Whistleblowing 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

InterAtlas Estate wants wrongdoing to be reported early and handled properly. This policy protects anyone who, in good faith, raises a concern about misconduct within our business.

2. 2. What to report

- Fraud, bribery, money laundering or sanctions breaches.
- Misuse of client funds or misleading of investors.
- Data-protection violations or unauthorised access to client records.
- Modern slavery in our operations or supply chain.
- Any deliberate breach of law or of our published policies - or the concealment of any of the above.

3. 3. How to report

- To management directly, or by email to compliance@atlasestate.estate.

- Anonymously, by post or via an intermediary, where the reporter prefers - anonymous reports are investigated to the extent the information allows.
- Externally to a competent regulator or law-enforcement authority, where the reporter considers internal routes inappropriate. This policy does not restrict any legal right to do so.

4. 4. Protection of whistleblowers

Retaliation of any kind - dismissal, demotion, harassment or disadvantage - against a person who raises a genuine concern in good faith is itself a serious breach of this policy and will be disciplined accordingly. Confidentiality of the reporter's identity is protected to the fullest extent possible.

5. 5. Investigation

Concerns are acknowledged within 3 business days and investigated by a person independent of the matter. The reporter receives an outcome summary where confidentiality allows, normally within 15 business days.

6. The investigation, step by step

- Day 0-3: acknowledgement to the reporter; case logged with restricted access; investigator appointed (independent of the matter).
- Day 3-10: evidence gathering - records, systems, interviews; interim protective measures where needed (e.g. suspending a permission).
- Day 10-15: findings and recommendation; decision by management (or by the Board where management is implicated).
- Closure: outcome summary to the reporter where confidentiality allows; remediation actions tracked to completion.

7. Examples of matters to report

- A colleague approving their own transactions, or bypassing dual-approval controls.
- Client funds used for anything other than the client's instructions.
- Marketing that promises guaranteed returns, or misstates a property's status.
- Anyone asked to alter, backdate or destroy a record.

8. If management is the problem

Where a concern implicates management itself, the reporter may go directly to a competent external authority. Doing so in good faith is protected by this policy in exactly the same way as internal reporting.

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:

- Fear of retaliation is the primary suppressor of early reporting.
- Small-team structures make anonymity harder to preserve and require extra care.
- Concerns implicating management need a route that bypasses management.
- Cross-border staff face differing local protections; our standard applies group-wide at the highest level.

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.

- Reporting routes: line management; compliance@atlasestate.estate; anonymous post or intermediary; and always the competent external authority.
- Acknowledgement within 3 business days; investigator independent of the matter appointed at once.
- Days 3-10: evidence collection (records, systems, interviews) with interim protective measures where needed.
- Days 10-15: findings and decision; Board decides where management is implicated.
- Reporter identity is restricted to those strictly required; files are access-logged.
- Retaliation in any form is a disciplinary offence up to dismissal; the reporter's career progression is monitored for 12 months as a safeguard.
- Outcomes and remediation actions are tracked to closure and reported to the Board quarterly in anonymised form.

12. Application across our markets

Application across our markets: our protections apply group-wide at the highest common standard, independent of weaker local minimums.

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 employee suspects their own manager of taking kickbacks. Response: the report goes directly to compliance or the Board route - the implicated manager is bypassed entirely.
- Situation: a reporter asks to remain anonymous. Response: accepted - identity is restricted to those strictly required, and the file is access-logged.

- Situation: a reporter's bonus is cut months after their report. Response: investigated as retaliation; disciplinary consequences apply, and the 12-month career-monitoring safeguard is extended.

14. Definitions

- Whistleblowing — reporting, in good faith, suspected wrongdoing or dangers within the organisation.
- Good faith — an honest belief, on reasonable grounds, that the information reported is true.
- Retaliation — any detriment imposed on a person because they raised, or intended to raise, a concern.

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:

- EU Whistleblowing Directive protections as implemented in our EU markets
- Local employment-law protections for protected disclosures

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.