INFORMATION SECURITY

JADEV-GROUP: Security Approach and Commitments

Date : March 2026

CONFIDENTIEL

Introduction

This document describes how JADEV GROUP SRL manages information security when delivering software development and IT services to its clients.

JADEV GROUP SRL, incorporated in Belgium, is the contractual and GDPR-responsible entity for all client engagements. Operational delivery is performed by JADEV-CORP SARL (Casablanca, Maroc), our nearshore subsidiary, under the full contractual responsibility of JADEV GROUP SRL. Delivery by JADEV-CORP SARL is governed by intra-group Standard Contractual Clauses and the operating model described in this document.

This document is intended for client security officers, CTOs, and data protection officers evaluating JADEV as a partner.

1. Operating model

We work within your environment. Our teams connect to your tools, your repositories, and your infrastructure. We do not impose our own platform or require your data to leave your perimeter.

Principle	What this means in practice
Client-owned environments	Your cloud infrastructure (AWS, Azure, GCP), your source control (Azure DevOps, GitHub, GitLab), your project management tools, your CI/CD pipelines. Source code is cloned locally for development on encrypted workstations and remains under your version control.
Client-owned access control	You provision accounts for our team members in your identity provider. You control who has access to what, and you can revoke at any time.
Client-owned audit trail	Every commit, every ticket update, every login is logged in your systems. You have full visibility without depending on us for reports.
Data stays with you	Code, test results, documentation, and artifacts remain in your tools. We do not extract or replicate project data to external systems.
Hardware flexibility	Our team members work on JADEV-managed laptops by default, or on client-provided hardware if your policies require it.

Example: For a typical development engagement, our engineer receives a named account on the client's source control, a project management seat, and VPN credentials. All code is committed to the client's repository, all tasks are tracked in the client's project board, and all access is logged in the client's identity provider. When the engagement ends, the account is disabled.

2. Access control

- One named account per team member. No shared or generic accounts.
- Multi-factor authentication (MFA) on all services, enforced by policy.

- Least privilege: each person gets access only to the repositories, environments, and tools required for their specific assignment.
- Access revoked within 24 hours when a team member leaves the engagement.
- Periodic access review with the client to confirm active accounts match the current team roster.

3. Endpoint security

JADEV workstations are centrally managed via the Microsoft ecosystem. Windows devices are managed via Intune. macOS devices are subject to equivalent controls (FileVault encryption, Defender for Endpoint, Intune MDM).

Layer	Solution	What it provides
Identity	Azure Entra ID	Single sign-on, MFA enforcement, conditional access policies, authentication logs
Device management	Microsoft Intune	Compliance policies, forced OS and app updates, remote wipe capability, device health checks
Disk encryption	BitLocker / FileVault	Full disk encryption on all workstations, enforced via Intune policy. Data is unreadable if a device is lost or stolen.
Threat protection	Microsoft Defender for Endpoint	Real-time threat detection, endpoint detection and response (EDR), automatic remediation
Screen lock	Intune policy	Automatic lock after 5 minutes of inactivity
Passwords	Bitwarden (managed)	Minimum 12 characters, password manager required for all accounts
Patching	Intune + Windows Update	OS and application patches applied within 72 hours of release

4. Connections and data transfers

- All connections to client environments go through the client's VPN or a secure tunnel (SSH, TLS).
- Encrypted protocols only: HTTPS, SSH, TLS 1.2+.
- No file transfers to personal cloud services (Dropbox, Google Drive, OneDrive personal, WeTransfer, etc.).
- No use of personal email for client-related communication.

5. Incident management

If a security incident occurs (suspected compromise, unauthorized access, lost or stolen device), we follow a defined escalation process:

Step	Timeline	Action
Detection	Immediate	The team member reports the incident to their direct manager
Internal escalation	Within 1 hour	Jamal Abdelkhalek (Director) is notified and takes ownership
Client notification	Within 24 hours	The client receives a written notification with a description of what happened and what we know so far
Remediation	Ongoing	Corrective actions are implemented and documented
Incident report	Within 72 hours	A written report is delivered to the client: root cause, impact, actions taken, and measures to prevent recurrence

The 24-hour client notification and 72-hour incident report are contractual commitments. They are stricter than what GDPR Article 33(2) requires of a processor ('without undue delay').

6. GDPR and international data transfers

Our structural advantage: JADEV GROUP SRL, incorporated in Belgium, is an EU-established entity subject to the GDPR. It is the contracting party for all client engagements. Clients contract with a European entity under European law.

Role under GDPR: Where engagements involve the processing of personal data on behalf of a client, JADEV acts as a data processor within the meaning of Article 4(8) GDPR, under the client's documented instructions. A Data Processing Agreement (DPA) aligned with Article 28 GDPR is available as a standard annex to every service agreement.

Morocco and data transfers: JADEV-CORP SARL is established in Morocco. Morocco has its own data protection law (Loi 09-08), supervised by the CNDP (Commission Nationale de controle de la Protection des Donnees a Caractere Personnel). However, Morocco does not currently hold an EU adequacy decision. Transfers of personal data from the EU to Morocco therefore require appropriate safeguards under Article 46 GDPR.

Safeguards:

- The intra-group relationship between JADEV GROUP and JADEV-CORP is governed by a Subcontracting Agreement, a Data Processing Agreement (DPA), and Standard Contractual Clauses (SCC 2021, Module 3: Processor to Sub-processor) in accordance with Article 46(2)(c) GDPR.
- A sub-processor register is maintained. No additional sub-processors are engaged without client notification and a minimum 30-day objection period.

