Politique de Sécurité de l'Information (PSI)

Version 1.0 — En vigueur au 5 juin 2026

Cette politique définit les principes directeurs de la sécurité de l'information chez Maestor. Elle s'appuie sur le cadre **ISO/IEC 27001:2022** (93 contrôles suivis, voir https://trust.maestor.eu/conformite).

1. Objet et périmètre

Protéger la **confidentialité, l'intégrité et la disponibilité** des informations traitées par Maestor — données des clients cuisinistes, de leurs clients finaux, et données internes. Le périmètre couvre l'application Maestor, son infrastructure dédiée et les processus associés.

2. Principes directeurs

- **Defense in depth** : sécurité à chaque couche (réseau, système, application, données).
- **Least privilege** : chaque accès est restreint au strict nécessaire.
- **Secure by default** : configuration sûre par défaut, refus par défaut.
- **Souveraineté** : données et supervision en Suisse / UE, minimisation des transferts hors UE.
- **Honnêteté** : Maestor ne publie que des mesures réellement en place.

3. Gouvernance

- La direction porte la responsabilité de la sécurité de l'information.
- Revue de code et **revue de sécurité** obligatoires avant tout déploiement sensible (authentification, contrôle d'accès, facturation).
- Suivi des 93 contrôles ISO 27001 et de l'analyse de risques (10 risques majeurs identifiés et traités).

4. Domaines de contrôle

Domaine	Mesures clés
Contrôle d'accès	RBAC granulaire, double authentification, accès admin par clé.
Cryptographie	Chiffrement en transit (TLS 1.3) et au repos (BDD + volume).
Sécurité physique	Datacenter Infomaniak certifié ISO 27001 (Genève).
Exploitation	Durcissement système, fail2ban, mises à jour automatiques, journalisation.
Continuité	Sauvegardes chiffrées off-site, RPO 24 h / RTO 4 h, restauration testée.
Sous-traitance	Sélection, DPA, registre tenu à jour, privilège aux acteurs UE/CH.
Incidents	Détection, qualification, notification 72 h, post-mortems publics.
RH	NDA, sensibilisation, arrivée/départ.

5. Conformité

- **RGPD** : minimisation, durées de conservation, purge automatisée, droits des personnes, DPA article 28.
- **eIDAS** : signature électronique qualifiée pour les documents engageants.
- **ISO 27001:2022** : démarche d'alignement documentée et suivie publiquement.

6. Révision

La présente politique est revue au moins **annuellement** et à chaque évolution majeure de l'architecture ou de la réglementation.

Détail des mesures : https://trust.maestor.eu/securite — Contrôles ISO : https://trust.maestor.eu/conformite

---