POLITIQUE INTERNE

Sécurité informatique et protection des données

[Nom du cabinet dentaire]
[Adresse complète]

Version 1.0 | [Date]
Conforme à la nLPD (RS 235.1)

1. Objet et champ d'application

La présente politique définit les règles de sécurité informatique et de protection des données applicables à l'ensemble du personnel du cabinet. Elle s'inscrit dans le cadre des obligations prévues par la Loi fédérale sur la protection des données (nLPD, RS 235.1), notamment l'Art. 8 relatif à la sécurité des données.

Elle s'applique à toutes les personnes ayant accès aux systèmes informatiques ou aux données du cabinet : praticiens, assistantes dentaires, personnel administratif, stagiaires, remplaçants et tout prestataire externe intervenant dans les locaux ou sur les systèmes du cabinet.

2. Responsabilités

Le responsable du cabinet est le responsable du traitement au sens de la nLPD. Il est personnellement responsable de la mise en œuvre, de la communication et du respect de la présente politique.

Chaque collaborateur est tenu de respecter les règles ci-dessous. Toute violation peut entraîner des mesures disciplinaires internes, sans préjudice des sanctions pénales prévues par la nLPD (Art. 60 à 63) et le Code pénal (Art. 321).

3. Accès aux systèmes informatiques

- Chaque collaborateur dispose d'un compte nominatif personnel. Les comptes partagés (« cabinet », « admin », « accueil ») sont interdits.
- Les identifiants de connexion sont strictement personnels et ne doivent jamais être communiqués, même à un collègue ou à un supérieur.
- Les mots de passe doivent comporter au minimum 12 caractères, combinant majuscules, minuscules, chiffres et symboles. Ils doivent être stockés exclusivement dans le coffre-fort de mots de passe mis à disposition par le cabinet.
- La double authentification (2FA) doit être activée sur tous les accès critiques : messagerie professionnelle, logiciel de gestion, sauvegardes cloud, accès à distance.
- Les comptes des collaborateurs quittant le cabinet sont désactivés immédiatement, le jour même du départ.

4. Utilisation des postes de travail

- Les postes de travail sont destinés à un usage exclusivement professionnel.
- L'écran doit être verrouillé à chaque départ du poste, même pour quelques instants
  Système Windows : *Windows+L*
  Apple MacOS : *Ctrl+Commande+Q*
- L'installation de logiciels non autorisés est interdite. Seul le prestataire informatique est habilité à installer ou mettre à jour des logiciels.
- Les mises à jour du système d'exploitation et des applications doivent être appliquées dès qu'elles sont disponibles. Les postes doivent être redémarrés au moins une fois par semaine pour permettre l'installation des correctifs.

5. Messagerie et communications

- Toute communication contenant des données patients identifiables (radiographies, diagnostics, numéros AVS, comptes-rendus) doit transiter par la messagerie chiffrée du cabinet (HIN Mail, ProtonMail ou équivalent conforme).
- L'envoi de données patients via des messageries grand public (Gmail, Hotmail, Bluewin, WhatsApp, SMS, réseaux sociaux) est strictement interdit.
- Les pièces jointes et liens contenus dans des e-mails inattendus ne doivent jamais être ouverts. En cas de doute, contacter le responsable du cabinet ou le prestataire informatique avant toute action.

6. Données patients et confidentialité

- Les données patients ne doivent jamais être copiées sur des supports personnels : clés USB, disques durs, téléphones, tablettes ou services cloud personnels.
- Les documents papier contenant des données patients doivent être détruits à l'aide d'une déchiqueteuse. Ils ne doivent jamais être jetés à la poubelle.
- Aucun dossier patient, radiographie imprimée ou document administratif contenant des données personnelles ne doit être laissé visible sur un comptoir, un bureau ou à proximité de zones accessibles aux patients.
- L'ensemble du personnel est soumis au secret professionnel (Art. 321 du Code pénal). Cette obligation s'applique pendant et après la durée du contrat de travail.

7. Appareils personnels (BYOD)

[Choisir l'option applicable au cabinet :]

Option A : L'utilisation d'appareils personnels (téléphones, tablettes, ordinateurs portables, clés USB) pour accéder aux données ou aux systèmes du cabinet est strictement interdite.

Option B : L'utilisation d'appareils personnels est autorisée sous les conditions suivantes : [préciser les conditions, par exemple : uniquement pour la consultation de l'agenda, avec chiffrement activé, verrouillage par code, et sans stockage local de données patients].

