charte informatique

de L’ENTREPRISE

# TABLE DES MATIERES

[TABLE DES MATIERES 2](#_Toc147149466)

[1. Validité du document 4](#_Toc147149467)

[Historique des révisions 4](#_Toc147149468)

[Approbation 4](#_Toc147149469)

[Introduction 5](#_Toc147149470)

[Contexte 5](#_Toc147149471)

[Objectif 5](#_Toc147149472)

[Organisation 5](#_Toc147149473)

[Définitions 5](#_Toc147149474)

[Articles 6](#_Toc147149475)

[Article 1 : Engagements 6](#_Toc147149476)

[Article 2 : Accès aux locaux 6](#_Toc147149477)

[Article 3 : Accès aux ressources 6](#_Toc147149478)

[Article 3 : l’utilisation des moyens informatiques 7](#_Toc147149479)

[Article 4 : Respect des obligations 7](#_Toc147149480)

[Article 5 : Protection des données personnelles et de la propriété intellectuelle 8](#_Toc147149481)

[Article 6 : Utilisation d’internet 8](#_Toc147149482)

[Article 7 : Utilisation de la messagerie d’entreprise 8](#_Toc147149483)

[Article 8 : Postes de travail 9](#_Toc147149484)

[Article 9 : Equipements nomades 9](#_Toc147149485)

[Connexion des supports amovibles 9](#_Toc147149486)

[Actions requises lors d’un déplacement 9](#_Toc147149487)

[Utilisation des téléphones mobiles 9](#_Toc147149488)

[Dans les locaux de l’entreprise, l’utilisation des téléphones mobiles personnels est autorisée dans les limites suivantes : 9](#_Toc147149489)

[Enjeux de sécurité du télétravail 10](#_Toc147149490)

[Article 10 : Publication sur les réseaux sociaux en cas des activités professionnelles 10](#_Toc147149491)

[Article 11 : Manquement à la charte 11](#_Toc147149492)

[Engagement de confidentialité pour les personnes ayant vocation à manipuler des donnees à caractere personnel 11](#_Toc147149493)

[ENGAGEMENT utilisateur 12](#_Toc147149494)

[annexe : Rappel des principes lois françaises 12](#_Toc147149495)

# Validité du document

## Historique des révisions

|  |  |  |
| --- | --- | --- |
| Version | Date | Motif de l’évolution |
| 01 | XX/XX/XXXX | Création du document |

## Approbation

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Modifié par | Vérifié par | Approuvé par |
| 01 | Information | Prénom Nom | Création du document |

# Introduction

## Contexte

L'entreprise met à disposition de tous les utilisateurs des équipements informatiques tels que des ordinateurs, des logiciels, et des moyens de communication tels que la messagerie et l'accès à Internet. Ces ressources permettent à chaque utilisateur d'exercer ses activités professionnelles en respectant les lois et les règlements techniques établis par l'entreprise.

L'utilisation de ces ressources comporte des risques, qui affectent à la fois les systèmes informatiques et les informations stockées, notamment les données personnelles et les données soumises à des réglementations nationales ou internationales. Ces risques concernent l'intégrité, la disponibilité, et la confidentialité des données. En conséquence, l'entreprise, ainsi que sa réputation, peuvent être menacées par un usage inapproprié, des cyberattaques ou l'introduction de virus. Il est donc essentiel que tous les utilisateurs des ressources informatiques et de communication au sein de l'entreprise soient pleinement conscients de ces risques.

Pour faire face à ces risques, il est impératif que les utilisateurs respectent strictement les règles de conduite énoncées dans ce document et prennent conscience de leur responsabilité personnelle en cas de non-respect de ces règles.

Cette charte établit les directives concernant l'utilisation des ressources informatiques et des réseaux au sein de l'entreprise.

## Objectif

Les objectifs de cette charte sont les suivants :

* Informer les utilisateurs de leurs droits et responsabilités en ce qui concerne l'utilisation des ressources informatiques ;
* Sensibiliser les utilisateurs aux enjeux de sécurité associés à cette utilisation.

