INNOVA
GLOBAL LIMITED

AML & KYC

1. Introduction and Summary

These procedures are to be used by all staff members for reference purposes. Additional reference materials may be accessed in the personal area.

This manual has been drafted in compliance with the applicable regulations in the current jurisdiction.

Anti-Money Laundering (AML) requirements, as applied by His Majesty's Revenue and Customs (HMRC) and the National Crime Agency (NCA), may be broadly summarised as follows:

- Innova Global Limited must obtain satisfactory evidence of the identity of each customer with whom it establishes a business relationship through appropriate Customer Due Diligence (CDD) procedures;
- Evidence of client identity must be retained for the duration of the client relationship and for a period of five (5) years after termination; transaction records must also be retained for five (5) years from the date the relationship ends;
- The Company must understand the beneficial ownership structure of business customers, including identifying the individuals who ultimately benefit financially;
- The Company must identify the customer and verify their identity using reliable and independent sources;
- The Company must identify the source of funds where required under a risk-based approach;
- Where the beneficial owner differs from the customer, the Company must take appropriate measures to verify their identity and understand ownership and control structures;
- The Company must obtain information on the purpose and intended nature of the business relationship;
- Enhanced due diligence must be conducted for higher-risk clients, including Politically Exposed Persons (PEPs);

- Any suspicious transaction must be reported immediately to the designated Money Laundering Reporting Officer (MLRO);
- The MLRO shall determine whether to report such suspicions to the relevant authorities, including the NCA in the United Kingdom;
- Appropriate training must be provided to all relevant staff to ensure awareness of AML procedures and legal obligations;

2. Money Laundering

Money laundering is the process by which criminally obtained funds or assets are converted into assets that appear to have legitimate origin.

Criminal property may include money, securities, tangible or intangible assets, or any financial benefit derived from criminal activity, including funds used for terrorism financing.

Examples of money laundering activities include:

- Acquiring, using, or possessing criminal property;
- Handling proceeds of crimes such as theft, fraud, or tax evasion;
- Participating in transactions involving criminal or terrorist property;
- Facilitating the laundering of criminal or terrorist funds;
- Investing proceeds of crime in financial instruments or assets;
- Transferring criminal property;

Money laundering does not occur in a single stage and may involve various methods, from simple transactions to complex financial structures.

The process typically involves three stages:

- **Placement:** Introduction of illegal funds into the financial system (e.g., deposit into a bank account);
- **Layering:** Movement of funds through multiple transactions to obscure their origin;

- **Integration:** Reintroduction of funds into the economy as apparently legitimate assets;

Financial institutions may only observe certain stages of this process, making detection more challenging.

Counter-Terrorist Financing (CTF)

Terrorist financing involves providing funds to support terrorist activities or organisations. This may involve legitimate or illegitimate funds.

Firms must ensure that:

- Customers are not associated with terrorist organisations;
- Their services are not used to facilitate terrorist financing;

Challenges in detecting terrorist financing include:

- Small amounts of funds may be sufficient;
- Legitimate funds may be used, making detection more difficult;

Regulatory Framework

Employees must be aware of and comply with applicable legislation, including:

- The Terrorism Act 2000 and the Anti-Terrorism, Crime and Security Act 2001;
- The Proceeds of Crime Act 2002 (PoCA);
- The Serious Organised Crime and Police Act 2005;
- The Money Laundering Regulations 2017;
- The Counter-Terrorism Act 2008;

Proceeds of Crime Act 2002

The Act establishes criminal offences related to money laundering, including:

- Concealing criminal property;
- Assisting in concealing or transferring criminal funds;
- Entering into arrangements facilitating the use of criminal property;
- Acquiring, using, or possessing criminal property;
- Tipping off individuals about investigations;
- Failure to disclose suspicions of money laundering;

Penalties may include imprisonment and/or fines. Reports must be submitted to the MLRO promptly upon suspicion.

Money Laundering Regulations 2017

The regulations apply to financial institutions and require:

- Customer identification and verification;
- Implementation of AML policies and procedures;
- Ongoing monitoring and compliance measures;

Failure to comply may result in criminal penalties, including imprisonment and fines.

Fourth Money Laundering Directive (MLD4)

The directive introduced a risk-based approach and includes:

- Expanded definition of Politically Exposed Persons (PEPs);
- Requirement for enhanced due diligence;
- Reduced thresholds for certain transactions;
- Increased transparency in beneficial ownership;
- Inclusion of tax crimes as predicate offences;

Fifth Money Laundering Directive (MLD5)

The directive strengthens AML measures, including:

- Regulation of virtual currencies and prepaid instruments;
- Enhanced due diligence for high-risk jurisdictions;
- Improved verification methods using electronic identification;
- Greater transparency in beneficial ownership structures;

Financial Conduct Authority (FCA)

The FCA promotes the integrity of the UK financial system, including the prevention of financial crime and money laundering.

The MLRO provides guidance to staff on AML obligations and compliance requirements.

Joint Money Laundering Steering Group (JMLSG)

The JMLSG provides practical guidance for implementing AML legislation within the financial services industry.

Penalties

Non-compliance with AML laws may result in criminal prosecution, civil liability, and reputational damage. Financial institutions must maintain high standards of integrity, as involvement in financial crime may severely impact business operations and public trust.

