



# Charte d'Utilisation des Systèmes d'Information

Modèle adapté aux TPE-PME, associations et collectivités — à personnaliser, faire approuver par la direction et signer par chaque utilisateur.

**Mode d'emploi :** (1) Remplacez tous les champs *[entre crochets]* par les informations de votre structure. (2) Faites valider par votre direction ou conseil d'administration. (3) Faites signer par chaque collaborateur, agent ou bénévole avant tout accès au SI. (4) Conservez l'exemplaire signé dans le dossier individuel. **Mise à jour recommandée :** annuelle ou après tout incident significatif.

## EN-TÊTE — À COMPLÉTER AVANT DIFFUSION

|                            |                                            |
|----------------------------|--------------------------------------------|
| Structure :                | [NOM COMPLET DE LA STRUCTURE]              |
| Adresse :                  | [Adresse — Code postal — Ville]            |
| Date d'entrée en vigueur : | [JJ/MM/AAAA]                               |
| Version :                  | 1.0                                        |
| Approuvée par :            | [NOM DU DIRIGEANT / DG / PRÉSIDENT]        |
| DPO désigné :              | [Nom et email du DPO — ou « Non désigné »] |

## PRÉAMBULE

[NOM DE LA STRUCTURE] met à la disposition de ses collaborateurs, agents, bénévoles et stagiaires des ressources informatiques nécessaires à l'exercice de leurs missions. L'utilisation de ces ressources est soumise au respect de la présente charte, établie conformément au RGPD, aux recommandations de l'ANSSI et au droit applicable.

Le non-respect de cette charte peut entraîner des sanctions disciplinaires et, le cas échéant, des poursuites judiciaires.

## ARTICLE 1 — CHAMP D'APPLICATION

La présente charte s'applique à toute personne ayant accès aux systèmes d'information de [NOM DE LA STRUCTURE], notamment :

- Les salariés (CDI, CDD, temps partiel) et agents (titulaires et contractuels)
- Les stagiaires, apprentis et bénévoles disposant d'un accès informatique
- Les prestataires et intervenants extérieurs (pour la durée de leur mission)

**Systèmes concernés :** postes de travail fixes et portables, équipements mobiles (smartphones, tablettes), serveurs, applications métier, messagerie, réseaux Wi-Fi, accès distants (VPN).

## ARTICLE 2 — RÈGLES D'AUTHENTIFICATION ET D'ACCÈS

**2.1 Mots de passe :** Minimum 12 caractères, combinant majuscules, minuscules, chiffres et caractères spéciaux. Changement obligatoire tous les [90/180] jours. Interdiction de partager ou d'afficher son mot de passe.



**2.2 Authentification renforcée (MFA) :** Obligatoire pour l'accès à la messagerie, au VPN, aux applications métier et aux données sensibles.

**2.3 Verrouillage des postes :** Tout poste doit être verrouillé lors de toute absence, même courte (Windows + L / Cmd + Ctrl + Q). Verrouillage automatique : [5/10] minutes.

**2.4 Comptes personnels :** Chaque utilisateur dispose d'un compte nominatif. Les comptes génériques ou partagés sont interdits sauf exception documentée.

## ARTICLE 3 — UTILISATION DES RESSOURCES

**3.1 Usage professionnel :** Les ressources sont mises à disposition pour l'activité professionnelle. Une utilisation personnelle raisonnable est tolérée hors heures de travail, à condition qu'elle ne compromette pas la sécurité du SI.

**3.2 Usages interdits :** Téléchargement de logiciels non autorisés · Installation de matériel non approuvé · Navigation sur sites illicites · Utilisation à des fins commerciales personnelles · Contournement des mesures de sécurité.

**3.3 Messagerie électronique :** Interdiction de transmettre des données confidentielles sans chiffrement · Vigilance face aux emails suspects (phishing) · Signalement immédiat de tout email douteux au responsable informatique.

**3.4 Stockage et sauvegardes :** Les données professionnelles doivent être stockées sur les espaces autorisés (serveur, cloud professionnel). Interdiction de stocker des données sensibles sur des supports personnels non chiffrés.

## ARTICLE 4 — PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Chaque utilisateur s'engage à respecter le RGPD dans le cadre de son activité :

- Collecter uniquement les données nécessaires à la finalité poursuivie (minimisation)
- Ne pas transmettre de données personnelles à des tiers non autorisés
- Signaler immédiatement tout incident susceptible d'affecter des données personnelles
- Respecter les droits des personnes (accès, rectification, effacement)

**Référence légale :** Règlement UE 2016/679 (RGPD) · Loi Informatique et Libertés

## ARTICLE 5 — INCIDENTS ET SIGNALEMENT

Tout incident de sécurité (perte de matériel, virus, accès non autorisé, tentative de phishing, ransomware) doit être signalé **immédiatement** à :

- **Responsable informatique :** [Nom] — [Email] — [Téléphone]
- **DPO :** [Nom/contact ou « voir mentions légales »]

**Ne pas tenter de résoudre seul un incident grave.** Isoler le poste concerné (déconnecter du réseau) et attendre les instructions.

## ARTICLE 6 — SANCTIONS

Le non-respect de la présente charte peut entraîner :

- Des sanctions disciplinaires (avertissement, mise à pied, licenciement) selon la gravité et le contexte
- Des poursuites judiciaires en cas d'infraction pénale (fraude informatique, violation de données, diffusion de contenus illicites)
- La mise en jeu de la responsabilité personnelle de l'utilisateur



## PAGE DE SIGNATURE — À CONSERVER DANS LE DOSSIER INDIVIDUEL

Je soussigné(e), [Prénom Nom], en qualité de [Fonction] au sein de [NOM DE LA STRUCTURE], atteste avoir pris connaissance de la Charte d'Utilisation des Systèmes d'Information et m'engage à en respecter l'ensemble des dispositions.

|              |       |
|--------------|-------|
| Nom & Prénom | _____ |
| Fonction     | _____ |
| Date         | _____ |
| Signature    | _____ |