## Organisation

Cette charte est applicable à l'ensemble du personnel de l'entreprise, ainsi qu'à toutes les personnes, qu'elles soient permanentes ou temporaires, qui utilisent les ressources informatiques de l'entreprise.

## Définitions

**Les ressources informatiques**, sans que cette liste soit exhaustive, englobent les moyens informatiques, les dispositifs de stockage de données, ou de gestion locale, ainsi que ceux auxquels il est possible d'accéder à distance, que ce soit directement ou via le réseau de l'entreprise. Ce terme comprend :

* Les équipements réseau,
* Les systèmes d'information gérés par l'entreprise,
* Les postes de travail,
* Les dispositifs d'acquisition, de stockage et de restitution tels que les clés USB,
* Les équipements d'impression,
* Les systèmes d'information pour la recherche et la gestion,
* Les applications informatiques associées, ainsi que divers services de communication d'informations comme le web et la messagerie.

**Services Internet** se réfère à la mise à disposition, qu'elle soit effectuée par des serveurs locaux ou distants, de moyens permettant des échanges et l'accès à diverses informations, tels que le Web, la messagerie, les forums, la téléphonie IP (Internet Protocol), la visioconférence, et d'autres moyens similaires.

**Le terme Utilisateur** englobe toute personne, quelle que soit sa situation ou son statut, qui a accès aux ressources informatiques et aux services Internet de l'entreprise ou qui les utilise.

**Équipements nomades** désigne l'ensemble des dispositifs techniques communicants, tels que les ordinateurs portables, les tablettes, les smartphones, les montres connectées, les clés 3G, les dispositifs Bluetooth ou Wifi, ainsi que les supports amovibles comme les clés USB et les cartes mémoire.

# Articles

## Article 1 : Engagements

L'entreprise prend les engagements suivants :

* Elle s'engage à mettre à disposition les systèmes et les outils nécessaires pour garantir au mieux la sécurité globale des réseaux, des données, des applications et des accès aux postes de travail.
* Elle veille à ce que les procédures mises en place pour répondre aux exigences de sécurité des ressources informatiques et de communication soient respectées. Cela comprend l'attribution des accès protégés aux nouveaux employés, la révocation des droits des employés qui quittent l'entreprise, ainsi que la gestion des mots de passe.

L'utilisateur s'engage à :

* Ne pas détourner le système pour une utilisation autre que celle prévue par l'entreprise.
* Respecter rigoureusement les règles énoncées dans ce document.
* Signaler tout incident de sécurité constaté ou suspecté en envoyant un e-mail au référent informatique.

## Article 2 : Accès aux locaux

L'accès aux locaux de l'entreprise est exclusivement réservé aux salariés de l'entreprise. Tout autre individu, qu'il s'agisse d'un intervenant extérieur, d'un client, d'un candidat ou d'un partenaire, doit faire l'objet d'une surveillance ou d'une assistance particulière.

## Article 3 : Accès aux ressources

L'utilisation des ressources informatiques, des services Internet et de l'accès au réseau est destinée exclusivement à l'activité professionnelle des utilisateurs, conformément à la législation en vigueur. L'utilisation des ressources informatiques partagées au sein de l'entité et la connexion d'un équipement privé et extérieur (comme un ordinateur, un commutateur, un modem, une borne d'accès sans fil) au réseau nécessitent une autorisation préalable du responsable de l'entité.

Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être transmises, même temporairement, à une tierce personne. Elles peuvent être révoquées à tout moment et expirent dès que l'activité professionnelle qui les justifiait prend fin.

Chaque utilisateur est responsable de l'utilisation des ressources informatiques auxquelles il a accès. Il s'engage à ne pas perturber délibérément le bon fonctionnement des ressources informatiques et des réseaux, que ce soit par des manipulations inappropriées du matériel ou par l'introduction de logiciels nuisibles tels que virus, chevaux de Troie ou bombes logiques. Cela s'applique à l'intégrité des outils informatiques ainsi qu'aux relations internes et externes de l'entreprise.

