Anti-Money-Laundering & Counter-Terrorist-Financing 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

Real estate is a recognised target for money laundering. This policy sets out how InterAtlas Estate prevents its platform and services from being used to launder the proceeds of crime or to finance terrorism.

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. Our controls

- Know Your Customer: every investor completes identity verification before investing - government identity document, a photograph holding that document, and a live face capture -

reviewed by trained staff before approval.

- Sanctions and PEP screening: customers and counterparties are screened against applicable sanctions lists, and politically exposed persons receive enhanced due diligence.
- Source of funds: for significant transactions we request and assess evidence of the source of funds and source of wealth.
- Transaction monitoring: an immutable ledger records every money movement; unusual patterns (structuring, rapid in-out flows, third-party funding) are escalated for review.
- Withdrawals are released only to the verified account holder - never to unverified third parties.
- Record keeping: KYC records and transaction data are retained securely (encrypted at rest) for at least five years after the relationship ends, or longer where law requires.

4. 4. Reporting suspicious activity

Any employee who suspects money laundering must escalate immediately to management and must not tip off the customer. Where required, suspicious activity is reported to the competent financial intelligence unit.

5. 5. Breaches

Breaches of this policy are treated seriously. Employees who breach it face disciplinary action up to termination; engagements with third parties who breach it may be suspended or ended. Where conduct may be unlawful, we will notify the competent authorities and cooperate fully.

6. Risk-based approach and customer risk rating

- Every customer is assigned a risk rating (standard / elevated / high) at onboarding, reviewed on trigger events and at least every 24 months.
- Elevated risk factors: non-resident customers from higher-risk jurisdictions, complex ownership structures, unusually large transactions relative to profile, reluctance to provide information.
- High risk (Enhanced Due Diligence mandatory): politically exposed persons, adverse media findings, source-of-funds inconsistencies, or any sanctions-adjacent connection.
- EDD measures: senior management approval of the relationship, independent corroboration of source of funds and wealth, tighter transaction limits and more frequent reviews.

7. Red flags every employee must escalate

- Payment offered from a third party unrelated to the verified account holder.
- Requests to split a purchase into multiple smaller payments without commercial rationale (structuring).
- Rapid deposit followed by a withdrawal request with little or no investment activity (in-out flows).
- Customer indifference to price, fees or investment performance.
- Documents that appear altered, inconsistent between one another, or refusal to complete face verification.
- Requests to route refunds to a different account or jurisdiction than the source of funds.

8. Ongoing monitoring

The transaction ledger is reviewed for unusual patterns on a risk basis. Alerts are documented, investigated and either cleared with rationale or escalated. Where suspicion remains after investigation, a report is made to the competent financial intelligence unit and the file is sealed against tipping-off.

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:

- Real estate is a preferred vehicle for laundering large sums in single transactions.
- Cross-border customer base with documents in many languages and formats.
- Crypto deposits introduce chain-of-funds opacity requiring specialised tracing.
- Fractional tokens lower ticket sizes, creating structuring opportunities across many small purchases.
- Secondary-market trades between investors could be abused for value transfer between colluding parties.
- Third-party introducers may present customers whose identity work we did not perform ourselves.

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.

- Onboarding: identity document capture (front/back), photograph holding the document, and live face capture are mandatory before any deposit is accepted; manual review approves or rejects with reasons recorded.
- Risk rating assigned at approval (standard/elevated/high) using nationality, residency, product, channel and behaviour factors; re-rated on trigger events and at least every 24 months.
- Enhanced due diligence for high-risk: senior approval, independent source-of-funds corroboration, tightened limits, six-monthly review.
- Screening against applicable sanctions and PEP lists at onboarding, on list updates and

before significant transactions.

- Deposits reconcile to the named, verified account holder; third-party payments are rejected and returned to source.
- Crypto deposits: only from wallets the customer attests to controlling; amounts and transaction hashes recorded; blockchain screening applied on a risk basis.
- Ledger monitoring reviews unusual patterns (structuring, rapid in-out, dormancy followed by large flows) on a risk-based cycle; alerts are dispositioned in writing within 5 business days.
- Withdrawals are released only to the verified holder's own account; destination changes require re-verification and a cooling-off review.
- Internal suspicion reports go to the compliance function immediately; where suspicion stands, external reports are filed with the competent FIU and the file is sealed against tipping-off.
- Records of CDD, monitoring and reports are retained at least 5 years after the relationship ends.

12. Application across our markets

Application across our markets: identity documents from dozens of issuing states are accepted only against the document-type register maintained by compliance; where a document type cannot be reliably validated, enhanced verification applies. Local reporting thresholds and FIU procedures are documented per market in the AML operating annex.

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 investor attempts a deposit from a relative's bank account. Response: third-party payment - rejected and returned to source; the investor is invited to pay from their own verified account.
- Situation: a customer makes nine deposits of EUR 1,900 within three weeks. Response: structuring alert raised; enhanced due diligence and source-of-funds corroboration; external report filed if suspicion stands.
- Situation: a crypto deposit arrives from a wallet associated with a mixing service. Response: funds held, chain analysis performed, escalated to compliance; likely refusal, return where lawful, and report.
- Situation: an introducer offers pre-verified clients without underlying documents. Response: no reliance without evidence - we perform our own full CDD or the clients are not onboarded.

14. Definitions

- Money laundering — concealing, converting or transferring the proceeds of crime to make them appear legitimate.
- Terrorist financing — providing or collecting funds, from any source, intended to support terrorist acts or organisations.
- KYC (Know Your Customer) — the identification and verification of a customer's identity and risk profile before and during a business relationship.

- PEP (Politically Exposed Person) — an individual entrusted with a prominent public function, their family members and close associates.
- Source of funds / source of wealth — the origin of the money used in a transaction, and of the customer's overall wealth.

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:

- FATF Recommendations, notably customer due diligence and record keeping
- EU Anti-Money-Laundering Directives as implemented in our EU markets
- UAE AML framework applicable to real-estate transactions
- Local FIU reporting regimes in each operating market

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.