun accès, ferme le navigateur, ou redémarre l'ordinateur si la fenêtre refuse de se fermer, puis prévient le prestataire : cette fausse alerte n'est pas une attaque du poste, et la consigne de l'article 19 de ne pas redémarrer ne s'applique pas. Microsoft et les éditeurs ne contactent jamais spontanément un utilisateur au sujet d'une alerte de sécurité. Si le prestataire contacte l'utilisateur au sujet d'un incident, il ne lui demande ni mot de passe ni code, et l'utilisateur peut toujours raccrocher et le rappeler aux coordonnées de l'annexe A avant toute action (article 18).

Article 10. Stockage, partage et sauvegarde des données

Les fichiers de travail sont enregistrés dans les espaces professionnels fournis (OneDrive professionnel, SharePoint, Teams), qui sont sauvegardés. Le bureau Windows non synchronisé, le disque local, une clé USB ou un téléphone peuvent ne pas l'être : l'utilisateur n'y conserve pas durablement de données de l'entreprise. Il est recommandé de ne pas multiplier les copies d'un même document sensible.

Le recours à un service de stockage, de partage ou de messagerie personnel (Google Drive, Dropbox, iCloud, OneDrive personnel, messageries instantanées grand public) pour des données personnelles ou des informations confidentielles de l'entreprise est interdit. Les échanges internes passent par les outils fournis (Teams). Sans validation du référent, l'utilisateur ne crée pas de compte sur un service en ligne avec son adresse professionnelle et ne dépose aucun document de l'entreprise sur un service en ligne (convertisseur PDF, traducteur, signature électronique, création graphique). Si un outil manque pour travailler, il le demande au référent au lieu d'utiliser un service non autorisé.

Un partage vers l'extérieur se fait par un lien nominatif (« Personnes spécifiques »), limité au besoin et supprimé quand il n'est plus utile. Les liens accessibles à toute personne qui les détient (« Tout le monde ») sont interdits, sauf autorisation du référent, et toujours avec une date d'expiration.

Les sauvegardes sont assurées par le prestataire selon les modalités décrites en annexe C ; elles ne couvrent que les données enregistrées dans les espaces professionnels. L'utilisateur ne fait aucune sauvegarde « maison » sur un service ou un disque personnel. Toute suppression accidentelle ou perte de fichier est signalée sans attendre : un fichier supprimé ne reste récupérable que pendant une durée limitée.

Article 11. Données personnelles et informations confidentielles

Données personnelles. L'utilisateur n'accède qu'aux données personnelles nécessaires à ses missions et ne les utilise que pour ces missions. Il ne les copie, ne les exporte et ne les communique qu'aux personnes autorisées et dans la mesure nécessaire. Il ne crée pas de fichier de données personnelles en dehors des outils prévus et respecte les durées de conservation fixées par l'entreprise. Toute demande d'une personne qui souhaite exercer ses droits (accès, rectification, effacement, limitation, opposition, portabilité) est transmise sans délai à [nom ou fonction de la personne chargée du RGPD].

Informations confidentielles. Sont confidentielles notamment [les données des clients, les tarifs et conditions commerciales, les contrats, les données financières, les données des salariés, les codes d'accès, les projets non publics, à adapter]. L'utilisateur ne les divulgue à aucune personne non autorisée, ni pendant ni après son contrat, et ne les emporte pas à l'extérieur sans nécessité. Il ne les évoque pas dans les lieux publics. Cette obligation ne fait obstacle ni aux signalements protégés de l'article 25, ni à la production en justice, par un salarié, des documents strictement nécessaires à l'exercice de ses droits de la défense.

Article 12. Intelligence artificielle

Seuls les outils d'intelligence artificielle validés par l'entreprise et listés en annexe C, utilisés avec le compte professionnel, sont autorisés pour le travail. Il ne se sert jamais, pour le travail, d'un compte d'IA personnel ni d'un compte ouvert avec une adresse personnelle.

Sauf outil expressément autorisé pour ce type de données, il est interdit de saisir dans un outil d'IA :

- des données personnelles (clients, salariés, candidats, patients) ;

- des informations confidentielles au sens de l'article 11, des documents contractuels, juridiques ou financiers, des projets non publics ;
- des secrets informatiques (mots de passe, codes et clés d'accès).

Même dans un outil autorisé, l'utilisateur ne soumet que ce qu'il est autorisé à partager et réduit au minimum les informations qui permettent d'identifier une personne. Une saisie de ce type faite par erreur est signalée comme un incident (article 19).

L'IA peut se tromper et inventer des faits ou des sources. L'utilisateur vérifie toute production avant de l'envoyer, de la publier ou de s'en servir pour décider, et il en reste responsable ; la décision finale appartient toujours à une personne. Un code informatique produit par une IA n'est jamais exécuté sans contrôle. Une image, une vidéo ou une voix générées pour représenter une personne réelle ne sont diffusées qu'avec son accord et avec la mention de leur caractère artificiel ; la loi punit leur diffusion sans consentement lorsque ce caractère n'est ni évident ni signalé (annexe E).

Il est interdit, sans l'accord écrit de la direction et du prestataire, d'installer une extension ou un agent d'IA capable d'agir de façon autonome (exécuter des commandes, piloter le navigateur, envoyer des courriels, manipuler des fichiers), et de connecter un outil d'IA à la messagerie, à l'agenda ou aux espaces de fichiers de l'entreprise. L'utilisateur ne demande pas à un assistant d'IA d'agir (envoyer, payer, modifier, supprimer) à partir de contenus venus de l'extérieur (courriels, pages web, documents reçus), qui peuvent contenir des instructions cachées. Il n'utilise un outil de transcription ou de résumé automatique pendant un appel ou une réunion qu'après en avoir informé tous les participants, dans les conditions de l'article 20.