L'autorisation d'utiliser les moyens et ressources informatiques de l'entreprise cesse immédiatement en cas de départ de l'utilisateur de l'entreprise ou de modification de ses fonctions qui justifiaient une habilitation spécifique d'accès à ces ressources. En cas de départ, l'utilisateur doit restituer tout le matériel fourni et effacer tous les fichiers et données personnels de son poste de travail, sauf autorisation écrite de son supérieur hiérarchique. Si l'équipement appartient à l'utilisateur, il doit également effacer tous les documents et fichiers liés à l'entreprise.

Chaque accès est strictement réservé à faciliter les activités professionnelles de son titulaire dans le cadre de sa mission au sein de sa structure, excluant toute utilisation à des fins personnelles.

Les comptes utilisateurs sont personnels et nominatifs. Chaque utilisateur est responsable de leur utilisation et s'engage à ne pas partager ses identifiants et mots de passe avec des tiers, que ce soit à l'intérieur ou à l'extérieur de l'entreprise. En cas de soupçon de violation de son compte, l'utilisateur doit en informer l'administrateur. La confidentialité des informations et des données est essentielle, et leur diffusion est strictement interdite, sauf pour les diffusions internes nécessaires aux intérêts de l'entreprise et conformes aux procédures en vigueur.

Sous l'autorité de la direction de l'entreprise, les administrateurs des ressources informatiques, des réseaux et des services Internet sont habilités à prendre des mesures conservatoires en cas d'urgence ou en cas de manquements graves ou répétés aux règles de sécurité.

## Article 3 : l’utilisation des moyens informatiques

L'entreprise a la possibilité de prendre des mesures légales à l'encontre des utilisateurs en cas d'utilisation des ressources à des fins illégales, illicites ou pouvant porter préjudice à l'entreprise.

## Article 4 : Respect des obligations

Chaque utilisateur doit s'engager à respecter les bonnes pratiques informatiques énumérées ci-dessous :

* Utiliser l'authentification multi-facteurs (MFA) lorsque cela est possible pour renforcer la sécurité des accès aux ressources informatiques.
* Ne jamais divulguer son identifiant ou son mot de passe à un tiers.
* Verrouiller son ordinateur dès qu'il quitte son poste de travail.
* Ne pas accéder, essayer d'accéder ou supprimer des informations qui ne relèvent pas de ses responsabilités.
* Protéger ses fichiers confidentiels liés à son travail ou contenant des données personnelles.
* Ne jamais laisser des supports informatiques contenant des données confidentielles liées au travail ou des données personnelles en accès libre.

## Article 5 : Protection des données personnelles et de la propriété intellectuelle

En ce qui concerne le traitement de données personnelles, l'utilisateur doit se conformer au règlement (UE) 2016/679 du Parlement Européen et du Conseil du mai 2016, qui concerne la protection des données à caractère personnel et la libre circulation de ces données, communément appelé le RGPD.

L'utilisateur est informé que les données à caractère personnel le concernant seront conservées par le service informatique pendant toute la durée de la relation contractuelle et conformément aux délais de prescription en vigueur.

De plus, l'utilisateur est informé qu'il dispose de droits conformes au RGPD pour des motifs légitimes reconnus par l'entité, notamment le droit d'accès, de rectification, d'opposition, de suppression, de portabilité, de limitation du traitement, en ce qui concerne toutes les informations le concernant.

L'entreprise a nommé un Délégué à la Protection des Données pour assurer la conformité avec le RGPD.

Il est également important de noter que l'utilisateur ne doit pas faire de copies de logiciels à des fins quelconques, telles que la reproduction, le téléchargement, la copie, la diffusion, la modification ou l'utilisation de logiciels, de bases de données, de pages web, d'images, de photographies ou d'autres créations protégées par le droit d'auteur ou tout autre droit privatif, sans avoir obtenu au préalable l'autorisation des titulaires de ces droits.

