

INTERNE RICHTLINIE

IT-Sicherheit und Datenschutz

[Name der Zahnarztpraxis]
[Vollständige Adresse]

Version 1.0 | [Datum]
Konform mit dem DSG (SR 235.1)

1. Zweck und Geltungsbereich

Diese Richtlinie legt die Regeln zur IT-Sicherheit und zum Datenschutz fest, die für das gesamte Personal der Praxis gelten. Sie ist Teil der Pflichten nach dem Bundesgesetz über den Datenschutz (DSG, SR 235.1), insbesondere nach Art. 8 zur Datensicherheit.

Sie gilt für alle Personen, die Zugang zu den IT-Systemen oder zu den Daten der Praxis haben: Zahnärztinnen und Zahnärzte, Dentalassistentinnen, administratives Personal, Praktikantinnen und Praktikanten, Stellvertretungen sowie alle externen Dienstleister, die in den Räumlichkeiten oder an den Systemen der Praxis tätig sind.

2. Verantwortlichkeiten

Die Praxisleitung nimmt die Rolle des Verantwortlichen im Sinne des DSG wahr. Sie ist persönlich für die Umsetzung, die Bekanntmachung und die Einhaltung dieser Richtlinie verantwortlich.

Alle Mitarbeitenden sind verpflichtet, die nachstehenden Regeln einzuhalten. Jeder Verstoss kann interne disziplinarische Massnahmen nach sich ziehen, unter Vorbehalt der strafrechtlichen Sanktionen nach dem DSG (Art. 60 bis 63) und dem Strafgesetzbuch (Art. 321).

3. Zugang zu den IT-Systemen

- Alle Mitarbeitenden verfügen über ein persönliches, auf ihren Namen lautendes Konto. Gemeinsam genutzte Konten («Praxis», «Admin», «Empfang») sind verboten.
- Die Zugangsdaten sind streng persönlich und dürfen nie weitergegeben werden, auch nicht an Kolleginnen und Kollegen oder an Vorgesetzte.
- Passwörter müssen mindestens 12 Zeichen lang sein und Gross- und Kleinbuchstaben, Ziffern und Sonderzeichen kombinieren. Sie dürfen ausschliesslich im Passwort-Manager gespeichert werden, den die Praxis zur Verfügung stellt.
- Die Zwei-Faktor-Authentifizierung (2FA) muss für alle kritischen Zugänge aktiviert sein: geschäftliches E-Mail-Konto, Praxisverwaltungssoftware, Cloud-Backups, Fernzugriff.
- Die Konten von Mitarbeitenden, welche die Praxis verlassen, werden sofort deaktiviert, noch am Tag des Austritts.

4. Nutzung der Arbeitsplätze

- Die Arbeitsplätze sind ausschliesslich für die berufliche Nutzung bestimmt.
- Der Bildschirm muss bei jedem Verlassen des Arbeitsplatzes gesperrt werden, auch bei nur kurzer Abwesenheit

Windows: *Windows+L*

Apple macOS: *Ctrl+Cmd+Q*

- Die Installation nicht bewilligter Software ist verboten. Nur der IT-Dienstleister ist befugt, Software zu installieren oder zu aktualisieren.
- Updates des Betriebssystems und der Anwendungen müssen installiert werden, sobald sie verfügbar sind. Die Computer müssen mindestens einmal pro Woche neu gestartet werden, damit die Sicherheitsupdates installiert werden können.

5. E-Mail und Kommunikation

- Jede Kommunikation mit identifizierbaren Patientendaten (Röntgenbilder, Diagnosen, AHV-Nummern, Berichte) muss über das verschlüsselte E-Mail-System der Praxis laufen (HIN Mail, ProtonMail oder eine gleichwertige konforme Lösung).
- Der Versand von Patientendaten über frei verfügbare Mail- und Messaging-Dienste (Gmail, Hotmail, Bluewin, WhatsApp, SMS, soziale Netzwerke) ist streng verboten.
- Anhänge und Links in unerwarteten E-Mails dürfen nie geöffnet werden. Im Zweifelsfall vor jeder Handlung die Praxisleitung oder den IT-Dienstleister kontaktieren.

6. Patientendaten und Vertraulichkeit

- Patientendaten dürfen nie auf private Datenträger kopiert werden: USB-Sticks, Festplatten, Telefone, Tablets oder private Cloud-Dienste.
- Papirdokumente mit Patientendaten müssen mit einem Aktenvernichter vernichtet werden. Sie dürfen nie in den Abfall geworfen werden.
- Keine Patientenakte, kein ausgedrucktes Röntgenbild und kein administratives Dokument mit Personendaten darf sichtbar auf einer Theke, einem Schreibtisch oder in der Nähe von Bereichen liegen bleiben, die für Patientinnen und Patienten zugänglich sind.
- Das gesamte Personal untersteht dem Berufsgeheimnis (Art. 321 des Strafgesetzbuches). Diese Pflicht gilt während und nach der Dauer des Arbeitsvertrags.

7. Private Geräte (BYOD)

[Für die Praxis zutreffende Option wählen:]

Option A: Die Nutzung privater Geräte (Telefone, Tablets, Laptops, USB-Sticks) für den Zugriff auf Daten oder Systeme der Praxis ist streng verboten.

Option B: Die Nutzung privater Geräte ist unter folgenden Bedingungen erlaubt: [Bedingungen angeben, zum Beispiel: nur zum Einsehen der Agenda, mit aktivierter Verschlüsselung, Sperrcode und ohne lokale Speicherung von Patientendaten].

