CHARTE INFORMATIQUE

MODÈLE RGPD

Document à signer par chaque collaborateur — Modèle personnalisable

Entreprise : ***[Nom de l'entreprise]*** Version : ***[Version]***

Date d'entrée en vigueur : ***[Date]*** Rédigée par : ***[Responsable]***

1 OBJET ET CHAMP D'APPLICATION

La présente charte informatique (ci-après « la Charte ») définit les règles d'utilisation des systèmes d'information mis à disposition des collaborateurs de ***[Nom de l'entreprise]*** (ci-après « l'Entreprise »).

Elle s'applique à **tout collaborateur, prestataire, stagiaire ou visiteur** ayant accès aux ressources informatiques de l'Entreprise, quel que soit le lieu d'utilisation (locaux, télétravail, déplacement).

Les ressources concernées comprennent notamment :

- Les ordinateurs, tablettes, téléphones professionnels et tout équipement numérique fourni par l'Entreprise
- Le réseau informatique, Wi-Fi et accès Internet de l'Entreprise
- Les logiciels, applications et services en ligne (SaaS) mis à disposition
- Les serveurs, bases de données et espaces de stockage partagés
- La messagerie électronique professionnelle et les outils de communication

Important : Cette charte a valeur contractuelle. Sa violation peut entraîner des sanctions disciplinaires, y compris le licenciement, ainsi que des poursuites civiles ou pénales.

2 UTILISATION DU MATÉRIEL INFORMATIQUE

Le matériel informatique mis à disposition est destiné à un usage **principalement professionnel**. Un usage personnel raisonnable est toléré dans les conditions définies ci-après.

- Le collaborateur est responsable du matériel qui lui est confié et doit le conserver en bon état
- Tout incident, perte, vol ou dégradation doit être signalé immédiatement au service informatique
- L'installation de logiciels non autorisés est **strictement interdite**
- Le téléchargement de contenus illégaux (logiciels piratés, fichiers protégés) est interdit et engage la responsabilité du collaborateur
- Le matériel professionnel ne doit pas être prêté à des tiers, y compris des membres de la famille
- Les mises à jour de sécurité ne doivent pas être différées ou désactivées

L'Entreprise se réserve le droit d'auditer les équipements mis à disposition afin de vérifier le respect de la présente Charte.

3 INTERNET ET MESSAGERIE ÉLECTRONIQUE

L'accès à Internet est fourni dans le cadre de l'activité professionnelle. Les usages personnels doivent rester marginaux et ne pas nuire à la productivité ni à la sécurité du réseau.

Usages autorisés	Usages interdits
Navigation professionnelle sur sites légaux	Sites de jeux d'argent, streaming illégal, téléchargement P2P
Consultation ponctuelle de sites personnels	Contenus à caractère violent, pornographique, haineux
Utilisation des outils collaboratifs autorisés	Contournement du pare-feu (proxy, VPN non autorisé)
Messagerie professionnelle pour usage pro	Envoi de données confidentielles depuis messagerie personnelle

Phishing / Hameçonnage : Ne cliquez jamais sur un lien ou pièce jointe suspect. En cas de doute, signalez immédiatement au service informatique avant toute action.

CHARTE INFORMATIQUE

Suite — *[Nom de l'entreprise]*

4 MOTS DE PASSE ET AUTHENTIFICATION

La sécurité des accès repose sur chaque collaborateur. Les règles suivantes sont **obligatoires** :

- Tout mot de passe doit comporter au minimum **12 caractères**, incluant majuscules, minuscules, chiffres et caractères spéciaux
- Les mots de passe ne doivent pas être partagés, communiqués, notés sur papier ou enregistrés dans un navigateur non sécurisé
- Chaque compte (messagerie, ERP, VPN, etc.) doit disposer d'un mot de passe **unique**
- Les mots de passe doivent être renouvelés tous les *[90/180]* jours ou immédiatement en cas de soupçon de compromission
- L'authentification à deux facteurs (MFA) est **obligatoire** sur tous les accès distants et comptes sensibles
- L'utilisation d'un gestionnaire de mots de passe agréé par l'Entreprise est **recommandée**

Gestionnaire autorisé : *[Bitwarden / KeePass / Autre]* — Se rapprocher du service informatique pour la configuration.