Aucun outil d'IA n'est utilisé pour déduire les émotions d'une personne au travail, pratique interdite par le règlement européen sur l'IA sauf raisons médicales ou de sécurité. Aucun outil d'IA n'est utilisé pour recruter, évaluer, sanctionner ou répartir le travail sans décision de la direction et information préalable des salariés et de leurs représentants. L'entreprise prend des mesures pour favoriser la maîtrise de l'IA par son personnel : [sensibilisation, formation, à préciser].

Article 13. Réseaux sociaux et expression en ligne

Chaque salarié conserve sa liberté d'expression, dans l'entreprise et en dehors, y compris sur ses réseaux sociaux et ses messageries personnels. La présente charte n'y apporte que des restrictions justifiées par la nature des tâches et proportionnées au but recherché. Elle ne limite pas le droit d'expression directe et collective des salariés sur leur travail. L'entreprise ne surveille pas les comptes personnels de ses salariés.

Sont interdits, sur les outils de l'entreprise et sur tout espace public ou largement accessible :

- les propos injurieux, diffamatoires ou excessifs visant l'entreprise, ses dirigeants, ses salariés, ses clients ou ses partenaires ;
- tout contenu à caractère sexiste, sexuel, raciste ou discriminatoire adressé à des collègues.

La divulgation d'informations confidentielles au sens de l'article 11 est interdite quel que soit le support, y compris par des captures d'écran ou des photos laissant voir des écrans, des documents, des badges ou des accès. Les messages envoyés avec les outils de l'entreprise, téléphone professionnel compris, sont présumés professionnels. Une conversation de nature privée, qui n'est pas destinée à être rendue publique, ne peut fonder une sanction que si elle constitue un manquement à une obligation du contrat de travail.

Seules les personnes désignées par la direction s'expriment au nom de l'entreprise et gèrent ses comptes officiels, protégés par la double authentification. L'utilisateur reste discret, en ligne, sur l'organisation interne, les procédures de paiement, ses déplacements et les projets de l'entreprise : ces informations servent à préparer

des escroqueries ciblées. Il est recommandé de se méfier d'une sollicitation inhabituelle, même venant d'un contact connu dont le compte peut avoir été piraté. Tout faux profil qui usurpe l'identité de l'entreprise, d'un dirigeant ou d'un collègue est signalé au référent. L'usage personnel des réseaux sociaux pendant le temps de travail reste ponctuel et raisonnable.

Article 14. Matériel nomade et déplacements

Hors des locaux, l'utilisateur garde son ordinateur, son téléphone et ses documents sous sa surveillance et ne les laisse jamais dans une voiture, un train ou une chambre d'hôtel. Le poste nomade lui est attribué personnellement et n'est prêté à personne. Il utilise le filtre de confidentialité fourni dans les transports et les lieux publics, n'y consulte pas de document sensible, ne tape pas un mot de passe à la vue d'autrui et reste discret sur ses conversations professionnelles.

Il est recommandé de préférer le réseau mobile aux réseaux Wi-Fi publics (gare, hôtel, café, salon). Sur un Wi-Fi public, l'utilisateur passe par le VPN de l'entreprise et n'effectue aucune opération sensible. Il est recommandé d'éviter les bornes de recharge USB en libre-service et de désactiver Wi-Fi, Bluetooth et NFC quand ils ne servent pas. L'utilisateur n'emporte que les données nécessaires et ne désactive pas le chiffrement du disque.

Avant un déplacement à l'étranger, il lit les conseils aux voyageurs du ministère de l'Europe et des Affaires étrangères et interroge le référent sur la législation locale, notamment en matière de chiffrement. Si ses équipements sont inspectés ou retenus à une frontière, il prévient l'entreprise et les fait vérifier à son retour. Au retour, il change les mots de passe utilisés pendant le déplacement.

L'utilisateur signale immédiatement par téléphone, au référent et au prestataire, toute perte, tout vol, toute inspection ou toute saisie de matériel ; ils peuvent bloquer l'appareil, en effacer les données à distance et fermer les sessions. Pour un téléphone, l'utilisateur note à l'avance le numéro IMEI de l'appareil (affiché en composant *#06#) et le conserve ailleurs que sur le téléphone : il sert à la suspension de la ligne et à la plainte.

Article 15. Télétravail

En télétravail, les règles de la présente charte s'appliquent sans changement ; conformément à l'article L1222-10 du Code du travail, elle informe le télétravailleur des restrictions d'usage des outils et des sanctions encourues (article 24). Les conditions du télétravail elles-mêmes, dont les plages horaires pendant lesquelles le salarié peut être contacté, sont fixées par [la charte ou l'accord de télétravail de l'entreprise].

Le matériel professionnel n'est utilisé que par le salarié, dans les conditions de l'article 4 ; il n'est confié à aucun membre du foyer, à qui aucun mot de passe n'est communiqué. Le salarié sécurise sa connexion domestique : mot de passe d'administration de la box changé s'il est par défaut, mises à jour de la box appliquées, Wi-Fi protégé en WPA3, ou à défaut en WPA2, avec une clé longue, fonction WPS désactivée. En cas de doute sur ces réglages, il demande l'aide du prestataire. Il se connecte au VPN de l'entreprise lorsque l'accès aux ressources internes l'exige [et au moins une fois par jour de télétravail, si les mises à jour passent par le VPN]. Il enregistre son travail dans les espaces professionnels et range les documents papier.

