

Politique de Gestion des Incidents

Version 1.0 — En vigueur au 5 juin 2026

Cette politique décrit la manière dont Maestor détecte, qualifie, traite et communique les incidents de sécurité et de disponibilité.

1. Détection

- **Supervision continue** : uptime externe (sondes 60 s), métriques infrastructure temps réel, remontée des erreurs applicatives (auto-hébergée).
- **Alerting automatique** en cas d'indisponibilité ou d'anomalie.
- Signalement possible par les clients (security@maestor.eu) et via la politique de divulgation responsable (<https://trust.maestor.eu/divulgation>).

2. Qualification par sévérité

Sévérité	Définition
Mineur	Impact limité, pas de perte de données, contournement possible.
Modéré	Dégradation de service partielle ou temporaire.
Majeur	Indisponibilité significative ou risque sur les données.
Critique	Violation de données personnelles avérée ou indisponibilité totale.

3. Traitement

1. **Endiguement** : limiter l'impact (isolation, bascule, blocage).
2. **Investigation** : identifier la cause racine.
3. **Remédiation** : corriger et rétablir le service.
4. **Suivi** : surveillance renforcée post-incident.

4. Communication client

- **Notification sous 72 h** pour tout incident impliquant des **données personnelles** (RGPD, article 33/34), avec les informations utiles à l'évaluation du risque.
- Notification des incidents **majeurs / critiques** de disponibilité aux clients concernés.
- **Post-mortem public** publié pour chaque incident **majeur ou critique** : <https://trust.maestor.eu/incidents>.

5. Coordination avec les autorités

- Notification à l'autorité de contrôle compétente (CNIL) sous 72 h lorsque la réglementation l'exige.
- Coordination avec les CERT/autorités (ex. ANSSI) si applicable.

6. Amélioration continue

Chaque incident majeur donne lieu à des **leçons apprises** et, le cas échéant, à une mise à jour des mesures techniques et organisationnelles.

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

Maestor — Document de conformité. La version officielle signée prévaut. Contact : security@maestor.eu / dpo@maestor.eu