

# INTERNAL POLICY

## IT security and data protection

[Name of the dental practice]  
[Full address]

*Version 1.0 | [Date]*  
*Compliant with the FADP (SR 235.1)*

## 1. Purpose and scope

This policy sets out the IT security and data protection rules that apply to all practice staff. It is part of the obligations laid down by the Federal Act on Data Protection (FADP, SR 235.1), in particular Art. 8 on data security.

It applies to everyone who has access to the practice's IT systems or data: practitioners, dental assistants, administrative staff, trainees, locums and any external provider working on the practice's premises or systems.

## 2. Responsibilities

**The head of the practice** is the controller within the meaning of the FADP. They are personally responsible for implementing, communicating and enforcing this policy.

**Every member of staff** must comply with the rules below. Any breach may lead to internal disciplinary measures, without prejudice to the criminal penalties provided for by the FADP (Art. 60 to 63) and the Swiss Criminal Code (Art. 321).

## 3. Access to IT systems

- Each member of staff has a personal, named account. Shared accounts ("practice", "admin", "reception") are prohibited.
- Login credentials are strictly personal and must never be disclosed, not even to a colleague or a superior.
- Passwords must have at least 12 characters, combining upper-case and lower-case letters, numbers and symbols. They must be stored exclusively in the password manager provided by the practice.
- Two-factor authentication (2FA) must be enabled on all critical access: work e-mail, practice management software, cloud backups, remote access.
- The accounts of staff leaving the practice are deactivated immediately, on the day they leave.

## 4. Use of workstations

- Workstations are intended for professional use only.
- The screen must be locked every time you leave your workstation, even for a few moments  
**Windows:** *Windows+L*  
**Apple macOS:** *Ctrl+Command+Q*
- Installing unauthorised software is prohibited. Only the IT provider is authorised to install or update software.
- Operating system and application updates must be applied as soon as they are available. Computers must be restarted at least once a week so that security updates can be installed.

## 5. E-mail and communications

- Any communication containing identifiable patient data (X-rays, diagnoses, AHV numbers, reports) must go through the practice's encrypted e-mail (HIN Mail, ProtonMail or a compliant equivalent).
- Sending patient data through consumer messaging services (Gmail, Hotmail, Bluewin, WhatsApp, text messages, social networks) is strictly prohibited.
- Attachments and links in unexpected e-mails must never be opened. If in doubt, contact the head of the practice or the IT provider before taking any action.

## 6. Patient data and confidentiality

- Patient data must never be copied to personal media: USB sticks, hard drives, phones, tablets or personal cloud services.
- Paper documents containing patient data must be destroyed with a shredder. They must never be thrown in the bin.
- No patient file, printed X-ray or administrative document containing personal data may be left visible on a counter, a desk or near areas accessible to patients.
- All staff are bound by professional secrecy (Art. 321 of the Swiss Criminal Code). This obligation applies during and after the employment contract.

## 7. Personal devices (BYOD)

[Choose the option that applies to the practice:]

**Option A:** Using personal devices (phones, tablets, laptops, USB sticks) to access the practice's data or systems is strictly prohibited.

**Option B:** Using personal devices is permitted under the following conditions: [specify the conditions, for example: only for viewing the appointment book, with encryption enabled, a lock code, and no local storage of patient data].

## 8. Physical security

- Rooms containing servers, backups or network equipment must be locked and accessible only to authorised staff.
- Visitors, suppliers and external technicians must not be left alone in areas where screens display patient data or where sensitive documents are accessible.
- Screens visible from the waiting room or from passageways must be positioned so as not to expose patient data, or fitted with privacy filters.

## 9. WiFi network

- The practice's main network (workstations, server, printers) is separate from the guest network intended for patients.
- The password for the main network must never be given to patients or displayed in areas open to the public.
- Connecting personal devices to the main network is prohibited unless explicitly authorised by the head of the practice.

## 10. Incident procedure

If you suspect a cyberattack, a loss of data or any unusual event:

1. Isolate the computer concerned: unplug the network cable, turn off the WiFi. Do not switch the computer off.
2. Inform the head of the practice immediately.
3. Contact the practice's IT provider.
4. Document the incident: photograph the screens, note the exact time, describe the symptoms observed.
5. Never try to solve the problem yourself, do not pay a ransom, do not delete suspicious messages.

The emergency numbers are displayed near each workstation.

## 11. Penalties for non-compliance

Any breach of this policy may lead to internal disciplinary measures up to and including dismissal, without prejudice to the personal criminal liability provided for by the FADP (Art. 60 to 63, fines of up to CHF 250,000) and the Swiss Criminal Code (Art. 321, breach of professional secrecy).

## 12. Updating the policy

This policy is reviewed and updated at least once a year, or whenever there is a significant change in the IT infrastructure, the tools used or the legal framework. Each update is communicated again to all staff and signed again.

---

### Acknowledgement

I, the undersigned, confirm that I have read, understood and accepted this IT security and data protection policy of the practice. I undertake to comply with all the rules above in the course of my duties.

**Surname and first name:** \_\_\_\_\_

**Role:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Staff member's signature:** \_\_\_\_\_

**Signature of the head of the practice:** \_\_\_\_\_

## Legal notice and terms of use

This document was written by **DentalSystems Sàrl** for information and awareness purposes. It does not constitute legal advice. The information in this document is up to date as of March 2026 and may change as legislation and regulations evolve. This English version is a translation; the French version prevails.

For any legal question relating to the FADP, the GDPR or data protection in the medical context, consult a lawyer specialising in the field.

## Intellectual property

This document is the exclusive property of DentalSystems Sàrl. All of its content (texts, structure, layout and graphic elements) is protected by copyright in accordance with the Federal Act on Copyright and Related Rights (CopA, SR 231.1).

## Permitted use

This template is made available free of charge. It may be modified and used under the practice's name, including with its patients, staff and providers, without keeping our references.

## Prohibited use

Unless DentalSystems Sàrl has given its prior written consent, the following are prohibited:

- Selling this document, even in modified form.
- Offering it for download to third parties (download sites, sharing platforms, resellers).

**The terms of use published on [www.dentalsystems.ch](http://www.dentalsystems.ch) apply; in the event of a discrepancy, they prevail over this notice.**

## Limitation of liability

This document is provided free of charge, for information. To the extent permitted by Swiss law, DentalSystems Sàrl is not liable for the consequences of its use; this limitation does not apply in the event of intent or gross negligence. Users remain responsible for adapting it to their situation. It replaces neither a professional audit nor legal advice.

## DentalSystems Sàrl

Thomas Alvino, IT Technician

[www.dentalsystems.ch](http://www.dentalsystems.ch) | [talvino@dentalsystems.ch](mailto:talvino@dentalsystems.ch) | +41 77 245 48 44

© 2026 DentalSystems Sàrl. All rights reserved.