[Si l'option B de l'article 16 est retenue :] L'usage d'un ordinateur personnel pour travailler est soumis à autorisation préalable de [la direction] ; il suppose un système à jour, un antivirus et une session réservée au salarié. Aucune donnée de l'entreprise n'y est conservée. [Si l'option A est retenue : l'usage d'un ordinateur personnel pour travailler est interdit.] Il est recommandé de ne pas imprimer de documents confidentiels à domicile ; le salarié qui le fait les rapporte au bureau ou les détruit après usage.

Les réunions à distance se tiennent avec les outils fournis par l'entreprise. Avant de partager son écran, le salarié ferme les documents et les fenêtres sans rapport avec la réunion ; il est recommandé de partager une seule fenêtre plutôt que l'écran entier. Il coupe micro et caméra quand ils ne sont pas nécessaires et peut flouter son arrière-plan. Les liens de réunion ne sont pas diffusés au-delà des participants. L'activité en télétravail est suivie par les objectifs et les comptes rendus, sans dispositif de surveillance continue. Si une règle est difficile à appliquer chez lui, le salarié le signale au lieu de la contourner.

Article 16. Smartphones, tablettes et appareils personnels

Tout appareil mobile qui accède aux données de l'entreprise est protégé par un code de verrouillage (jamais 0000 ni 1234) et se verrouille automatiquement. Il est chiffré et maintenu à jour, et ne reçoit que des applications issues des magasins officiels (App Store, Google Play), dont l'utilisateur vérifie les autorisations. Aucun mot de passe n'est noté dans les contacts, les notes ou les messages. Un appareil dont le système a été modifié pour lever ses protections (« jailbreak », « root ») ne peut pas accéder aux données de l'entreprise.

Le smartphone professionnel est inscrit dans l'outil de gestion des appareils mobiles du prestataire ; l'utilisateur ne le retire pas et ne contourne pas ses réglages. Il est destiné à l'usage professionnel, un usage personnel ponctuel restant toléré dans les conditions de l'article 4 ; l'utilisateur n'y synchronise pas ses comptes personnels de messagerie, d'agenda ou de réseaux sociaux et n'y installe que les applications validées. L'assistant vocal y est désactivé.

[Option A, recommandée par l'ANSSI : l'accès aux données de l'entreprise depuis un appareil personnel, y compris un ordinateur personnel, est interdit.]

[Option B, admise par la CNIL si l'usage est encadré :] L'accès depuis un appareil personnel est soumis à autorisation préalable et se fait uniquement par les applications professionnelles gérées (Outlook, Teams, OneDrive), qui cloisonnent les données de l'entreprise. En cas de perte, de vol ou de départ, seules les données professionnelles sont effacées à distance ; l'entreprise n'accède à aucun contenu privé de l'appareil (photos, messages, contacts, historique) et l'outil de gestion n'empêche pas l'usage personnel.

Article 17. Réseau, Wi-Fi, objets connectés et imprimantes

Le réseau interne, filaire ou Wi-Fi, est réservé aux équipements fournis et gérés par l'entreprise. Les appareils personnels et ceux des visiteurs, clients ou fournisseurs se connectent uniquement au réseau Wi-Fi invités. Sans l'accord du prestataire, il est interdit de communiquer la clé du réseau interne, de brancher sur une prise réseau ou sur la box un équipement non fourni par l'entreprise (borne Wi-Fi, répéteur, commutateur) et de connecter un objet connecté personnel (enceinte, assistant vocal, caméra). Les visiteurs sont accompagnés hors des zones d'accueil, et un intervenant extérieur n'est pas laissé seul dans un local sensible.

Les objets connectés de l'entreprise (caméra, alarme, écran de salle de réunion) et l'imprimante multifonction sont installés et maintenus par le prestataire, mots de passe par défaut changés. L'utilisateur n'en modifie pas les réglages. Il récupère ses impressions aussitôt et ne laisse aucun document confidentiel sur l'imprimante ; il n'envoie ses numérisations qu'à des adresses professionnelles. Il signale tout comportement anormal d'un équipement. Le disque de l'imprimante est effacé de façon sécurisée avant toute restitution ou réparation.

Article 18. Support informatique et prestataire

Le support informatique est assuré par [nom du prestataire], joignable uniquement aux coordonnées figurant en annexe A. Le support ne demande jamais de mot de passe, ni de lui lire un code reçu par SMS ou affiché dans

l'application d'authentification, ni de valider une notification de connexion.

À un appel ou un message non sollicité qui se présente comme le support (le prestataire, Microsoft, un éditeur), l'utilisateur ne donne rien : il raccroche et rappelle le prestataire aux coordonnées de l'annexe A. Il n'installe jamais lui-même un logiciel de prise en main à distance (logiciel qui permet de piloter l'ordinateur à distance, comme AnyDesk ou TeamViewer) et ne donne jamais d'accès à distance à un interlocuteur qu'il n'a pas authentifié ; si c'est arrivé, il le signale aussitôt.

