**CHARTE D’UTILISATION DES RESSOURCES INFORMATIQUES**

Dans le cadre de son activité, [nom de l’entreprise] met à disposition de ses collaborateurs des outils informatiques et de communication.

La présente charte définit les conditions d’accès et d’utilisation des moyens informatiques et ressources mises à disposition des collaborateurs. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l’utilisation de ces ressources en termes d’intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. L’imprudence, la négligence ou la malveillance d’un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale, ainsi que celle de l’entreprise.

Le champ d’application de la charte

La charte s’applique à tout utilisateur des outils informatiques ou de communication mis à sa disposition par [nom de l’entreprise] pour l’exercice de ses activités professionnelles. L’utilisation à titre privé de ces outils est tolérée mais doit être raisonnable et ne pas perturber le bon fonctionnement du service.

On désigne sous le terme « utilisateur » toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de [nom de l’entreprise] et à les utiliser (employés, stagiaires, intérimaires, prestataires, etc).

Les termes « outils informatiques et de communication » recouvrent tous les équipements informatiques, de télécommunications et de reprographie de [nom de l’entreprise].

1. **Protection des données à caractère personnel**

La réglementation en vigueur en matière de protection des données personnelles[[1]](#footnote-1) définit les conditions dans lesquelles des traitements de données personnelles peuvent être effectués et impose une utilisation des données personnelles qui soit responsable, pertinente et limitée aux stricts besoins d’une entreprise ou de tout autre organisme. Ainsi, toute information se rapportant directement ou indirectement à une personne physique ne peut être utilisée que de manière transparente et en respectant les droits des personnes concernées.

[Nom de l’entreprise] a désigné un délégué à la protection des données personnelles qui a pour mission d’informer, de conseiller et de veiller à la conformité des traitements à la réglementation en matière de données personnelles. Il doit être consulté préalablement à la création d’un traitement et veille au respect des droits des personnes (droit d’accès, de rectification, d’opposition, d’effacement, de portabilité, de limitation du traitement). En cas de difficultés rencontrées lors de l’exercice de ces droits, les personnes concernées peuvent saisir le délégué à la protection des données personnelles.

1. Confidentialité sur les données traitées par le salarié

Chaque salarié est soumis à une obligation de confidentialité pour l’ensemble des données personnelles auxquelles il a accès dans le cadre de ses fonctions (qu’il s’agisse des données de consommateurs, de clients professionnels, de salariés…). Tout usage ou utilisation illicite de ces données est passible de sanctions pour l’entreprise et pour le salarié.

1. Protection des données des salariés

Les données personnelles des salariés sont collectées par l’employeur dans le cadre de la mise à disposition d’outils informatiques pour contrôler et/ou limiter l’utilisation des outils mis à disposition (internet, messagerie…). Ce contrôle a pour objectif :

* d’assurer la sécurité des réseaux contre d’éventuelles attaques (virus, cheval de Troie…) ;
* de limiter les risques d’abus d’une utilisation trop personnelle d’internet ou de la messagerie.

Conformément à la jurisprudence prise en application de l’article 1121-1 du Code du travail, il est rappelé que les fichiers et les courriels ont un caractère professionnel par défaut. Pour qu’ils soient protégés par le secret des correspondances privées, les messages personnels doivent être identifiés comme « Personnel » ou « Privé ».

Ces données sont destinées exclusivement à l’employeur et au service informatique. Elles peuvent être communiquées à des prestataires externes auxquels l’employeur fait appel pour la gestion des outils informatiques. L’utilisation des données du salarié par des tiers est alors strictement limitée à cette finalité.

La durée de conservation des données personnelles est liée à la finalité du traitement pour lequel les données sont collectées et elle vous est indiquée lors de la collecte de ces données.

[Nom de l’entreprise] met en œuvre des mesures techniques et organisationnelles pour assurer la sécurité des données personnelles contre tout accès, utilisation ou modification non autorisés, toute suppression involontaire ou encore contre le vol des données.

Conformément à la réglementation applicable en matière de données à caractère personnel, les salariés disposent d’un droit d’accès, de rectification, d’effacement et de portabilité des données les concernant, ainsi qu’un droit d’opposition et de limitation du traitement. Ces droits peuvent être exercés par le salarié [par courrier/par mail] à l’adresse suivante [adresse postale/adresse électronique].

En cas de difficulté en lien avec la gestion des données personnelles, les salariés peuvent également déposer une plainte auprès de la CNIL ou de toute autre autorité compétente.

1. **Les règles d’utilisation du système d’information**

Chaque utilisateur accède aux outils informatiques nécessaires à l’exercice de son activité professionnelle dans les conditions définies par [nom de l’entreprise].

1. Les modalités d’intervention du service de l’informatique interne

Le service de l’informatique interne de la commission assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de [nom de l’entreprise]. Ils ont accès à l’ensemble des données techniques mais s’engagent à respecter les règles de confidentialité applicables aux données qu’ils sont amenés à connaître dans le cadre de leurs fonctions.

1. L’authentification

L'accès aux ressources informatiques repose sur l’utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son arrivée dans l’entreprise. Un mot de passe est associé à cet identifiant de connexion. Les moyens d’authentification sont personnels et confidentiels.

1. Les règles de sécurité

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

* signaler au service informatique interne de [nom de l’entreprise] toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement ;
* ne jamais confier son identifiant/mot de passe ;
* 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 modifier les paramétrages du poste de travail ;
* ne pas installer de logiciels sans autorisation ;
* verrouiller son ordinateur dès qu’il quitte son poste de travail ;
* ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas ;
* ne pas copier les données de l’entreprise sur un support externe, sauf accord du supérieur hiérarchique ou du service informatique.

