INTEGER WEALTH GLOBAL

Policy Document

Anti-Money Laundering & Countering the Financing of Terrorism (AML/CFT) Policy

Issue: February 2025 (Update from 2022)

1. Purpose

To establish IWG's framework to prevent, detect and report money laundering (ML), terrorist financing (TF) and related offences across all jurisdictions in which IWG operates, ensuring compliance with applicable EU law, FATF standards and local supervisory requirements. This policy implements a risk-based approach to AML/CFT and assigns responsibilities for governance, client due diligence, transaction monitoring and suspicious activity reporting.

(Legal basis: EU AML framework and FATF recommendations.) Finance+1

2. Applicability and legal/regulatory environment

This policy applies to all IWG legal entities and branches. IWG will comply with:

- EU AML directives and related EU regulation (including the AML legislative package / AMLA developments and Funds Transfer Regulation (EU) 2015/847). EUR-Lex+1
- FATF Recommendations as the international standard. FATF
- National laws, regulations and regulator guidance in Luxembourg (CSSF), Liechtenstein (FMA / AMLSC), Gibraltar (GFSC), Cyprus (CySEC and local AML laws). IWG will maintain and apply local legal requirements where they are stricter than EU rules. cysec.gov.cy+3CSSF+3fma-li.li+3

  Note: where EU-wide measures (including AMLA or EU Regulations) apply directly, IWG will ensure uniform baseline controls; local rules and supervisory guidance will be applied in addition.

3. Governance & responsibilities

3.1 Board of Directors

- Owns AML risk appetite and approves this AML Policy.
- Ensures adequate resources and oversight.

3.2 Senior Management

- Ensures implementation, resource allocation and escalation of material AML issues to the Board.

3.3 Group Money-Laundering Reporting Officer (Group MLRO)

- Appointed by the Board; responsible for day-to-day oversight of AML compliance across jurisdictions. Central point for SARs and escalation. Maintains relationships with local competent authorities and FIUs.

3.4 Local Compliance Officers (per jurisdiction/entity)

- Execute local AML program consistent with this policy; ensure local regulatory reporting (SARs, suspicious transaction reports, regulatory notifications). Coordinate with Group MLRO.

3.5 All Employees

- Must complete AML training, follow CDD/EDD, escalate suspicious activity and maintain records.

4. Risk-based approach (RBA)

IWG adopts an RBA to allocate resources proportionate to ML/TF risk. Factors considered:

- Customer (type, ownership, jurisdiction, PEP status, source of funds/wealth)
- Product / service (investment management, custody, payment handling)
- Delivery channel (remote onboarding, face-to-face)
- Geographic risk (high-risk jurisdictions, sanctioned jurisdictions)
- Transactional behaviour (volume, velocity, unusual patterns)

IWG will maintain a documented Group Business Risk Assessment (BRA) and require each business line to maintain local risk assessments updated at least annually or when material change occurs. (Guidance from EU and national supervisors supports an RBA). Finance+1

5. Customer Due Diligence (CDD) & Know Your Customer (KYC)

5.1 When to apply CDD

CDD must be applied when:

- Establishing a business relationship;
- Carrying out occasional transactions above thresholds set by local law;
- Suspicions of ML/TF arise;
- Doubts about completeness/accuracy of previously obtained data.

5.2 Elements of CDD

At onboarding, IWG must obtain and verify:

- Customer identity (natural persons: name, DOB, nationality, address, government ID);
- Legal persons: legal name, registration number, registered office, constitution documents;
- Beneficial ownership: identification of natural persons exercising ultimate control (UBO), using reliable sources and registry checks;

- Purpose and intended nature of relationship;
- Source of funds and, where material, source of wealth;
- Expected transaction profile.

Documentation and verification must be risk-sensitive (ID documents, corporate documents, independent electronic verification, public registries). Where electronic verification is used, controls must confirm reliability and provenance. (Fits FATF/EU guidance and national regulator expectations.) FATF+1

5.3 Enhanced Due Diligence (EDD)

EDD is mandatory for higher risk situations, including:

- PEPs (domestic, foreign, prominent public function holders) or their close associates/family;
- Customers from high-risk or non-cooperative jurisdictions;
- Complex ownership structures or opaque beneficial owners;
- Unusual transaction patterns or large incoming/outgoing transfers with no clear economic rationale;
- Cross-border transactions involving high-risk jurisdictions.

