Corporate Governance Policy

Policy year 2026-27 · Effective 1 April 2026 to 31 March 2027 · Version 1.0 · Approved by the Management Board

Contents

1. 1. Purpose

This policy describes how InterAtlas Estate is directed and controlled: who is accountable for what, how decisions are made, and how we safeguard the interests of clients, partners and the company.

2. 2. Accountability

- Management holds ultimate responsibility for strategy, risk appetite, financial integrity and compliance.
- Clear delegation: operational decisions are documented with defined approval thresholds; client-money movements always require identity-verified instruction and appropriate review.
- Conflicts of interest are declared as they arise and recorded; no one approves a matter in which they hold a personal interest.

3. 3. Risk management and internal control

- A maintained risk register covering market, counterparty, operational, technology and compliance risk, reviewed at least quarterly.
- Segregation of duties, dual review of significant transactions, and reconciliation of the transaction ledger to underlying accounts.
- Business continuity: encrypted backups of records and documented recovery procedures.

4. 4. Integrity of information

Financial records are kept accurately and completely. Public statements, listings and marketing are reviewed for accuracy before publication, and corrected promptly when an error is found.

5. 5. Related policies

This policy operates alongside our Code of Conduct, Anti-Bribery & Corruption, Anti-Fraud, AML/CTF, Data Protection, Sanctions, Tax and Whistleblowing policies, all published on our Governance page.

6. Approval thresholds

- Up to EUR 10,000: single manager approval, documented.
- EUR 10,000 to 50,000: two-person approval (manager + finance).
- Over EUR 50,000, any client-money movement outside normal flows, or any new market/product: Management Board approval.
- Contracts binding the company beyond 12 months: Management Board approval regardless of value.

7. Meeting and reporting cadence

- Management Board: meets at least quarterly; minutes recorded; standing agenda includes risk register, compliance report, finance report and client-money reconciliation.
- Risk register: reviewed quarterly; each risk has an owner, likelihood/impact score and mitigation with deadline.
- Policies: reviewed annually on a published calendar; versions controlled centrally.

8. Internal control catalogue (extract)

- Client funds: segregated accounts; ledger as single source of truth; daily automated balance derivation; withdrawal release only to verified holders.
- Access: role-based permissions; encrypted PII; access to KYC documents logged.
- Change management: production changes tested and reversible; backups encrypted and restore-tested.

9. Governance and oversight

We operate three lines of defence. The first line is the business itself: every employee and manager owns the risks of their own activity and applies this policy in daily decisions. The second line is the compliance function, which designs the controls, advises the business, monitors adherence and reports independently. The third line is independent review - periodic

internal audit work and, where engaged, external examination - which tests that the first two lines actually work. The Management Board sits above all three: it approves this policy, receives quarterly reporting on incidents, exceptions and control performance, and is escalated to within 24 hours for material events.

10. Risk assessment

Risk in this domain is assessed formally at least annually, and whenever our products, markets or the external environment change materially. Each identified risk is scored for likelihood and impact, assigned an owner and a mitigation with a deadline, and entered in the risk register reviewed quarterly by the Management Board. The factors below weigh most heavily in this policy's domain:

- Rapid product expansion (tokenization, alliances) can outpace control design if not gated.
- Concentration of knowledge in few people creates key-person and override risk.
- Third-party dependencies (payment rails, hosting, developers) import external failures.
- Multi-language public content risks inconsistency between locales.
- Manual admin actions on balances demand dual control and immutable logging.

11. Procedures and controls

The operating procedures below are mandatory. Deviation requires prior written approval from the compliance function, recorded in the exceptions log with rationale and expiry.

- Decision thresholds: to EUR 10,000 single manager; EUR 10,000-50,000 manager plus finance; above EUR 50,000, new markets, new products or 12-month-plus contracts require Board approval.
- Conflicts of interest are declared on appearance, recorded in the register, and the conflicted person is excluded from the decision.
- The risk register assigns each risk an owner, scoring and mitigation deadline; reviewed quarterly by the Board.
- Client money remains in segregated accounts; the ledger is the single source of balance truth and is reconciled to bank statements monthly with documented sign-off.
- Production changes are tested, reversible and logged; encrypted backups are restore-tested twice yearly.
- Public statements, listings and statistics are reviewed for accuracy before publication and corrected within 2 business days of an error being confirmed.
- Minutes record decisions, dissent and follow-up owners; actions are tracked to closure.

12. Application across our markets

Application across our markets: local engagement of counsel, notaries and banking partners follows the same approval thresholds; market-specific delegations are recorded in the delegation register.

