

Politique de Sauvegarde & de Continuité d'Activité (PCA/PRA)

Version 1.0 — En vigueur au 5 juin 2026

Ce document décrit le dispositif **réel** de sauvegarde et de reprise d'activité de Maestor.

1. Objectifs de continuité

Indicateur	Cible	Signification
RPO (Recovery Point Objective)	24 h	Perte de données maximale tolérée en cas de sinistre.
RTO (Recovery Time Objective)	4 h	Délai maximal de remise en service visé.

Objectifs alignés sur l'architecture actuelle (serveur dédié unique). Ils évolueront avec la redondance multi-nœuds prévue (cible).

2. Dispositif de sauvegarde

- **Fréquence** : sauvegardes **quotidiennes** automatisées.
- **Chiffrement** : chiffrement **de bout en bout** (les sauvegardes sont illisibles sans la clé, conservée séparément).
- **Externalisation** : stockage **hors-serveur** chez un dépositaire **suisse** (souveraineté des données conservée).
- **Périmètre** : base de données applicative, fichiers utilisateurs (uploads, exports), configuration.
- **Rétention** : conservation glissante des points de restauration.
- **Intégrité** : sauvegardes vérifiées ; déduplication et chiffrement gérés par l'outil de sauvegarde.

3. Restauration

- **Restauration testée** : la procédure de restauration a été exécutée et validée (pas seulement déclarée).
- La clé de chiffrement des sauvegardes et la clé de chiffrement au repos sont **conservées de manière sécurisée et séparée** — leur perte rendrait les données irrécupérables, elles font l'objet d'une protection spécifique.

4. Scénarios couverts

- **Corruption / suppression de données** : restauration au dernier point sain.
- **Perte du serveur** : reconstruction sur une nouvelle instance Infomaniak (provisionnement en quelques minutes) puis restauration des sauvegardes off-site.
- **Sinistre datacenter** : les sauvegardes étant externalisées hors du serveur, elles restent disponibles.

5. Maintenance et tests

- Les fenêtres de **maintenance planifiée** sont annoncées à l'avance et n'entrent pas dans le calcul de l'indisponibilité.
- Tests de restauration périodiques (cible : test formalisé documenté à intervalle régulier).

6. Articulation avec la disponibilité

Le dispositif de sauvegarde complète la supervision de disponibilité (objectif **99 %/mois**) décrite sur <https://trust.maestor.eu/disponibilite>.

Document de conformité Maestor. Contact : security@maestor.eu