## Article 6 : Utilisation d’internet

Internet est un outil de travail ouvert à des usages professionnels, et son utilisation doit être conforme à des principes généraux ainsi qu'aux règles spécifiques établies par les différents sites web qui le proposent. Par conséquent, chaque utilisateur doit faire preuve de discrétion lors de la publication ou de la collecte d'informations concernant les activités de l'entreprise.

Il est strictement interdit à l'utilisateur d'usurper l'identité d'une autre personne ou d'intercepter les communications entre tiers. De plus, l'utilisateur ne doit pas utiliser ces services pour partager ou rendre accessibles à des tiers des données et des informations confidentielles.

En cas de cessation, même temporaire, de l'activité professionnelle, toutes les autorisations d'accès peuvent être révoquées à tout moment.

L'accès aux sites internet à caractère pornographique, dangereux, de téléchargement illégal, de jeux en ligne ou de divertissements est formellement interdit.

**Les utilisateurs sont informés et acceptent que les traces de leurs connexions soient conservées pendant au moins un an**.

## Article 7 : Utilisation de la messagerie d’entreprise

La messagerie mise à disposition des utilisateurs est destinée exclusivement à un usage professionnel. Toutefois, l'utilisation ponctuelle et raisonnable de la messagerie à des fins personnelles est tolérée, à condition qu'elle ne perturbe pas le déroulement des missions des salariés ni la sécurité du réseau informatique.

Les utilisateurs doivent éviter d'envoyer des copies de messages à un nombre excessif de destinataires et veiller à limiter la diffusion des messages aux seuls destinataires concernés, afin d'éviter la saturation inutile de la messagerie et la dégradation du service.

Chaque utilisateur doit prendre les mesures nécessaires pour conserver les messages qui pourraient être indispensables ou simplement utiles en tant qu'éléments de preuve.

Il est important de noter que tous les messages, qu'ils soient entrants ou sortants, peuvent faire l'objet d'un filtrage automatique pour vérifier que leur contenu n'est pas malveillant. En cas de détection de virus par le filtrage, le message ne sera pas distribué, et des informations complémentaires pourront être demandées aux personnes concernées.

Il est recommandé aux utilisateurs de la messagerie de procéder régulièrement au nettoyage de leur boîte de réception en supprimant ou en archivant les messages devenus inutiles. De plus, il est conseillé d'éviter d'ouvrir des courriels suspects, de cliquer sur des pièces jointes ou des liens provenant d'expéditeurs inconnus.

## Article 8 : Postes de travail

L'utilisateur a la responsabilité de contribuer à la sécurité globale et à une utilisation rationnelle et équitable des ressources informatiques, dans le but d'éviter leur saturation ou leur utilisation abusive à des fins personnelles.

Chaque poste de travail de l'utilisateur doit être équipé d'un logiciel antivirus actif et mis à jour. L'utilisateur est tenu de s'assurer que son poste dispose d'une solution antivirus conforme aux exigences de l'entreprise.

Le partage de dossiers et de fichiers en réseau entre utilisateurs doit respecter les exigences de la charte informatique en matière de confidentialité et d'intégrité des données. Pour chaque partage, des autorisations nominatives (utilisateur ou groupe d'utilisateurs) et des attributs d'accès spécifiques doivent être établis, tels que la lecture ou l'écriture.

La configuration des ordinateurs portables doit être conforme aux règles de sécurité en vigueur au sein de l'entreprise, ce qui inclut l'utilisation d'antivirus, la mise à jour régulière des systèmes et la mise en place de la double authentification lorsque nécessaire.

La sécurité des données doit être respectée par les utilisateurs, où qu'ils se trouvent, afin de préserver l'intégrité et la confidentialité des informations de l'entreprise.