Sauf incident de sécurité exigeant une intervention urgente, dont l'utilisateur est informé dès que possible, une prise en main à distance du poste n'a lieu qu'avec l'accord de l'utilisateur, à sa demande ou dans le cadre d'un rendez-vous convenu, et reste visible pendant toute sa durée. Les opérations automatiques (mises à jour, protection antivirale) se font sans prise en main de l'écran. Un technicien n'intervient sur place que si sa venue a été annoncée par le prestataire ou confirmée auprès de lui ; il est accompagné pendant son intervention. Aucune personne extérieure non autorisée, même un proche « qui s'y connaît », n'intervient sur le matériel de l'entreprise.

Article 19. Incidents de sécurité : signaler et réagir

L'utilisateur signale immédiatement au référent et au prestataire, par téléphone ou de vive voix plutôt que par courriel (l'attaquant peut lire la messagerie), tout événement suspect, notamment :

- un clic ou une saisie d'identifiants sur un message douteux, une demande de double authentification non sollicitée ;
- un comportement anormal du poste : lenteur soudaine, fichiers renommés ou illisibles, programmes ou comptes inconnus, alerte de l'antivirus ;
- la perte ou le vol d'un appareil ou d'un support ;
- un courriel contenant des données personnelles envoyé au mauvais destinataire, une saisie de données sensibles dans un outil non autorisé ;
- une demande suspecte de virement ou de changement de coordonnées bancaires, un appel d'un faux support, un message de rançon.

En cas de suspicion d'attaque du poste, l'utilisateur débranche le câble réseau et coupe le Wi-Fi, sans éteindre ni redémarrer l'appareil, pour préserver les traces utiles à l'analyse. Il ne supprime rien, photographie l'écran avec un téléphone, note l'heure et ce qu'il a fait, ne tente aucune réparation, ne contacte pas les attaquants et ne paie aucune rançon.

Le signalement rapide est un devoir. Le fait de signaler n'est jamais reproché, et une erreur involontaire signalée sans délai n'est pas sanctionnée ; seul un manquement délibéré ou répété aux règles de la charte peut l'être. Deux délais courts justifient cette exigence : l'entreprise doit notifier à la CNIL, si possible dans les 72 heures, une violation de données personnelles présentant un risque pour les personnes (article 33 du RGPD) ; et l'indemnisation d'une cyberattaque par l'assureur suppose une plainte déposée au plus tard 72 heures après sa découverte (article L12-10-1 du Code des assurances). La conduite à tenir figure dans la fiche réflexe de l'annexe B.

Article 20. Administration du système d'information et contrôles

Qui administre. Le système d'information est administré par [nom du prestataire], sous-traitant de l'entreprise au sens de l'article 28 du RGPD, dans le cadre d'un contrat qui fixe ses obligations de sécurité et de confidentialité, et par [le référent, pour les seules tâches qui lui sont confiées]. Les administrateurs n'accèdent

aux données que dans la mesure nécessaire à leurs missions (maintenance, sécurité, sauvegardes, support) et ne demandent jamais de mot de passe. Ils ne divulguent pas ce qu'ils découvrent à cette occasion, sauf obligation légale ; une atteinte à la sécurité ainsi découverte n'est signalée qu'à la direction. Leurs interventions sont tracées. Leurs engagements figurent en annexe F.

Contrôles mis en œuvre. Pour assurer la sécurité et le bon fonctionnement du système et vérifier, en cas d'anomalie, le respect de la présente charte, et seulement à ces fins, l'entreprise met en œuvre les dispositifs suivants, et aucun autre [liste à ajuster aux outils réellement en place] :

- filtrage de la navigation par catégories de sites et blocage des sites malveillants ;
- protection des postes et des serveurs (antivirus ou outil de détection et de réponse) ;
- filtrage des courriels (antispam, analyse des pièces jointes et des liens) ;
- journalisation des connexions et des accès (comptes, VPN, messagerie, Microsoft 365, réseau) ;
- outil de gestion à distance des postes et des smartphones professionnels (inventaire, mises à jour, configuration) ;
- sauvegardes des données décrites en annexe C ;
- [le cas échéant : historique des requêtes des outils d'IA de l'annexe C, conservé par l'outil].

[Si l'outil de filtrage examine le contenu des connexions sécurisées (adresses en https) : les sites de banque, de santé et d'administrations publiques en sont exclus ; le contenu des requêtes n'est pas conservé ; le filtrage s'applique aussi en télétravail par l'intermédiaire de [VPN ou agent].]

[Si l'entreprise organise des campagnes d'hameçonnage simulé : elles sont annoncées dans leur principe ; leurs résultats individuels servent à la formation et ne fondent aucune sanction ; elles figurent en annexe D.]

Les journaux sont conservés [entre 6 et 12 mois, durée à fixer ; une durée plus longue doit être justifiée dans l'annexe D], conformément à la recommandation de la CNIL, puis supprimés, sauf s'ils sont nécessaires à une procédure en cours. Ils sont protégés contre l'accès des personnes dont ils tracent l'activité. Les contrôles portent d'abord sur des données globales et non nominatives ; un contrôle individuel n'intervient qu'en cas d'anomalie, de soupçon d'abus ou d'incident de sécurité, et l'utilisateur concerné en est informé dès que cela ne compromet plus la vérification, et en tout état de cause avant toute décision le concernant.