8. Physische Sicherheit

- Räume mit Servern, Datensicherungen oder Netzwerkgeräten müssen abgeschlossen und nur für berechtigtes Personal zugänglich sein.
- Externe Personen (Besuchende, Lieferanten, Technikerinnen und Techniker) dürfen in Bereichen, in denen Bildschirme Patientendaten anzeigen oder sensible Dokumente zugänglich sind, nicht allein gelassen werden.
- Bildschirme, die vom Wartezimmer oder von Durchgangsbereichen aus sichtbar sind, müssen so ausgerichtet sein, dass keine Patientendaten einsehbar sind, oder mit Blickschutzfiltern ausgestattet werden.

9. WLAN

- Das Hauptnetz der Praxis (Arbeitsplätze, Server, Drucker) ist vom Gastnetz für Patientinnen und Patienten getrennt.
- Das Passwort des Hauptnetzes darf nie an Patientinnen und Patienten weitergegeben oder in öffentlich zugänglichen Räumen ausgehängt werden.
- Das Verbinden privater Geräte mit dem Hauptnetz ist verboten, ausser mit ausdrücklicher Bewilligung der Praxisleitung.

10. Vorgehen bei einem Vorfall

Bei Verdacht auf einen Cyberangriff, einen Datenverlust oder ein anderes ungewöhnliches Ereignis:

1. Den betroffenen Computer isolieren: Netzkabel ausstecken, WLAN deaktivieren. Den Computer nicht ausschalten.
2. Sofort die Praxisleitung informieren.
3. Den IT-Dienstleister der Praxis kontaktieren.
4. Den Vorfall dokumentieren: Bildschirme fotografieren, genaue Uhrzeit notieren, beobachtete Symptome beschreiben.
5. Nie versuchen, das Problem selbst zu lösen, kein Lösegeld bezahlen, keine verdächtigen Nachrichten löschen.

Die Notfallnummern sind bei jedem Arbeitsplatz ausgehängt.

11. Sanktionen bei Nichteinhaltung

Jeder Verstoß gegen diese Richtlinie kann interne disziplinarische Massnahmen bis hin zur Kündigung nach sich ziehen, unter Vorbehalt der persönlichen strafrechtlichen Verantwortung nach dem DSG (Art. 60 bis 63, Bussen bis CHF 250'000) und dem Strafgesetzbuch (Art. 321, Verletzung des Berufsgeheimnisses).

12. Aktualisierung der Richtlinie

Diese Richtlinie wird mindestens einmal pro Jahr überprüft und aktualisiert, ausserdem bei jeder wesentlichen Änderung der IT-Infrastruktur, der eingesetzten Werkzeuge oder des rechtlichen Rahmens. Jede Aktualisierung wird dem gesamten Personal erneut bekanntgegeben und neu unterzeichnet.

Bestätigung der Kenntnisnahme

Mit meiner Unterschrift bestätige ich, dass ich diese Richtlinie der Praxis zu IT-Sicherheit und Datenschutz gelesen, verstanden und akzeptiert habe. Ich verpflichte mich, alle obigen Regeln im Rahmen meiner Tätigkeit einzuhalten.

Name und Vorname: _____

Funktion: _____

Datum: _____

Unterschrift der Mitarbeiterin / des Mitarbeiters:

Unterschrift der Praxisleitung: _____

Rechtliche Hinweise und Nutzungsbedingungen

Dieses Dokument wurde von **DentalSystems Sàrl** zu Informations- und Sensibilisierungszwecken verfasst. Es stellt keine Rechtsberatung dar. Die Angaben in diesem Dokument entsprechen dem Stand von März 2026 und können sich mit Änderungen von Gesetzen und Verordnungen ändern. Diese deutsche Fassung ist eine Übersetzung; massgebend ist die französische Fassung.

Bei rechtlichen Fragen zum DSG, zur DSGVO oder zum Datenschutz im medizinischen Umfeld wenden Sie sich an eine spezialisierte Juristin oder einen spezialisierten Juristen.

Geistiges Eigentum

Dieses Dokument ist ausschliessliches Eigentum der DentalSystems Sàrl. Sein gesamter Inhalt (Texte, Aufbau, Gestaltung und grafische Elemente) ist urheberrechtlich geschützt gemäss dem Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (URG, SR 231.1).

Erlaubte Nutzung

Diese Vorlage wird kostenlos zur Verfügung gestellt. Sie darf angepasst und unter dem Namen der Praxis verwendet werden, auch gegenüber deren Patientinnen und Patienten, Mitarbeitenden und Dienstleistern, ohne unsere Hinweise beizubehalten.

Verbotene Nutzung

Ohne vorgängige schriftliche Zustimmung der DentalSystems Sàrl ist Folgendes verboten:

- Der Verkauf dieses Dokuments, auch in geänderter Form.
- Das Anbieten zum Herunterladen für Dritte (Download-Websites, Austauschplattformen, Wiederverkäufer).

Es gelten die auf www.dentalsystems.ch veröffentlichten Nutzungsbedingungen; bei Abweichungen gehen sie diesem Hinweis vor.

Haftungsbeschränkung

Dieses Dokument wird kostenlos und zu Informationszwecken zur Verfügung gestellt. Soweit nach schweizerischem Recht zulässig, haftet die DentalSystems Sàrl nicht für die Folgen seiner Verwendung; diese Beschränkung gilt nicht bei Vorsatz oder grober Fahrlässigkeit. Die Nutzerin oder der Nutzer bleibt dafür verantwortlich, es an die eigene Situation anzupassen. Es ersetzt weder ein professionelles Audit noch eine Rechtsberatung.

DentalSystems Sàrl

Thomas Alvino, IT-Techniker

www.dentalsystems.ch | talvino@dentalsystems.ch | +41 77 245 48 44

© 2026 DentalSystems Sàrl. Alle Rechte vorbehalten.