## Article 9 : Equipements nomades

**Gestion des supports amovibles** :

Les disques amovibles peuvent constituer une source potentielle d'attaques contre la sécurité. Il est impératif de maintenir le logiciel d'analyse activé en permanence pour se prémunir contre ces menaces. Lors de l'insertion d'une clé USB ou d'un disque amovible, l'utilisateur doit attendre la fin de l'analyse du support avant de l'utiliser.

**Précautions lors des déplacements** : Lorsque cela est techniquement possible, les dispositifs d'information et de communication nomades doivent bénéficier d'une sécurisation spécifique, en fonction de la sensibilité des documents qu'ils peuvent stocker. De plus, lors des déplacements en transport en commun, il est recommandé d'éteindre l'ordinateur portable pour garantir le chiffrement des données transportées.

**Utilisation des réseaux Wi-Fi publics** : En situation de mobilité, il est préférable de se connecter à Internet en utilisant son abonnement téléphonique (3G ou 4G) plutôt que les réseaux Wi-Fi publics. Ces derniers sont souvent mal sécurisés et peuvent être surveillés ou usurpés par des pirates.

**Utilisation des téléphones mobiles** : Dans les locaux de l'entreprise, l'utilisation des téléphones mobiles personnels est autorisée dans certaines limites, notamment :

* Ne pas prendre de photos ni filmer à l'intérieur de l'entreprise sans autorisation.
* En cas de vol, de perte ou de détérioration du matériel, il est nécessaire de contacter immédiatement l'entreprise, qui prendra les mesures appropriées, telles que la déclaration aux assurances, la suppression des accès au système d'information, l'échange, la réparation ou le remplacement du matériel. En ce qui concerne les équipements personnels, il est également recommandé de prévenir l'entreprise afin que les administrateurs puissent prendre les mesures nécessaires, comme la suppression éventuelle des données, etc.
* L'utilisation des téléphones portables comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol. Par conséquent, il est conseillé de verrouiller automatiquement ces appareils lorsqu'ils ne sont pas utilisés pendant quelques minutes, afin de prévenir tout accès non autorisé aux données qu'ils contiennent. Il est également recommandé de désactiver l'affichage des courriers électroniques entrants sur l'écran de verrouillage du téléphone.

**Enjeux de sécurité liés au télétravail :**

En télétravail, il est essentiel :

* Il est essentiel de maintenir une séparation stricte entre les usages personnel et professionnel en créant des comptes distincts avec des droits limités, des mots de passe forts et en évitant le partage avec d'autres personnes.
* Chiffrer les disques durs et effectuer des sauvegardes régulières.
* Assurer le bon paramétrage de la box Internet, notamment en vérifiant le mot de passe d'accès administrateur, en le modifiant s'il est faible et en mettant à jour le logiciel interne.
* En ce qui concerne le Wi-Fi, activer l'option de chiffrement WPA2 ou WPA3 avec un mot de passe long et complexe, désactiver la fonction WPS et supprimer le Wi-Fi invité. Éviter les accès partagés avec des tiers.
* Utiliser des mots de passe longs et complexes.
* Limiter les applications installées aux seules provenant de plates-formes officielles.
* Respecter la charte informatique de l'entreprise.
* Faire preuve de vigilance face aux tentatives d'hameçonnage.
* Prendre des précautions lors de l'utilisation des équipements et des accès professionnels.

## Article 10 : Publication sur les réseaux sociaux en cas des activités professionnelles

La charte d'utilisation des réseaux sociaux vise à définir les orientations, le ton et la position que l'entreprise souhaite adopter sur les médias sociaux. Elle sert également à informer sur les obligations concernant le contenu diffusé. Voici les principales directives de cette charte :