Ce que l'entreprise ne fait pas. Elle n'utilise ni enregistreur de frappe, ni capture d'écran périodique, ni relevé du temps d'inactivité des salariés, ni copie automatique des messages à des fins de surveillance, ni surveillance par la caméra ou le micro des postes. Le verrouillage automatique et l'indicateur de présence de Teams ne sont ni enregistrés ni utilisés pour évaluer l'activité, et les sauvegardes de l'annexe C ne servent qu'à restaurer des données. L'entreprise ne lit pas les messages et fichiers identifiés comme personnels, hors des cas prévus au paragraphe suivant, et ne prend pas connaissance des messages d'une messagerie personnelle, même consultée depuis le poste professionnel.

Accès aux fichiers et messages. Les messages et fichiers présumés professionnels (article 4) peuvent être consultés par l'entreprise, y compris hors de la présence de l'utilisateur. Un élément identifié comme personnel n'est ouvert qu'en présence de l'utilisateur ou après qu'il a été régulièrement invité à y assister, sauf risque ou événement particulier, ou sur décision de justice.

Visioconférence et enregistrements. L'activation de la caméra n'est pas imposée de façon systématique ; le floutage de l'arrière-plan est possible. Elle peut être demandée pour certains échanges : [entretien individuel, rendez-vous client, accueil d'un nouvel arrivant]. Aucun appel, aucune réunion ni aucune visioconférence n'est enregistré ou transcrit, y compris par un outil d'IA, sans que tous les participants en aient été informés au préalable ; un salarié peut demander que ses propos ne soient pas enregistrés, sauf enregistrement décidé par

l'entreprise pour une finalité annoncée ; un participant extérieur peut toujours refuser l'enregistrement. Ces enregistrements sont ponctuels, limités à leur finalité, accessibles aux seules personnes habilitées et conservés [6 mois] au plus.

Autres dispositifs. [Le cas échéant : la vidéosurveillance des locaux et la géolocalisation des véhicules font l'objet d'une information distincte ; elles ne sont pas régies par la présente charte.]

Information et droits. Les traitements de données liés à ces contrôles, leurs finalités, leurs bases légales, leurs durées de conservation et leurs destinataires sont décrits en annexe D, qui précise comment exercer ses droits, y compris le droit d'accès aux courriels professionnels que l'on a émis ou reçus. Les membres du comité social et économique disposent par ailleurs d'un droit d'alerte en cas d'atteinte injustifiée aux droits des personnes ou aux libertés individuelles.

Article 21. Absence et départ de l'utilisateur

Absence prévue. Avant une absence, l'utilisateur programme un message d'absence qui indique un contact et, si nécessaire, donne à un collègue désigné un accès délégué à sa messagerie ou à ses dossiers professionnels.

Absence imprévue. Lorsque la continuité de l'activité l'exige, l'administrateur peut, sur demande écrite de la direction, donner accès aux messages et dossiers professionnels strictement nécessaires d'un utilisateur absent. Les éléments identifiés comme personnels ne sont pas ouverts. L'utilisateur en est informé dès que possible. Son mot de passe ne lui est jamais demandé : l'accès est donné par l'administrateur.

Départ. L'entreprise informe par écrit l'utilisateur qui la quitte de la date de fermeture de ses comptes, en lui laissant [10 jours ouvrés] pour transférer ses messages personnels vers sa messagerie personnelle, récupérer ses autres éléments personnels et placer les données professionnelles utiles dans les espaces partagés. L'utilisateur ne supprime pas les données professionnelles. En cas de départ immédiat ou de suspension des accès, ses éléments personnels lui sont remis par l'administrateur, qui les extrait en présence de l'utilisateur ou d'une personne de confiance qu'il désigne. Au plus tard le dernier jour :

- l'utilisateur restitue tout le matériel, les supports, les badges et les moyens d'authentification, ainsi que l'ensemble des données de l'entreprise, sans en conserver de copie ;
- ses comptes et accès sont désactivés, les codes partagés qu'il connaissait sont changés (comptes génériques, Wi-Fi, alarme, accès de partenaires) et les données professionnelles de son éventuel appareil personnel sont effacées à distance, et seulement elles.

Un message automatique indique ensuite un nouveau contact pendant [3 mois], puis l'adresse nominative est supprimée ; le contenu de la boîte qui n'a pas été versé dans les espaces partagés est [archivé pendant [durée] ou supprimé]. Les postes et supports restitués sont effacés de façon sécurisée avant réaffectation. L'obligation de confidentialité de l'article 11 demeure après le départ.

Article 22. Droit à la déconnexion

Aucun salarié n'est tenu de consulter les messages, appels ou sollicitations professionnels ni d'y répondre en dehors de ses horaires de travail, pendant ses congés, ses temps de repos ou ses arrêts de travail. L'absence de réponse en dehors de ces horaires ne peut lui être reprochée. Il est recommandé de programmer l'envoi différé des messages rédigés tard le soir ou le week-end et de ne pas attendre de réponse immédiate.

Seules font exception [les astreintes organisées et les incidents de sécurité majeurs], le temps de travail ainsi effectué étant décompté et rémunéré [selon les règles de l'astreinte en vigueur dans l'entreprise]. En télétravail,

les plages pendant lesquelles le salarié peut être contacté sont celles de la charte ou de l'accord de télétravail. [Si des salariés sont en forfait en jours et qu'aucun accord ne le prévoit : le présent article définit les modalités du droit à la déconnexion au sens de l'article L3121-65 du Code du travail.]