In practice: Most software development engagements do not involve processing personal data. Our team members work within client environments and do not extract or store personal data on local systems. The SCC and DPA safeguards apply for the residual risk of incidental access to personal data during development or testing.

Health and life sciences data: For clients in healthcare, diagnostics, or life sciences, written authorization from the DPO or compliance lead is required before accessing health-related systems. Development and testing use staging environments with anonymized data. No health data is stored locally. JADEV aligns with client regulatory frameworks (ISO 13485, IVD-R, FDA 21 CFR Part 11) and audit trails are maintained in the client infrastructure.

Financial and payment data: For engagements involving payment service providers or financial institutions (PSD2, PCI DSS, DORA scope), JADEV operates within the client's secure environment and does not store or process cardholder data, KYC documents, or transaction records on its own systems. Access to sensitive financial data requires explicit authorization from the client's compliance officer. Development and testing use anonymized or tokenized data.

Data subject rights: JADEV supports the client in responding to data subject requests (access, deletion, rectification, portability) by providing relevant information within 5 business days of the client's request.

7. Data-intensive engagements

Some engagements require working with real or sensitive data: data science, analytics, machine learning, or data engineering. For these engagements, ensuring that data is processed within the client's managed environment, not on local workstations, is a hard requirement.

Core principle: We analyze your data where it lives, not where we live.

How we handle this:

- We work within client-managed cloud platforms. The data stays in the platform, not on our machines.
- Platforms we currently operate on include Microsoft Fabric, Azure Data Explorer, and Databricks. All three provide browser-based access, role-based permissions, and built-in audit trails.
- Our team members connect through the client's identity provider (SSO + MFA), so every query, every notebook execution, and every data access is logged under a named account in your system.
- There is no JADEV data lake, no staging environment, no copy of your data.
- For non-production work, we recommend anonymized or synthetic datasets whenever possible.

What we expect from the client for data engagements:

- A dedicated workspace or environment with appropriate access controls.
- Clear data classification and handling rules communicated before work starts.
- Audit logging enabled on the platform.
- A named contact for data governance questions.

Example: In a data discovery phase, a JADEV data engineer receives a compute role (e.g. Databricks Contributor) within the client's Azure workspace. They access raw or anonymized data via notebooks, produce outputs (reports, models, pipelines) that remain in the client's environment, and the entire session

is logged in Azure Monitor. At engagement end, the role is revoked and no artifact leaves the client's perimeter.

8. Confidentiality and contractual framework

JADEV considers the following documents as prerequisites to any engagement involving sensitive information:

- Bilateral NDA. JADEV provides a standard template; client templates are also accepted. We recommend the client define an NDA adapted to their specific context.
- Data Processing Agreement (Article 28 GDPR). JADEV provides a standard DPA annex. Client-specific DPAs are also accepted.
- For engagements involving health or special category data: explicit written authorization from the client's DPO or equivalent.

Additional commitments:

- A confidentiality clause is included in every service agreement.
- Each JADEV team member signs an individual confidentiality commitment before starting work on a client engagement.
- Confidentiality obligations remain in force for two (2) years after the engagement ends, or longer if required by the client's policies or applicable regulations.

9. What we expect from the client

Security works both ways. For a productive and secure collaboration, we ask the client to provide the following before work begins:

Item	Why it matters
NDA or confidentiality agreement	Defines the legal framework for information exchange. We recommend the client's own template.
Access credentials via your identity provider	Named accounts provisioned by the client ensure traceability and give you full control over access.
Dedicated development/staging environment	Allows our team to work without touching production data.
Relevant security policies	Shared upfront so our team can align from day one, not discover constraints mid-project.
Named security contact	One person on the client side who can answer security questions and handle incident escalation.
Regulatory constraints (if any)	If specific regulations apply (healthcare, finance, government), we need to know before scoping the engagement.
Legal basis for any data	If our team will have access to personal data, the client confirms they hold

access	a valid legal basis and that the scope of our access is consistent with that basis.

10. Security awareness and training

- Every team member receives security training before their first client assignment.
- Annual refresher covering phishing, social engineering, password hygiene, and safe handling of client environments.
- Training records are maintained and available upon request.
- When a client has specific security onboarding (e.g., ISO 27001 awareness, HIPAA basics), our team members complete it before starting work.

11. End of engagement

- All access is revoked on the last business day of the engagement.
- Client-provided hardware is returned within 48 hours.
- Any local data related to the engagement is deleted from JADEV workstations. Written confirmation is provided upon request.
- Client tools and VPN configurations are removed from our devices.

12. Compliance posture

JADEV GROUP SRL is not ISO 27001 certified at this time. We are formalizing our Information Security Management System (ISMS) and working toward certification.

In the meantime, we align with the security requirements of each client and adapt our practices to their compliance framework. We have experience working within ISO 27001-certified environments and can demonstrate compliance with specific controls upon request.

Our endpoint stack (Azure Entra ID, Intune, BitLocker, Defender for Endpoint) addresses the workstation security controls in ISO 27001:2022 Annex A, Section 8. The remaining gap is primarily in formal governance documentation: written policies, risk assessment, Statement of Applicability, and audit records. We are working through these systematically.