Les visiteurs ou prestataires extérieurs ne peuvent avoir accès aux outils informatiques et de communication sans l’accord préalable du service informatique. Ils doivent alors s’engager à respecter et faire respecter la présente charte par leurs propres salariés.

1. **Les moyens informatiques**
2. Configuration du poste de travail

[Nom de l’entreprise] met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l’accomplissement de ses fonctions.

L’'utilisateur ne doit pas :

* modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle ;
* connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par l’équipe informatique interne.
* déplacer l’équipement informatique (sauf s’il s’agit d’un «équipement mobile»)
* nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires (logiciels de consultation de fichiers multimédia) est subordonnée à l’accord du service informatique interne.

1. Equipements mobiles

On entend par « équipements mobiles » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB, etc).

L’utilisation de smartphones ou Blackberry pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu’ils contiennent.

L’utilisateur qui reçoit un matériel en prêt en assure la garde et la responsabilité et doit informer le service informatique en cas d’incident (perte, vol, dégradation) afin qu’il soit procédé aux démarches telles que la déclaration de vol ou de plainte. Il 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.

1. Internet

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle, de quelque nature qu’ils soient. Une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public, et ne met pas en cause l'intérêt et la réputation de l’institution, est admise.

1. Messagerie électronique

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail ni la sécurité du réseau informatique de [nom de l’entreprise].

Tout message qui comportera la mention expresse ou manifeste de son caractère personnel bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel. [Nom de l’entreprise] s’interdit d’accéder aux dossiers et aux messages identifiés comme « personnel » dans l’objet de la messagerie du salarié.

L’utilisation de la messagerie électronique doit se conformer aux règles d’usage définies par le service informatique interne en matière de volumétrie de la messagerie, taille maximale de l’envoi et de la réception d’un message, nombre limité de destinataires simultanés lors de l’envoi d’un message, gestion de l’archivage de la messagerie…

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes.

Les utilisateurs peuvent consulter leur messagerie à distance, à l’aide d’un navigateur (webmail). Les fichiers qui seraient copiés sur l’ordinateur utilisé par le salarié dans ce cadre doivent être effacés dès que possible de l’ordinateur utilisé.

En cas d’absence prolongée d’un salarié (longue maladie), le supérieur peut demander au service informatique, après accord de la direction des ressources humaines, le transfert des messages reçus.

[Nom de l’entreprise] dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

1. Téléphone

[Nom de l’entreprise] met à disposition des utilisateurs, pour l’exercice de leur activité professionnelle, des téléphones fixes et/ou mobiles. L’utilisation du téléphone à titre privé est admise à condition qu’elle demeure raisonnable.

Des restrictions d’utilisation par les salariés des téléphones fixes sont mises en place en tenant compte de leurs missions. A titre d’exemple, certains postes sont limités aux appels nationaux, d’autres peuvent passer des appels internationaux.

[Nom de l’entreprise] s’interdit de mettre en œuvre un suivi individuel de l’utilisation des services de communications. Seules des statistiques globales sont réalisées sur l’ensemble des appels afin de vérifier que les consommations n’excèdent pas les limites des contrats passés avec les opérateurs.

[Nom de l’entreprise] s’interdit d’accéder à l’intégralité des numéros appelés via l’autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d’utilisation manifestement anormale, le service informatique, sur demande [nom de la personne compétente. Ex : DAF, DRH, DG…], se réserve le droit d’accéder aux numéros complets des relevés individuels.

1. **L’administration du système d’information**

Afin de surveiller le fonctionnement et de garantir la sécurité du système d’information, différents dispositifs sont mis en place.

1. Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information pour [nom de l’entreprise] et d'assurer la sécurité et la confidentialité des données sont mis en œuvre. Il s’agit notamment du filtrage des sites Internet, de l’élimination des courriels non sollicités, du blocage de certains protocoles (*peer to peer*, messagerie instantanée...).

1. Les systèmes automatiques de traçabilité

Le service informatique de [nom de l’entreprise] opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Il s’appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, postes de travail et objet de l’évènement.

Le service informatique est le seul destinataire de ces informations qui sont effacées à l’expiration d’un délai de trois mois.

1. Gestion du poste de travail

A des fins de maintenance informatique, le service informatique interne de [nom de l’entreprise] peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation expresse de l'utilisateur.

Dans le cadre de mises à jour et évolutions du système d’information, et lorsqu’aucun utilisateur n’est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l’environnement technique des postes de travail. Il s’interdit d’accéder aux contenus.

1. **Procédure applicable lors du départ de l’utilisateur**

Lors de son départ, l’utilisateur doit restituer au service de l’informatique interne les matériels mis à sa disposition. Il doit préalablement effacer ses fichiers et données privées. Aucune copie des documents professionnels ne peut être effectuée par le salarié, sauf accord exprès de [nom de l’entreprise].

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.

1. **Responsabilités – Sanctions**

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d’engager la responsabilité de l’utilisateur et d’entraîner des sanctions internes à son encontre. Le non-respect des lois et textes applicables en matière de sécurité des systèmes d’information est susceptible de sanctions pénales prévues par la loi[[2]](#footnote-2).

1. **Entrée en vigueur de la charte**

La présente charte est applicable à compter du…

1. Loi n°78-17 relative à l’informatique, aux fichiers et aux libertés du 6 janvier 1978 modifiée et Règlement général sur la protection des données personnelles (RGPD) n° (UE) 2016/679 du 27 avril 2016 [↑](#footnote-ref-1)
2. Loi n°78-17 relative à l’informatique, aux fichiers et aux libertés du 6 janvier 1978 modifiée qui insère les articles 226-16 à 226-24 et articles R. 625-10 à R. 625-13 du Code pénal ;

   Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique (articles 323-1 à 323-3 du Code pénal) ;

   Loi n°2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique (LCEN). [↑](#footnote-ref-2)