Article 23. Logiciels, licences et propriété intellectuelle

Seuls les logiciels dont l'entreprise détient les licences, installés par le prestataire, sont utilisés, dans les limites de leur licence (nombre de postes, usage commercial). Outre les interdits de l'article 9, il est interdit de télécharger, copier ou partager avec les moyens de l'entreprise, sans en avoir le droit, des logiciels ou des œuvres : films, musique, polices de caractères, photos et images. Le téléchargement et le partage illicites (logiciels de pair à pair, sites pirates) sont interdits sur la connexion de l'entreprise ; l'entreprise, titulaire de l'accès à internet, doit en effet veiller à ce qu'il ne serve pas à des actes de contrefaçon (article L336-3 du Code de la propriété intellectuelle). L'utilisateur respecte les conditions d'utilisation des contenus et services qu'il emploie.

Les droits patrimoniaux sur les logiciels et leur documentation créés par un salarié dans l'exercice de ses fonctions ou d'après les instructions de l'entreprise sont dévolus à l'entreprise, sauf stipulation contraire (article L113-9 du Code de la propriété intellectuelle). Toute invention réalisée par un salarié est déclarée à l'entreprise (article L611-7 du même code). Pour les autres créations (textes, visuels, supports), la charte n'opère aucune cession de droits : leur exploitation fait, si nécessaire, l'objet d'un accord écrit distinct.

Article 24. Responsabilités et sanctions

Le non-respect de la présente charte par un salarié peut entraîner, selon la gravité des faits et après la procédure prévue par les articles L1332-1 à L1332-5 du Code du travail, l'une des sanctions suivantes : avertissement, mise à pied disciplinaire de [3] jours au plus, mutation, rétrogradation, licenciement. [Si un règlement intérieur existe, reprendre son échelle des sanctions à l'identique.] Toute sanction est proportionnée à la faute. Aucune amende ni autre sanction pécuniaire ne peut être prononcée (article L1331-2 du Code du travail) ; la mise à pied suspend seulement le contrat et la rémunération des jours concernés. Le salarié dispose des droits de la défense prévus par la loi : griefs notifiés par écrit, entretien préalable lorsqu'il est requis, assistance par une personne de son choix appartenant au personnel.

Pour les personnes qui ne sont pas salariées de l'entreprise (intérimaires, stagiaires, intervenants extérieurs), un manquement est signalé à leur employeur, à leur établissement ou à leur société, et peut entraîner la suspension de leur accès et la fin de leur mission dans les conditions de leur contrat ou de leur convention.

Ces mesures s'entendent sans préjudice des poursuites civiles ou pénales encourues pour des faits contraires à la loi (annexe E). L'accès d'une personne aux moyens informatiques peut être suspendu à titre conservatoire si la sécurité du système l'exige. Le fait de signaler un incident n'est jamais sanctionné (article 19).

Article 25. Signalements protégés et représentants du personnel

Aucune disposition de la présente charte, notamment les obligations de confidentialité et de discrétion, ne fait obstacle ni à un signalement ou à une divulgation dans les conditions prévues par les articles 6 à 8 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (dite loi « Sapin II »), qui protège les lanceurs d'alerte, ni à l'information des représentants du personnel, ni au témoignage de faits de harcèlement ou de discrimination. Un signalement peut être adressé au responsable hiérarchique, à la direction ou directement aux autorités compétentes (dont la CNIL et l'ANSSI

pour les données personnelles et la sécurité des systèmes), au Défenseur des droits ou à l'autorité judiciaire. Aucune mesure de représailles ne peut être prise contre son auteur.

La charte ne restreint pas l'usage des outils numériques par les représentants du personnel dans l'exercice de leur mandat, dans les conditions prévues par la loi et, le cas échéant, par accord.

Article 26. Entrée en vigueur, diffusion et mise à jour

La charte entre en vigueur le [date], au moins un mois après l'accomplissement des formalités rappelées dans le préambule. Elle est remise à chaque nouvel arrivant avec ses identifiants, présentée lors des séances de sensibilisation et accessible à tout moment sur [emplacement]. L'accusé de réception de l'annexe G atteste que l'utilisateur en a pris connaissance.

Elle est revue au moins une fois par an et à chaque changement important d'outil, d'organisation ou de réglementation. Toute modification des règles qu'elle impose suit la même procédure que son adoption. L'annexe A peut être mise à jour, et des outils ajoutés à l'annexe C, sans cette procédure ; le retrait d'un outil autorisé et toute restriction nouvelle la suivent. Tout nouveau dispositif de contrôle est ajouté à la liste de l'article 20 et décrit dans l'annexe D, puis porté à la connaissance des utilisateurs avant sa mise en service.

Annexe A. Contacts utiles

Pour	Contact
Référent informatique	[nom, téléphone, courriel]
Support informatique (prestataire)	[nom du prestataire, téléphone, courriel, portail de support, horaires]
Direction	[nom, téléphone]
Validation des virements et des changements de coordonnées bancaires	[nom, téléphone]
Données personnelles (exercice des droits, violation de données)	[nom, courriel]
Assurance cyber	[assureur, numéro de contrat, numéro de déclaration de sinistre]
Banque (opposition, rappel de fonds)	[agence, numéro]
Dépôt de plainte en cas de cyberattaque (délai de 72 heures pour l'assurance)	[commissariat ou brigade de gendarmerie, adresse], ou plainte écrite au procureur de la République
Assistance et signalement d'une cyberattaque	17Cyber : 17cyber.gouv.fr (Police nationale, Gendarmerie nationale et Cybermalveillance.gouv.fr)
Escroqueries (conseil)	Info Escroqueries : 0 805 805 817
Harcèlement et agissements sexistes	Référent harcèlement désigné par le CSE : [nom, adresse, téléphone] · médecin du travail : [service, adresse, téléphone] · inspection du travail : [adresse, téléphone, nom de l'inspecteur] · Défenseur des droits : [adresse, téléphone], defenseurdesdroits.fr
Autorité de protection des données	CNIL : cnil.fr