8. Sécurité physique

- Les locaux contenant des serveurs, des sauvegardes ou des équipements réseau doivent être verrouillés et accessibles uniquement au personnel autorisé.
- Les visiteurs, fournisseurs et techniciens externes ne doivent pas être laissés seuls dans des zones où des écrans affichent des données patients ou où des documents sensibles sont accessibles.
- Les écrans visibles depuis la salle d'attente ou les zones de passage doivent être positionnés de manière à ne pas exposer les données patients, ou équipés de filtres de confidentialité.

9. Réseau WiFi

- Le réseau principal du cabinet (postes de travail, serveur, imprimantes) est séparé du réseau invité destiné aux patients.
- Le mot de passe du réseau principal ne doit jamais être communiqué aux patients ni affiché dans les locaux accessibles au public.
- La connexion d'appareils personnels au réseau principal est interdite sauf autorisation explicite du responsable.

10. Procédure en cas d'incident

En cas de suspicion d'attaque informatique, de perte de données ou de tout événement inhabituel :

1. Isoler le poste concerné : débrancher le câble réseau, désactiver le WiFi. Ne pas éteindre le poste.
2. Informer immédiatement le responsable du cabinet.
3. Contacter le prestataire informatique du cabinet.
4. Documenter l'incident : photographier les écrans, noter l'heure exacte, décrire les symptômes observés.
5. Ne jamais tenter de résoudre le problème soi-même, ne pas payer de rançon, ne pas supprimer les messages suspects.

Les numéros d'urgence sont affichés à proximité de chaque poste de travail.

11. Sanctions en cas de non-respect

Toute violation de la présente politique peut entraîner des mesures disciplinaires internes pouvant aller jusqu'au licenciement, sans préjudice des responsabilités pénales personnelles prévues par la nLPD (Art. 60 à 63, amendes jusqu'à 250'000 CHF) et le Code pénal (Art. 321, violation du secret professionnel).

12. Mise à jour de la politique

La présente politique est revue et mise à jour au minimum une fois par an, ou à chaque changement significatif dans l'infrastructure informatique, les outils utilisés ou le cadre légal. Chaque mise à jour fait l'objet d'une nouvelle communication à l'ensemble du personnel et d'une signature actualisée.

Attestation de prise de connaissance

Je soussigné(e) atteste avoir lu, compris et accepté la présente politique de sécurité informatique et de protection des données du cabinet. Je m'engage à respecter l'ensemble des règles ci-dessus dans le cadre de mes fonctions.

Nom et prénom : _____

Fonction : _____

Date : _____

Signature du collaborateur : _____

Signature du responsable du cabinet : _____

Mentions légales et conditions d'utilisation

Ce document a été rédigé par **DentalSystems Sàrl** à des fins d'information et de sensibilisation. Il ne constitue pas un avis juridique et ne saurait engager la responsabilité de son auteur. Les informations contenues dans ce document sont à jour en date de mars 2026 et sont susceptibles d'évoluer en fonction des modifications législatives et réglementaires.

Pour toute question juridique relative à la nLPD, au RGPD ou à la protection des données dans le contexte médical, consultez un juriste spécialisé.

Propriété intellectuelle

Ce document est la propriété exclusive de DentalSystems Sàrl. L'ensemble de son contenu — textes, structure, mise en page et éléments graphiques — est protégé par le droit d'auteur conformément à la Loi fédérale sur le droit d'auteur et les droits voisins (LDA, RS 231.1).

Utilisation autorisée

Ce document est mis à disposition gratuitement et peut être librement téléchargé, imprimé et utilisé en interne au sein d'un cabinet dentaire ou d'une structure médicale, à condition que la mention de l'auteur (DentalSystems Sàrl) et le présent avis soient conservés intégralement.

Utilisations interdites

Sont strictement interdits, sauf accord écrit préalable de DentalSystems Sàrl :

- La revente ou la commercialisation de ce document, sous quelque forme que ce soit, y compris en version modifiée.
- La modification, l'adaptation ou la création d'œuvres dérivées présentées comme étant d'un autre auteur.
- La suppression, l'altération ou la dissimulation des mentions d'auteur, du logo ou des coordonnées de DentalSystems Sàrl.
- La redistribution à grande échelle par des tiers (sites de téléchargement, plateformes de partage, revendeurs) sans autorisation écrite.

Toute utilisation commerciale non autorisée constitue une violation du droit d'auteur et pourra faire l'objet de poursuites judiciaires.

Limitation de responsabilité

DentalSystems Sàrl décline toute responsabilité quant aux conséquences directes ou indirectes résultant de l'utilisation de ce document. L'utilisateur est seul responsable de l'adaptation de ces informations à sa situation spécifique. Ce document ne se substitue ni à un audit professionnel, ni à un conseil juridique.

DentalSystems Sàrl
Thomas Alvino, Technicien IT
www.dentalsystems.ch | talvino@dentalsystems.ch | +41 77 245 48 44