* Les personnes responsables des comptes publics de l'entreprise sur les réseaux sociaux doivent suivre les directives fournies par l'entreprise.
* Une fois que vous avez indiqué votre affiliation à l'entreprise sur les réseaux sociaux, tout ce que vous publiez doit refléter les valeurs de l'entreprise et respecter les principes éthiques de celle-ci.
* Il est strictement interdit de partager un contenu confidentiel client ou de divulguer des informations de propriété intellectuelle sur les réseaux sociaux.
* Le comportement en ligne doit être en accord avec le code de conduite éthique.
* Il est interdit d'adopter un comportement en ligne inacceptable, telles que des remarques désobligeantes, des tentatives de maltraitance, d'intimidation ou de harcèlement, des insultes, ou la publication de contenu haineux, diffamatoire, menaçant, discriminatoire ou pornographique.
* Il est interdit de publier du contenu discriminatoire basé sur des critères tels que la culture, la langue, la religion, l'orientation sexuelle, le genre, la race, l'origine nationale, etc.
* La protection constante des données confidentielles et de toute autre information personnelle concernant les clients est essentielle.
* Les Conditions Générales d'Utilisation (CGU) des réseaux sociaux utilisés doivent être respectées.
* Les mots de passe doivent répondre à des critères stricts, tels que leur longueur et leur aléatoire, et doivent être changés régulièrement. Ils doivent être considérés comme inviolables et ne doivent pas être partagés entre les utilisateurs.
* Lorsqu'un employé quitte l'entreprise, un processus de départ doit être suivi. Les accès aux réseaux sociaux doivent être révoqués pour les comptes ou profils personnels qui étaient liés à l'entreprise, et les mots de passe partagés doivent être modifiés.

## Article 11 : Manquement à la charte

Le non-respect des règles énoncées dans cette charte peut entraîner la suspension, voire la suppression, de l'accès aux outils de communication pour les contrevenants. En fonction de la gravité de l'infraction, des sanctions disciplinaires peuvent être prises conformément à la réglementation en vigueur dans la fonction publique territoriale, et une procédure pénale peut être engagée. Il est donc essentiel de respecter scrupuleusement les directives de cette charte pour éviter de telles conséquences.

# ENGAGEMENT utilisateur

En signant ce document, je déclare comprendre les droits, devoirs et les risques décrits dans la Charte Informatique, adhérer à celle-ci et m’engager à la respecter.

En cas de non-respect des principes énoncés dans cette charte, que ce soit intentionnel ou par négligence, l’utilisateur sera soumis à un processus disciplinaire interne dont la sanction pourra aller du simple avertissement au licenciement pour faute grave. Ces sanctions pourront être complétées par des poursuites judiciaires dans le cas ou L’entreprise aurait subi un lourd préjudice.

**L’entreprise à la possibilité de se retourner contre les utilisateurs en cas d’utilisation des ressources à fins illégales, illicites, de nature à porter atteinte à l’entreprise ou en cas d'abus ou d'usages contraire à la charte**

Pour la bonne forme, nous vous serions obligés de bien vouloir nous retourner le deuxième exemplaire de cette annexe revêtu de votre signature précédée de la mention "lu et approuvé".

Fait à \_\_\_\_\_\_\_\_\_\_\_\_\_, le \_\_ / \_\_ / \_\_\_\_

En deux exemplaires.

Nom Prénom :

# Annexe : Rappel des principes lois françaises

Il est rappelé que toute personne sur le sol français doit respecter la législation française en particulier dans le domaine de la sécurité informatique.

Protection des Données personnelles :

* Directive 95/46/CE du Parlement Européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, publiée au journal officiel n° L 281 du 23/11/1995

Code Civil :

* Article 9 : droit au respect de la vie privée Code du travail :
* Articles L. 1121-1, L.2323-32 et L.1224-4

Protection des Données personnelles :

* Loi n°78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés, dite Informatique et Libertés, modifiée le 6 août 2004

Code pénal :

* Diffamation publique et diffamation privée : Loi du 29 juillet 1881 et R621-1 et R621-2
* Protection des mineurs et pornographie : articles 227-23 et 227-24 –
* Atteintes à la vie privée : articles 226-1 à 226-7
* Fraude informatique : articles 323-1 à 323-5
* Protection du secret des correspondances : article 226-15 alinéa 1

Code de la propriété intellectuelle :

* Contrefaçon (droit d’auteur) : articles L.335-2 et L.335-3