

GLOBAL HORIZONS CAPITAL ADVISORS (IFSC) PRIVATE LIMITED
ANTI-MONEY LAUNDERING (AML), COUNTER-TERRORIST
FINANCING (CFT) & SANCTIONS POLICY

*(Pursuant to Regulation 16 read with AML Guidelines under the IFSCA
(Capital Market Intermediaries) Regulations, 2025)*

1. Purpose and Regulatory Basis

This Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT) and Sanctions Policy ("**Policy**") is adopted as a core component of the governance, risk management, and internal control framework of **Global Horizons Capital Advisors (IFSC) Private Limited** ("**the Company**"), a registered Investment Banker and Capital Market Intermediary operating from the International Financial Services Centre.

This Policy is issued in accordance with **Regulation 16** of the IFSCA (Capital Market Intermediaries) Regulations, 2025 and the **AML Guidelines** issued thereunder, and gives operational effect to **Clause 9 (AML, CFT and Sanctions Compliance)** of the Company's **Code of Conduct**.

This Policy must be read together with, and is complementary to, the Company's:

- Code of Conduct
- Anti-Bribery and Anti-Corruption Policy
- Confidentiality, Inside Information & Market Abuse Policy
- Whistleblower Policy

In the event of any inconsistency, the stricter requirement shall prevail.

2. Applicability

This Policy applies to:

- Directors
- Key Managerial Personnel
- Senior Management
- Employees (permanent, contractual, deputed)
- Consultants, advisors, and any person acting for or on behalf of the Company

All such persons are referred to as "**Covered Persons**."

3. Core AML, CFT and Sanctions Principles

The Company adopts a **risk-based approach** to AML, CFT and sanctions compliance, recognising that its activities as an investment banker involve exposure to complex transactions, cross-border flows, structured products, and multiple intermediaries.

Covered Persons shall ensure that:

- the identity and background of clients and counterparties are known and understood,
- the source of funds and source of wealth are legitimate and verifiable,
- transactions have a clear commercial rationale, and
- the Company is not used, directly or indirectly, to facilitate money laundering, terrorist financing, or sanctions evasion.

Compliance with AML, CFT and sanctions obligations is a **mandatory condition of employment or engagement** and a **non-negotiable regulatory requirement**.

4. Prohibited Activities

The Company shall not knowingly:

- enter into or continue business relationships involving proceeds of crime,
- facilitate transactions designed to conceal or disguise the origin of funds,
- assist in structuring transactions to evade regulatory scrutiny,
- deal with sanctioned persons, entities, jurisdictions, or activities.

Covered Persons shall not assist, ignore, or tolerate arrangements that appear designed to:

- obscure beneficial ownership,
- use shell or opaque structures without commercial justification, or
- bypass due diligence or reporting requirements.

5. Client Due Diligence (CDD)

Appropriate **Client Due Diligence (CDD)** shall be conducted prior to entering into any business relationship and on an ongoing basis thereafter,

commensurate with the risk profile of the client, transaction, product, and jurisdiction.

CDD shall include:

- verification of client identity,
- identification and verification of beneficial owners,
- understanding ownership and control structures,
- assessment of the purpose and intended nature of the relationship.

Enhanced Due Diligence (EDD) shall be applied where higher risk is identified, including for:

- complex or unusual transactions,
- politically exposed persons (PEPs),
- high-risk jurisdictions, or
- structures lacking economic substance.

6. Source of Funds and Source of Wealth

Covered Persons shall take reasonable steps to verify the **source of funds** and, where appropriate, the **source of wealth**, particularly in relation to:

- debt syndication,
- capital raising,
- IPO preparedness,
- cross-border transactions, and
- high-value or structured arrangements.

Transactions where the source of funds cannot be satisfactorily established, appears inconsistent with the client's profile, or lacks credible explanation shall not proceed and must be escalated.

Example:

Unexplained urgency, routing funds through unrelated entities, or resistance to disclosure are red flags requiring escalation.

7. Sanctions Compliance

The Company shall comply with all applicable sanctions laws and lists, including restrictions relating to:

- sanctioned persons and entities,
- prohibited jurisdictions,

- restricted activities or sectors.

Covered Persons shall not engage in or facilitate any transaction that may result in sanctions breaches. Sanctions screening shall form part of onboarding and ongoing monitoring.

8. Ongoing Monitoring and Red Flags

Business relationships and transactions shall be subject to **ongoing monitoring** to identify unusual, suspicious, or inconsistent activity.

Red flags may include:

- unusual transaction patterns,
- complex structures without rationale,
- frequent changes in instructions,
- reluctance to provide information,
- links to high-risk jurisdictions or sectors.

Presence of red flags does not require proof of wrongdoing but **does require escalation**.

9. Escalation and Reporting of Suspicious Activity

Any Covered Person who becomes aware of, or reasonably suspects, money laundering, terrorist financing, sanctions breaches, or related misconduct shall **promptly escalate** the matter to the **Company Secretary & Compliance Officer**, in accordance with internal escalation procedures.

Suspicious Transaction Reports (STRs) or other regulatory reports shall be filed where required, strictly in accordance with applicable law and regulatory guidance.

Failure to escalate suspicious activity may itself constitute a breach of this Policy and the Code of Conduct.

10. Interaction with ABAC and Market Abuse Frameworks

Bribery, corruption, misuse of inside information, and market abuse may give rise to AML risks. Accordingly:

- suspected bribery or corruption shall be assessed for AML implications,

- misuse of confidential information may indicate market manipulation or ML risk,
- such matters shall be escalated under this Policy in coordination with the ABAC and Market Abuse frameworks.

11. Confidentiality and Non-Tipping-Off

All AML-related information, investigations, and reports shall be handled confidentially and on a strict need-to-know basis.

Covered Persons shall not disclose, directly or indirectly, the existence of any suspicion, investigation, or regulatory report to any unauthorised person ("tipping-off").

12. Training and Awareness

The Company shall provide periodic AML, CFT and sanctions training appropriate to roles and risk exposure. Covered Persons are required to familiarise themselves with this Policy and seek guidance where doubt exists.

13. Investigation and Enforcement

Violations of this Policy shall be investigated and enforced in accordance with **Annexure I (Disciplinary and Enforcement Matrix)** and may result in:

- disciplinary action,
- termination of employment or engagement,
- regulatory reporting, and
- civil or criminal proceedings.

Senior management and Directors are subject to heightened accountability for AML failures.

14. Review and Oversight

This Policy shall be reviewed periodically by the **Company Secretary & Compliance Officer**, and any material amendments shall be placed before the **Board of Directors** for approval.