EDD measures include obtaining additional identification, senior management approval, enhanced ongoing monitoring, obtaining independent source-of-funds/wealth evidence, and periodic review at higher frequency.

6. Politically Exposed Persons (PEPs)

- Implement definitions consistent with FATF/EU guidance. Screen onboarding and periodically (automated and manual) for PEP status.
- For PEPs, apply EDD, obtain senior management approval before establishing or continuing a relationship, and apply enhanced ongoing monitoring.
- Document rationale for the risk rating and EDD steps taken.

7. Sanctions, embargoes and watchlists

IWG will screen all customers, beneficial owners and relevant transactions against applicable sanctions lists (UN, EU, UK where relevant, OFAC if applicable to business, and local lists). If an alert is hit:

- Immediately freeze or block assets where required by law;
- Escalate to the Group MLRO and local AML Officer;
- File required notifications with relevant authorities;
- Maintain full documentation of decisions and actions.

Sanctions screening must be both name-based and identifier-based (e.g., DOB, nationality) and include ongoing automated screening of existing customers and transactions.

8. Transaction monitoring & detection

- Implement automated transaction monitoring systems tailored to expected transaction profiles and risk tiers. Monitor for: unusual sizes, frequency, round-sum transfers, rapid movement across jurisdictions, transfers inconsistent with stated business.
- Define alert thresholds and tuning to minimise false positives while capturing genuine risk.
- All alerts are triaged by compliance analysts, investigated, and escalated to MLRO when suspicious.
- For cross-border transfers, ensure payer/payee information complies with Regulation (EU) 2015/847 on information accompanying transfers of funds. EUR-Lex

9. Suspicious Activity Reporting (SAR) / Reporting obligations

- If a transaction or behaviour is suspicious, staff must report internally to the MLRO using the internal SAR form. The MLRO will investigate and decide whether to file an external SAR to the relevant FIU.
- External reporting timelines and formats follow each jurisdiction's requirements (e.g., CSSF FIU, FMA/Liechtenstein reporting channels, GFSC guidance, CySEC/Unit for Combating Money Laundering). IWG will ensure local reporting obligations are met and that no tipping-off occurs. cysec.gov.cy+3CSSF+3fma-li.li+3

10. Record keeping & retention

- Keep records of customer ID, CDD documents, transaction records, SAR investigations, risk assessments, training logs and compliance reviews for the period required by applicable law (commonly 5–10 years depending on jurisdiction). Records must be secure, retrievable and available to competent authorities upon lawful request.

11. Training & awareness

- Mandatory AML/CFT training for all staff on onboarding and annually thereafter, with role-specific modules for client-facing staff, compliance and senior management. Training content will include: CDD processes, red flags, sanctions, SAR procedures, PEPs and new typologies. Training completion and assessment records will be maintained.

12. Independent testing & audit

- Annual independent audit or review of AML programme (internal audit or external specialist) to test effectiveness, including CDD quality, transaction monitoring, SAR filings, system performance, staff training and governance. Findings reported to the Board and remedial actions tracked to closure.

13. Data protection & confidentiality

- AML processing involves personal data. Processing and retention will comply with applicable data protection laws (e.g., GDPR in the EU). Disclosures to FIUs and competent authorities are permitted by law and should be documented. Personal data access is role-restricted.

14. Cross-border & multi-jurisdictional considerations

Operating in Luxembourg, Liechtenstein, Gibraltar and Cyprus requires:

- Implementing the highest common baseline where EU law applies and adding stricter local requirements where present;
- Local Compliance Officers to maintain knowledge of national law and supervise local filings;
- Group MLRO to coordinate cross-border SARs, multi-jurisdictional investigations, and co-operation with foreign FIUs and supervisors;
- Consistent global standards for CDD, sanctions and monitoring while allowing local operational tailoring to meet supervisory expectations. (National regulators published guidance emphasising an RBA and local reporting). cysec.gov.cy+3CSSF+3fma-li.li+3

15. Escalation & communication

- All suspicious activity escalated to MLRO; MLRO escalation to Senior Management and Board where material.
- External communications with supervisors, law enforcement and FIUs coordinated by MLRO and legal counsel.

16. Technology & automation

- Use reliable AML systems for identity verification, beneficial ownership discovery, sanctions screening and transaction monitoring. Systems must be documented, tuned and reviewed regularly for effectiveness. Keep audit trails of automated decisions and human overrides.

17. Policy review

- This Policy will be reviewed at least annually and after material changes in law, business, supervisory expectations or following a significant AML/CFT incident.