13. Applying this policy: worked examples

The examples below illustrate how the requirements of this policy operate in practice. They are illustrative, not exhaustive; where a real situation is not covered, the escalation duty applies.

- Situation: a manager wants to sign an 18-month contract worth EUR 30,000. Response: Board approval required - the duration exceeds 12 months even though the value sits in the middle tier.
- Situation: a website statistic is found to be overstated. Response: corrected within 2 business days and the source-check step that failed is fixed.
- Situation: a new product is proposed without a risk register entry. Response: gated - no launch until risks are scored, owned and mitigated to appetite.
- Situation: an approver leaves and their counterparty approval chain breaks. Response: an interim delegation is recorded in the delegation register before any further approvals proceed.

14. Definitions

- Governance — the system of rules, practices and controls by which the company is directed and held accountable.
- Conflict of interest — a situation where personal interests could improperly influence professional judgement or duties.
- Segregation of duties — dividing responsibility for initiating, approving and recording a transaction among different people.
- Risk appetite — the level and type of risk the company is willing to accept in pursuit of its objectives.

15. Roles and responsibilities

- Management Board — owns this policy, approves it annually, sets the risk appetite and receives escalation of material issues within 24 hours of identification.
- Compliance function — maintains this policy, delivers training, performs monitoring, investigates concerns and reports quarterly to the Board on incidents, exceptions and control performance.
- Line managers — embed the policy in day-to-day operations, ensure their teams have completed training, and act as the first escalation point.
- All employees and associated persons — read and follow this policy, complete required training on joining and annually thereafter, and escalate concerns promptly rather than act on doubt.

16. Training and communication

Everyone in scope receives training on this policy at induction and at least annually, with targeted refreshers whenever the policy or the law changes materially. Completion is recorded. The current version of this policy is available to all staff and is published on the Governance page of atlasestate.estate; material changes are communicated directly.

- Induction: policy walkthrough within the first 10 working days, before unsupervised client contact.
- Annual refresher: scenario-based session covering the red flags and escalation routes in this document.
- Role-specific modules: deeper training for the functions most exposed to this policy's risks.
- Attestation: annual written confirmation of having read and understood the current version.

17. Records and retention

Records evidencing compliance with this policy - approvals, screenings, registers, training logs, investigation files - are kept accurately, stored securely with access restricted to those who need them, and retained for at least six years (or longer where law requires), after which they are securely destroyed.

18. Monitoring, audit and review

Compliance monitors adherence to this policy through periodic sample testing, exception reporting and review of escalations. Findings, together with any breaches and remediation actions, are reported to the Management Board quarterly. This policy is reviewed at least annually, and additionally whenever our operations, the law or regulatory guidance change materially.

- Quarterly: sample testing of controls and registers; exception-log review; Board reporting pack.
- Annually: full policy review against legal developments and incident learnings; training completion audit.
- Ad hoc: thematic reviews triggered by incidents, near misses or external findings.

19. Breaches and consequences

A breach of this policy is a serious matter. Confirmed breaches by employees are handled under our disciplinary process and may result in sanctions up to dismissal; breaches by suppliers, introducers or other associated persons may result in contract termination. Where conduct may amount to a criminal offence, we will cooperate fully with the competent authorities. Honest mistakes that are self-reported promptly are treated as learning opportunities, not misconduct - concealment, not error, is the aggravating factor.

20. Regulatory context and related documents

We design our controls by reference to internationally recognised frameworks and the local law of each market in which we operate. The frameworks most relevant to this policy include:

- General principles of recognised corporate-governance codes, applied proportionately to our scale
- Company law of our jurisdictions of establishment
- Contractual obligations to payment and banking partners

This policy forms part of the InterAtlas Estate governance framework and should be read together with the other policies published at atlasestate.estate/en/governance, including the Code of Conduct, the Whistleblowing Policy and the Data Protection Policy.

21. Version control

- Version 1.0 - 1 April 2026 - Initial adoption for policy year 2026-27 - Approved by the Management Board.
- Next scheduled review: March 2027 (or earlier upon material change in law or operations).
- Policy owner: Compliance function, compliance@atlasestate.estate.

Annex A - Contacts and escalation routes

- Compliance function: compliance@atlasestate.estate - policy questions, approvals, escalations and suspicion reports; acknowledgement within 1 business day.
- Whistleblowing routes: any route in the Whistleblowing Policy, including anonymous reporting; acknowledgement within 3 business days.
- Urgent matters (suspected live fraud, sanctions hit, data breach): escalate immediately by the fastest available channel, then confirm in writing the same day.
- External: nothing in this policy prevents any person from reporting directly to a competent authority at any time.