MoveWORK
BUSINESS INTELLIGENCE SOLUTIONS

Governance and continuity MoveWORK Flow: Ultra Cleaning

Document generated for customer use – 31/05/2025

General Backup and Restauration Policy

Objective

This document presents the general backup and restoration policy implemented to ensure service continuity and the protection of client data.

Backup

- Full and incremental backups are performed daily.
- Data is hosted in AWS-certified data centers (ISO 27001, HDS-ready) located in Europe (France and Ireland).
- Databases are replicated in a geo-redundant manner.

Restauration

- In the event of a major incident, a validated restoration procedure is initiated.
- Recovery times are defined to ensure RTO and RPO are aligned with healthcare industry best practices.
- Restoration is regularly tested to ensure its effectiveness.

Change Management Policy

Objective

This document summarizes the general change management policy applied to the MoveWORK Flow platform to ensure service continuity and the quality of deployed updates.

Change Management Cycle

- The organization follows an Agile development model based on 15-day sprints.
- Minor updates and bug fixes are deployed every Tuesday after full validation.
- Each change follows a Dev → QA → Fix → Prod cycle to ensure maximum quality before production release.
- The QA environment accurately replicates production to perform near-identical testing.

Security and Traceability

- All source code is version-controlled in Git with commit tracking and synchronization between environments.
- Each change is traceable and documented.
- Automated and manual tests are performed before each deployment to minimize regression risks.
- Proactive monitoring and application logs enable detection and analysis of any post-deployment incidents.

Continuity and Restoration

- The database is backed up on a rolling 10-day cycle on AWS, allowing restoration at any time.
- Application sources and infrastructure configurations are also versioned, allowing rollback to a previous state.
- Critical requests (such as time stamps) are logged and retained for one month, and can be replayed if necessary.
- The infrastructure relies on auto-scaled resources: any failure triggers the automatic creation of a replacement resource.
- This mechanism ensures high availability and rapid recovery in the event of an incident.

Continuous Improvement

Each deployment cycle is followed by continuous analysis of performance and incidents. Feedback contributes to the technical roadmap and strengthens the reliability of future releases.

Incident Management Policy

Objective

This document presents the general incident management policy for the MoveWORK Flow platform.

Classification and Detection

- Incidents are classified according to their impact (minor, major, critical).
- Proactive monitoring and automated alerts enable rapid detection.
- Critical incidents are handled as a priority with 24/7 availability.

Escalation and Communication

- Major incidents are subject to customer notification within 4 hours.
- Regular status updates are communicated until resolution.
- A summary incident report is provided upon closure.

Continuous Improvement

- Each incident is subject to a post-mortem analysis.
- Preventive action plans are integrated into the security roadmap.
- Recurring incidents result in long-term corrective measures.