Concevoir son environnement numérique de travail

> **Référentiel BTS — BC3 / C3.5** « Concevoir et maintenir sécurisé son environnement numérique de travail ».

> **L'essentiel :** un environnement de travail sûr se construit sur trois principes — **chacun n'a accès qu'à ce dont il a besoin**, **chaque équipement est connu et tenu à jour**, **rien de professionnel ne transite par du matériel ou des services personnels**.

Objectif

À la fin de cette page, vous savez :

- appliquer le principe du **moindre privilège** aux comptes d'un cabinet ;
- lister les équipements à inventorier et à maintenir ;
- dire pourquoi le matériel personnel et le cloud grand public posent problème.

1. Des comptes nominatifs, pas de compte partagé

Le compte partagé est l'erreur fondatrice. Un identifiant `cabinet` / `cabinet` utilisé par tout le monde, c'est :

- l'impossibilité de savoir **qui** a consulté ou modifié un dossier — la traçabilité exigée par la réglementation disparaît ;
- un mot de passe que personne ne change jamais, et que les anciens salariés connaissent encore ;
- une responsabilité impossible à établir en cas d'incident.

La règle : un compte **par personne**, avec un **profil de droits** adapté à son rôle.

Rôle	Ce qu'il lui faut	Ce qu'il ne lui faut pas
Orthoprothésiste	Dossiers patients, consultations, appareils, devis	Paramétrage comptable, gestion des utilisateurs
Technicien d'atelier	Dossiers de fabrication, planning, stock	Données de facturation et de droits sociaux
Secrétariat / administratif	Identité, droits, rendez-vous, facturation	Contenu clinique détaillé au-delà du nécessaire
Gérant	Tableaux de bord, comptabilité, utilisateurs	Un accès « tout » permanent : privilégier un compte courant + un compte d'administration séparé
Apprenti / stagiaire	Accès **restreint et temporaire**, sous tutorat	Droits de suppression, exports de masse

Le départ d'un salarié est un événement de sécurité : désactivation du compte le jour même, restitution des cartes et du matériel, changement des accès qu'il partageait.

2. Un parc connu et tenu à jour

On ne sécurise pas ce qu'on ne connaît pas. Tenez un **inventaire simple** : chaque poste, tablette, téléphone professionnel, imprimante, scanner 3D, machine d'atelier connectée, avec son responsable et sa version de logiciel.

Les gestes de maintenance :

- **Mises à jour automatiques** activées, système et applications — la majorité des attaques exploitent des failles **déjà corrigées**.
- **Antivirus / protection** actif et à jour sur chaque poste.
- **Verrouillage automatique** de session après quelques minutes d'inactivité, et verrouillage manuel dès qu'on quitte le poste (un poste ouvert à l'accueil est lisible par tous les patients qui passent).
- **Chiffrement du disque** sur les portables et les tablettes — un ordinateur volé dans une voiture ne doit pas livrer les dossiers.
- **Fin de vie** : un poste réformé ou revendu doit être **effacé de façon sûre**, pas simplement « vidé de la corbeille ».

3. Le réseau

- **Changer les mots de passe par défaut** de la box et des équipements réseau.
- **Séparer le Wi-Fi visiteurs** du réseau du cabinet. Les patients en salle d'attente n'ont rien à faire sur le réseau qui porte les dossiers.
- **Pas d'accès à distance ouvert « pour dépanner »** sans contrôle : un accès de télémaintenance doit être nominatif, limité dans le temps et tracé.
- Les **machines d'atelier connectées** (imprimante 3D, fraiseuse, scanner) sont souvent anciennes et non mises à jour : les isoler sur un segment réseau à part.

4. Matériel personnel et services grand public

C'est le point le plus sensible en petite structure, parce qu'il part toujours d'une bonne intention : « je finis le dossier chez moi », « je m'envoie la photo sur mon téléphone ».

Ce qui ne doit pas se faire :

- envoyer des données patient sur une **boîte mail personnelle** ;
- stocker des photos cliniques ou des scans 3D sur un **cloud grand public** non conforme à l'hébergement de données de santé ;
- utiliser une **messagerie instantanée grand public** pour transmettre un nom de patient avec une information de santé ;
- travailler sur un **ordinateur familial** partagé, sans compte séparé ;
- brancher une **clé USB personnelle** sur un poste du cabinet.

Ce qu'il faut à la place : un poste ou une session professionnelle, la **MSSanté** pour les échanges, un hébergement **certifié HDS** pour les données de santé (voir *Formation métier — Données de santé & réglementation*), et un accès distant maîtrisé si le télétravail est nécessaire.

> Le smartphone professionnel utilisé en visite à domicile mérite le même soin qu'un poste fixe : code de déverrouillage, chiffrement, effacement à distance en cas de perte, pas d'installation d'applications hors usage professionnel.

5. Les prestataires

Le cabinet travaille avec un éditeur de logiciel, parfois un infogérant, un hébergeur. Cela **ne transfère pas la responsabilité** : le cabinet reste responsable de traitement.

À exiger d'un prestataire : un **contrat écrit** précisant la sécurité et la sous-traitance au sens du RGPD, la **localisation** et la **certification HDS** de l'hébergement, les **modalités de sauvegarde et de restauration**, et la **réversibilité** (récupérer ses données si l'on change de prestataire).

À retenir

- **Un compte par personne**, des droits adaptés au rôle, désactivation au départ.
- **Mises à jour, verrouillage, chiffrement** : trois gestes qui couvrent la majorité des risques courants.
- **Wi-Fi visiteurs séparé**, machines d'atelier isolées.
- **Aucune donnée de santé** sur matériel personnel, mail personnel ou cloud grand public.
- Un prestataire est **sous-traitant**, pas responsable à votre place : contrat, HDS, réversibilité.

Revision #4
Created 2026-09-15 17:24:21 UTC by Antoine
Updated 2026-09-16 07:03:12 UTC by Antoine