Annexe B. Fiche réflexe en cas d'incident

> À afficher près des postes et à garder dans son téléphone. Support : [numéro] · référent : [numéro]

Un message, un appel ou une alerte vous semble suspect

- Ne cliquez pas, ne répondez pas, ne rappelez pas le numéro indiqué.
- Signalez le message avec le bouton « Signaler » d'Outlook et prévenez le référent.
- Une fenêtre affirme que l'ordinateur est infecté et affiche un numéro : n'appelez pas, fermez le navigateur (redémarrez si la fenêtre bloque l'écran), prévenez le support.
- Pour une demande de virement ou de nouveau RIB : contre-appel au numéro habituel, puis validation par une seconde personne.

Vous avez cliqué, ouvert une pièce jointe ou donné votre mot de passe

- Appelez immédiatement le support.
- Changez votre mot de passe depuis un autre appareil de confiance, selon les indications du support.
- Ne supprimez pas le message.

Votre poste se comporte anormalement ou affiche une demande de rançon

- Débranchez le câble réseau et coupez le Wi-Fi. N'éteignez pas, ne redémarrez pas.
- Photographiez l'écran avec un téléphone, notez l'heure et ce que vous faisiez.
- Appelez le support et le référent par téléphone, pas par courriel.
- Ne payez rien, ne contactez pas les attaquants, ne tentez aucune réparation.

Vous avez perdu ou on vous a volé un appareil

- Prévenez immédiatement le référent et le support, qui bloquent l'appareil et ferment les sessions.
- Pour un téléphone, donnez le numéro IMEI ; la plainte est déposée selon les indications du référent.

> Signaler vite n'est jamais reproché, même en cas d'erreur. L'entreprise dispose de délais courts pour prévenir la CNIL et pour déposer plainte.

Annexe C. Outils autorisés et sauvegardes

Usage	Outil autorisé
Messagerie, agenda, bureautique	Microsoft 365 [Business Standard ou Business Premium], avec le compte professionnel
Stockage et partage	OneDrive professionnel, SharePoint, Teams
Échanges internes et réunions à distance	Microsoft Teams
Envoi de fichiers confidentiels à l'extérieur	[lien nominatif OneDrive, chiffrement de message Outlook ou archive protégée par mot de passe : méthode à préciser]
Gestionnaire de mots de passe	[nom de l'outil]
Double authentification	[Microsoft Authenticator, clé de sécurité]
Accès à distance	[VPN ou service d'accès]
Intelligence artificielle	[par exemple Microsoft Copilot Chat avec le compte professionnel ; préciser pour chaque outil les données qui peuvent y être saisies]
Logiciels métier	[liste]

Sauvegardes. [Ce qui est sauvegardé (boîtes aux lettres, OneDrive, SharePoint, Teams, serveurs, postes), à quelle fréquence, combien de temps les copies sont conservées, où elles sont hébergées, qui les réalise et comment les restaurations sont testées.]

Annexe D. Information des utilisateurs sur les traitements de données

Responsable de traitement : [raison sociale, adresse]. Contact pour toute question ou pour exercer ses droits : [nom, courriel].

Dispositif	Finalité	Base légale	Durée de conservation	Destinataires
Journaux de connexion et d'accès	Sécurité du système, détection des intrusions, enquête après incident, vérification du respect de la charte en cas d'anomalie	Obligation légale de sécurité (article 32 du RGPD) pour la sécurité ; intérêt légitime (faire respecter la charte) pour la vérification en cas d'anomalie	[entre 6 et 12 mois]	Prestataire, référent, direction en cas d'incident ou d'anomalie
Filtrage de la navigation	Protection contre les sites malveillants, respect des règles d'usage	Intérêt légitime : protéger le système et faire respecter la charte	[entre 6 et 12 mois pour les journaux]	Prestataire
Protection des postes et filtrage des courriels	Détection et blocage des menaces	Intérêt légitime : protéger le système contre les menaces	[durée des alertes et journaux]	Prestataire, éditeur de la solution
Gestion des postes et des mobiles	Inventaire, mises à jour, effacement en cas de perte ou de départ	Intérêt légitime : maintenir et sécuriser le matériel	Durée d'attribution du matériel	Prestataire
Messagerie et espaces de fichiers	Activité professionnelle, continuité en cas d'absence	Exécution du contrat de travail ; intérêt légitime : continuité de l'activité	Boîte nominative : durée du contrat, puis [3 mois] de réponse automatique ; contenu non versé dans les espaces partagés : [archivé pendant [durée] ou supprimé] ; fichiers professionnels : selon les règles de conservation de l'entreprise	Utilisateur, personnes autorisées
Sauvegardes	Restauration des données	Intérêt légitime : continuité de l'activité	[durée de rétention]	Prestataire, hébergeur [nom et pays]
[Le cas échéant] Enregistrements et transcriptions de réunions	[finalité annoncée]	Intérêt légitime : [à préciser]	[6 mois au plus]	Personnes habilitées
[Le cas échéant] Historique des outils d'IA	Sécurité, enquête après incident	Intérêt légitime : protéger les données de l'entreprise	[durée]	Prestataire, éditeur de l'outil

