MoveWORK
BUSINESS INTELLIGENCE SOLUTIONS

Dossier Gouvernance & Continuité
MoveWORK Flow – Ultra Propreté

Document généré pour usage client – 31/05/2025

Politique générale de sauvegarde et restauration **3**
Objectif 3
Sauvegarde 3
Restauration 3
Politique de gestion des changements **4**
Objectif 4
Cycle de gestion des changements 4
Sécurité et traçabilité 4
Continuité et restauration 4
Amélioration continue 5
Politique de gestion des incidents **5**
Objectif 5
Classification et Détection 5
Escalade et Communication 5
Amélioration Continue 5

Politique générale de sauvegarde et restauration

Objectif

Ce document présente la politique générale de sauvegarde et de restauration mise en œuvre pour assurer la continuité de service et la protection des données client.

Sauvegarde

- Des sauvegardes complètes et incrémentales sont effectuées quotidiennement.
- Les données sont hébergées dans des data centers AWS certifiés (ISO 27001, HDS-ready) situés en Europe (France et Irlande).
- Les bases de données sont répliquées de façon géo-redondante.

Restauration

- En cas d'incident majeur, une procédure de restauration validée est déclenchée.
- Les temps de reprise sont définis pour garantir un RTO et RPO conformes aux bonnes pratiques du secteur santé.
- La restauration est testée régulièrement afin de garantir son efficacité.

Politique de gestion des changements

Objectif

Ce document résume la politique générale de gestion des changements appliquée à la plateforme MoveWORK Flow, afin de garantir la continuité de service et la qualité des évolutions déployées.

Cycle de gestion des changements

- L'organisation suit un mode de développement Agile basé sur des sprints de 15 jours.
- Les évolutions mineures et correctifs sont déployés chaque mardi après validation complète.
- Chaque changement suit un cycle Dev → QA → Fix → Prod pour garantir une qualité maximale avant mise en production.
- L'environnement QA reproduit fidèlement la production pour effectuer des tests quasi-conformes.

Sécurité et traçabilité

- L'intégralité du code source est versionnée sous Git avec contrôle des commits et synchronisation entre environnements.
- Chaque changement est traçable et documenté.
- Des tests automatisés et manuels sont exécutés avant tout déploiement pour limiter les risques de régression.
- Une surveillance proactive et des journaux applicatifs permettent de détecter et d'analyser tout incident post-déploiement.

Continuité et restauration

- La base de données est sauvegardée sur un cycle glissant de 10 jours sur AWS, permettant la restauration à tout moment.
- Les sources applicatives et la structure d'infrastructure sont également versionnées, autorisant un retour à un état antérieur.
- Les requêtes critiques (comme les pointages) sont journalisées et conservées pendant un mois, et peuvent être rejouées si nécessaire.
- L'infrastructure repose sur des ressources auto-scalées : toute défaillance déclenche la création automatique d'une ressource de remplacement.
- Ce mécanisme assure une haute disponibilité et une reprise rapide en cas d'incident.

Amélioration continue

Chaque cycle de déploiement est suivi d'une analyse continue des performances et incidents. Les retours d'expérience alimentent la roadmap technique et renforcent la fiabilité des prochaines mises en production.

Politique de gestion des incidents

Objectif

Ce document présente la politique générale de gestion des incidents pour la plateforme MoveWORK Flow.

Classification et Détection

- Les incidents sont classés selon leur impact (mineur, majeur, critique).
- Une surveillance proactive et des alertes automatisées permettent une détection rapide.
- Les incidents critiques sont traités en priorité avec une mobilisation 24/7.

Escalade et Communication

- Les incidents majeurs font l'objet d'une notification client sous 4h.
- Des points de situation réguliers sont communiqués jusqu'à la résolution.
- Un rapport d'incident synthétique est fourni à la clôture.

Amélioration Continue

- Chaque incident fait l'objet d'une analyse post-mortem.
- Les plans d'action préventifs sont intégrés à la roadmap sécurité.
- Les incidents récurrents donnent lieu à des mesures correctives durables.