Anti-Fraud 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 protects our investors, partners and the company itself from fraud - deliberate deception intended to secure an unfair or unlawful gain. We operate a zero-tolerance approach.

2. 2. Scope

This policy applies to InterAtlas Estate, its management, employees, contractors and anyone acting on its behalf, in every market where we operate. Third parties who act for us (agents, introducers, service providers) are expected to observe equivalent standards.

3. 3. What we consider fraud

- Misrepresenting a property, projection, price or availability to induce an investment.
- Falsifying documents, accounts, invoices or expense claims.
- Identity fraud, account takeover, or use of stolen payment credentials.
- Unauthorised use of client funds or company assets.

- Concealing or misstating material facts owed to a client or counterparty.

4. 4. Prevention and detection

- Segregation of duties between those who initiate, approve and record transactions.
- Identity verification (KYC) on every investor and manual review of deposits and withdrawals.
- An immutable transaction ledger and encrypted records supporting a full audit trail.
- Sample and illustrative content on our platform is clearly labelled; projected returns are always indicative, never guaranteed.

5. 5. Response

Suspected fraud is investigated promptly and discreetly by a person independent of the matter. We preserve evidence, recover losses where possible, and report criminal conduct to law enforcement.

6. 6. Reporting

Concerns can be raised with management or confidentially via compliance@atlasestate.estate, or anonymously under our Whistleblowing Policy. No one who raises a genuine concern in good faith will suffer retaliation of any kind.

7. Real-estate fraud typologies we defend against

- Deposit redirection: criminals intercept email threads and substitute their own bank details. Control: payment details are published only in the secure portal, never changed by email, and confirmed by a second channel on request.
- Fake or cloned listings: our listings carry verified photography with published licensing, and sample or illustrative content is always labelled.
- Identity fraud and account takeover: KYC with live face capture, 2FA, and withdrawal release only to the verified holder.
- Invoice and supplier fraud: dual approval of payables, verification of new supplier bank details by call-back, and segregation of duties.
- Internal misuse of client funds: client money segregation, immutable ledger, and reconciliation checks.

8. Fraud response plan

- Hour 0-24: contain (freeze affected accounts/permissions), preserve evidence (logs, documents, devices), appoint an investigator independent of the matter.
- Day 1-5: establish facts and quantify exposure; notify insurers and, where criminal, law enforcement; inform affected clients honestly.
- Day 5-15: complete investigation, remediate control gaps, document lessons; report to the Management Board.
- Recovery: pursue restitution through civil and criminal routes where proportionate.

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:

- High transaction values make single successful frauds severe.
- Email-based conveyancing culture invites payment-diversion attacks.
- Remote onboarding is targeted by synthetic and stolen identities.
- Investor unfamiliarity with off-plan mechanics can be exploited by impostors posing as us.
- Internal access to the ledger and client data requires strict least-privilege control.

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.

- Client payment details are published only inside the authenticated portal; we never change bank details by email, and any such request triggers call-back verification on a known number.
- New supplier bank details, and changes to existing ones, are verified by call-back and held for 48 hours before first payment.
- Dual approval for payables above EUR 10,000 and for any manual balance adjustment; approver cannot be initiator.
- Least-privilege access to the admin panel and ledger; access rights reviewed quarterly; departures deprovisioned same day.
- Listings are published only from verified data and licensed imagery; illustrative content is labelled.
- Customer-facing anti-impersonation notice: we list our only official domains and never solicit payments via messaging apps.
- Fraud attempts, successful or not, are logged in the incident register with vector, exposure and remediation.
- Hour 0-24 response: freeze affected access, preserve logs and documents, appoint an independent investigator; days 1-5: quantify, notify insurers/law enforcement/affected clients; days 5-15: findings, remediation, Board report.

12. Application across our markets

Application across our markets: conveyancing conventions differ (notarial systems in Spain, Greece and Portugal; registration practices in the UAE and Turkey), so the payment-details rule

is absolute and market-independent: details live only in the portal and never change by email.

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: an urgent email appearing to be from a director requests a transfer to a new beneficiary. Response: call-back verification on a known number; identified as business-email-compromise; logged and staff alerted.
- Situation: a client reports that our agent on a messaging app requested payment to a new IBAN. Response: impersonation protocol - client warned through official channels, account reported to the platform, incident logged.
- Situation: a supplier emails new bank details before an invoice run. Response: call-back verification and a 48-hour hold before any payment to the new details.
- Situation: a staff member requests a manual balance credit to fix a display bug. Response: no manual adjustment without dual approval and investigation of the underlying ledger record first.

14. Definitions

- Fraud — dishonestly making a false representation, failing to disclose information, or abusing a position, to make a gain or cause a loss.
- Misrepresentation — an untrue or misleading statement of fact that induces another party to act.
- Internal fraud — fraud committed by employees or management against the company or its clients.
- External fraud — fraud committed against the company or its clients by third parties, including identity theft and account takeover.

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:

- Local criminal fraud law of each operating market
- Payment-scheme rules applicable to card acquiring
- Consumer-protection and unfair-practice rules in our EU markets

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.