[Le cas échéant] Campagnes d'hameçonnage simulé	Sensibilisation et formation	Intérêt légitime : former le personnel	[durée]	Référent, prestataire

[Indiquer tout transfert de données hors de l'Union européenne et ses garanties, ou l'absence de transfert.] Chaque utilisateur dispose d'un droit d'accès à ses données, y compris au contenu et aux métadonnées des courriels professionnels qu'il a émis ou reçus, sous réserve des droits d'autrui, ainsi que d'un droit de rectification, d'effacement, de limitation et d'opposition dans les conditions du RGPD et, pour les traitements fondés sur le contrat de travail, d'un droit à la portabilité. L'entreprise répond dans un délai d'un mois, prolongeable de deux mois si la demande est complexe. L'utilisateur peut introduire une réclamation auprès de la CNIL (cnil.fr). Ces dispositifs sont inscrits au registre des traitements de l'entreprise.

Annexe E. Rappels légaux

Le Code du travail interdit le harcèlement moral (article L1152-1), le harcèlement sexuel (article L1153-1) et les agissements sexistes (article L1142-2-1), qui sont aussi sanctionnés disciplinairement. Indépendamment de la charte, la loi punit notamment les faits suivants (peines maximales encourues par une personne physique, textes en vigueur au [date de la dernière vérification : 8 octobre 2026 pour ce modèle]) :

Faits	Texte	Peine encourue
Accès ou maintien frauduleux dans un système informatique, y compris en dépassant ses propres droits d'accès	Code pénal, art. 323-1	3 ans et 100 000 euros ; 5 ans et 150 000 euros si des données sont supprimées ou modifiées ou si le fonctionnement est altéré
Entrave au fonctionnement d'un système ; introduction, extraction, modification ou suppression frauduleuse de données	Code pénal, art. 323-2 et 323-3	5 ans et 150 000 euros
Ouverture, détournement ou lecture de mauvaise foi des correspondances d'autrui, y compris électroniques	Code pénal, art. 226-15	1 an et 45 000 euros
Enregistrement ou transmission, sans consentement, de paroles prononcées à titre privé ou confidentiel, de l'image d'une personne dans un lieu privé ou de sa localisation	Code pénal, art. 226-1 et 226-2	1 an et 45 000 euros
Usurpation de l'identité d'un tiers, y compris en ligne	Code pénal, art. 226-4-1	1 an et 15 000 euros
Diffusion, sans son consentement, d'un montage ou d'un contenu généré par IA représentant une personne, lorsque son caractère artificiel n'est ni évident ni signalé	Code pénal, art. 226-8	1 an et 15 000 euros ; 2 ans et 45 000 euros en ligne
Collecte déloyale, détournement ou divulgation non autorisée de données personnelles	Code pénal, art. 226-16 à 226-24	Jusqu'à 5 ans et 300 000 euros
Harcèlement moral au travail	Code pénal, art. 222-33-2	2 ans et 30 000 euros

Harcèlement sexuel	Code pénal, art. 222-33	2 ans et 30 000 euros ; 3 ans et 45 000 euros notamment lorsqu'il passe par un service en ligne ou un support numérique
Consultation habituelle ou détention d'images pédopornographiques	Code pénal, art. 227-23	5 ans et 75 000 euros
Contrefaçon, notamment de logiciels (copie, installation ou diffusion sans droit)	Code de la propriété intellectuelle, art. L335-2 et L335-3	3 ans et 300 000 euros

L'entreprise, personne morale, encourt des amendes plus élevées. Ces montants sont donnés à titre d'information et peuvent évoluer : vérifier les textes sur legifrance.gouv.fr lors de chaque révision de la charte.

Annexe F. Engagements des administrateurs

Toute personne qui dispose de droits d'administration sur le système d'information, salarié ou intervenant du prestataire, s'engage à :

- n'utiliser ses droits que pour les missions qui lui sont confiées, avec un compte d'administration nominatif, jamais partagé, distinct de son compte de travail quotidien et protégé par la double authentification ;
- renouveler régulièrement les mots de passe des comptes d'administration et les changer au départ de toute personne qui les connaissait ;
- ne consulter des données que dans la mesure nécessaire à ses missions, ne jamais ouvrir un élément identifié comme personnel hors des cas prévus à l'article 20, et ne divulguer aucune information découverte à cette occasion, sauf obligation légale ; une atteinte à la sécurité ainsi découverte n'est signalée qu'à la direction ;
- ne jamais demander le mot de passe d'un utilisateur ;
- tracer ses interventions, ne pas altérer les journaux et en protéger l'accès ;
- ne pas copier de données sans nécessité et restituer toutes les données et tous les supports en fin de mission ;
- respecter cet engagement de confidentialité après la fin de ses fonctions.

Pour le prestataire, ces engagements sont repris dans le contrat de sous-traitance prévu par l'article 28 du RGPD. Pour un administrateur interne :

Nom, prénom, fonction	Date	Signature

Annexe G. Accusé de réception

Je soussigné(e) [nom, prénom], [fonction], reconnais avoir reçu la charte d'utilisation des moyens informatiques et des outils numériques de [raison sociale], version [1.0] du [date], et en avoir pris connaissance, ainsi que de l'information sur les traitements de données qui figure en annexe D.

Fait à	Le	Signature

Cet accusé de réception atteste de la remise de la charte ; il n'en conditionne pas l'application, qui résulte des formalités rappelées dans le préambule. Un exemplaire est conservé par l'entreprise, un autre par l'utilisateur.