5 PROTECTION DES DONNÉES PERSONNELLES (RGPD)

L'Entreprise traite des données à caractère personnel dans le cadre de son activité. Chaque collaborateur est acteur de leur protection :

- Les données personnelles (clients, prospects, salariés) ne doivent être consultées que dans le cadre des missions professionnelles
- Tout transfert de données hors de l'Union Européenne doit faire l'objet d'une autorisation préalable du DPO / responsable de traitement
- Les données sensibles (santé, opinions, données bancaires) bénéficient d'une protection renforcée et ne peuvent être partagées sans autorisation explicite
- En cas de violation de données (perte, vol, accès non autorisé), le collaborateur doit immédiatement alerter le DPO : *[Nom DPO — email DPO]*
- La copie de données personnelles sur des supports personnels (clé USB, cloud personnel) est **interdite**

Obligation légale : Le RGPD impose une notification à la CNIL dans les **72 heures** suivant la découverte d'une violation de données (Art. 33). Tout retard de signalement interne engage la responsabilité du collaborateur.

6 TÉLÉTRAVAIL ET ACCÈS DISTANTS

Le télétravail nécessite des précautions spécifiques pour maintenir le niveau de sécurité de l'Entreprise :

- Seuls les équipements fournis ou expressément autorisés par l'Entreprise doivent être utilisés
- La connexion au système d'information depuis l'extérieur doit obligatoirement passer par le **VPN de l'Entreprise**
- Les réseaux Wi-Fi publics (café, hôtel, gare) sont **interdits** sans VPN actif
- L'écran doit être verrouillé dès que le collaborateur s'éloigne de son poste (touche Windows + L)
- Les membres du foyer ne doivent pas avoir accès aux équipements professionnels
- Les documents professionnels imprimés à domicile doivent être déchiquetés

7 RÉSEAUX SOCIAUX ET COMMUNICATION EXTERNE

- Le collaborateur ne doit pas divulguer d'informations confidentielles sur les réseaux sociaux, même dans un contexte apparemment privé
- Toute prise de parole au nom de l'Entreprise sur les médias numériques doit être expressément autorisée
- Le collaborateur reste personnellement responsable de ses publications en ligne, même hors temps de travail, si elles portent atteinte à l'image de l'Entreprise

CHARTE INFORMATIQUE

Sanctions et signature — *[Nom de l'entreprise]*

8 SIGNALEMENT DES INCIDENTS

Tout collaborateur ayant connaissance ou suspicion d'un incident de sécurité informatique est tenu de le signaler **sans délai** :

Type d'incident	Contact immédiat	Délai
Perte / vol d'équipement professionnel	Service informatique + responsable hiérarchique	Immédiat
Suspicion de piratage / intrusion	RSSI / DSI : *[Contact]*	Immédiat
Violation de données personnelles	DPO : *[Contact]*	Immédiat (72h max CNIL)
Réception d'un message de rançon	RSSI + Direction + ne pas payer	Immédiat
Hameçonnage reçu (phishing)	Service informatique	Dans la journée

Contact unique sécurité 24h/24 : ***[Numéro / email d'urgence]***

9 SANCTIONS

Tout manquement aux dispositions de la présente Charte est susceptible d'entraîner des sanctions proportionnées à la gravité des faits :

Niveau	Exemple de manquement	Sanction possible
Mineur	Usage personnel excessif d'Internet	Avertissement oral ou écrit
Modéré	Installation de logiciel non autorisé	Mise en demeure, blâme
Grave	Partage de mot de passe, non-signalement d'incident	Mise à pied, licenciement pour faute
Très grave	Vol de données, sabotage, acte malveillant	Licenciement pour faute grave + poursuites pénales

Les dispositions pénales du Code Pénal (art. 323-1 à 323-7) relatives aux atteintes aux systèmes de traitement automatisé de données (STAD) s'appliquent indépendamment des sanctions disciplinaires internes.

10 MISE À JOUR DE LA CHARTE

La présente charte peut être mise à jour à tout moment. Toute modification substantielle sera portée à la connaissance des collaborateurs avec un délai de prévenance d'au moins **15 jours**. La version en vigueur est accessible sur : *[Intranet / emplacement partagé]*.

✎ ATTESTATION DE PRISE DE CONNAISSANCE ET D'ACCEPTATION

Je soussigné(e), reconnais avoir pris connaissance de la présente Charte Informatique de *[Nom de l'entreprise]* , en comprendre le contenu et m'engage à respecter l'ensemble des dispositions qui y sont mentionnées.

Collaborateur / Prestataire	Pour l'Entreprise (DRH / Responsable)
Nom et prénom :	Nom et prénom :
Fonction / Poste :	Fonction :
Date :	Date :
Signature :	Signature et cachet :

Besoin d'un accompagnement pour déployer et personnaliser cette charte ?

ayinedjimi-consultants.fr/contact