3. Measures to Prevent Money Laundering

Innova Global Limited implements a range of measures and internal controls to prevent money laundering and financial crime. These measures are applied throughout daily business operations and are continuously monitored for effectiveness.

- **Client Identification Procedures** – Client identification and due diligence are performed on all new customers and whenever required by legal or regulatory standards. The Company does not engage with clients who have not been properly verified through due diligence and background checks.

- **Due Diligence Questionnaire** – A structured questionnaire is used as part of the onboarding process to collect detailed information about the client. Business clients may be required to provide supporting documentation such as a Certificate of Incorporation or other relevant regulatory documents.

- **Traceable Transactions** – All transactions conducted by Innova Global Limited are recorded and maintained in a manner that allows full traceability, including through payment gateway settlement records.

- **Records Management** – All client-related documents, accounts, and transaction records are retained in accordance with applicable legal and regulatory retention requirements.

An appointed Money Laundering Reporting Officer (MLRO) is responsible for overseeing AML measures and submitting Suspicious Activity Reports (SARs), where appropriate.

All documentation relating to AML reporting, transactions, and customer due diligence is retained for a minimum of five (5) years.

The MLRO ensures that all reports include, at a minimum:

- Dates of the relevant activities;

- Status of transactions (completed, ongoing, or imminent);
- Location of the activity;
- Method by which the activity was carried out;
- Amount of funds involved;
- Grounds for suspicion;

Based on available information, the MLRO must assess whether there are reasonable grounds for knowledge or suspicion of money laundering and determine whether a report to the National Crime Agency (NCA) is required.

Firm Responsibility

Innova Global Limited is required to establish and maintain effective systems and controls to prevent its services from being used for money laundering or terrorist financing.

The MLRO has overall responsibility for AML oversight, including the implementation of financial crime prevention strategies and regulatory reporting obligations.

Compliance Monitoring

The MLRO is responsible for ensuring that AML systems, controls, and policies remain up to date and compliant with applicable regulations.

High-Risk Jurisdictions

The Company complies with directives issued by HM Treasury and international bodies such as the Financial Action Task Force (FATF).

Where required, the Company will:

- Refrain from entering into business relationships with clients from high-risk or non-cooperative jurisdictions;

- Apply enhanced due diligence measures;
- Monitor and act upon international findings related to AML deficiencies in specific countries;

Responsibility of Staff

All employees, regardless of their role, are required to:

- Remain aware of AML/CTF obligations;
- Report any suspicions of financial crime to the MLRO;
- Comply with all internal AML policies and procedures;

Failure to report suspicions or comply with AML requirements may result in disciplinary action.

Responsibility of the MLRO

The MLRO is responsible for overseeing the Company's AML framework, including:

- Receiving and reviewing internal reports of suspicious activity;
- Investigating potential financial crime;
- Submitting SARs to the NCA where required;
- Ensuring staff training and awareness;
- Reporting to regulators on AML effectiveness;
- Responding to regulatory requests (e.g., FCA);
- Assessing risks related to new products, jurisdictions, and business relationships;

- Approving relationships involving high-risk clients, including Politically Exposed Persons (PEPs);

The MLRO must balance timely reporting obligations with the need to gather sufficient information. Where necessary, an initial report may be submitted before completing a full investigation.

SARs may be submitted through approved channels, including:

- NCA SARs Online system;
- Secure electronic communication methods;
- Other officially recognized reporting mechanisms;

Where the MLRO decides not to submit a report, the reasoning must be clearly documented and retained.

4. Risk Assessment

Carrying Out the Risk Assessment

The first step in conducting Customer Due Diligence (CDD) is to assess the level of risk a prospective client may present. Based on this assessment, the appropriate level of due diligence should be applied.

Clients are categorized into three risk levels:

- **Low Risk**
- **Medium Risk**
- **High Risk**

When assessing a client's risk level, the following factors must be considered:

- The nature of the product or service requested;
- The nature and duration of any existing or previous relationship with the client;

- Any assurances from other Financial Conduct Authority (FCA)-regulated firms (e.g., introducer certificates). However, reliance on third parties does not remove the Company's responsibility to conduct its own due diligence;
- Whether the client is physically present during onboarding;
- Whether the client is a Politically Exposed Person (PEP);
- The client's geographic location, particularly if it is a high-risk jurisdiction;
- Any other indicators suggesting potential involvement in money laundering or terrorist financing;

A cautious approach should always be taken when performing risk assessments. If any "red flags" are identified, Enhanced Due Diligence (EDD) must be applied.

Low-Risk Examples

The following are examples of clients typically considered low risk (subject to no additional concerns):

- Financial institutions regulated under AML frameworks (e.g., FCA, EU regulators, or equivalent authorities);
- Companies listed on regulated markets;
- Beneficial owners of pooled accounts held by notaries or legal professionals;
- UK public authorities or equivalent bodies;
- Recognized international institutions;
- Pension funds;
- Child trust funds;

Medium-Risk Example

- Individuals based in the UK or another jurisdiction with equivalent regulatory standards;

High-Risk Examples

The following scenarios typically indicate higher risk and require Enhanced Due Diligence:

- Presence of a Politically Exposed Person (PEP) within a client structure or as an individual client;
- Complex or non-transparent ownership structures;
- Clients located in high-risk or non-cooperative jurisdictions;
- Non-face-to-face onboarding processes;

Sanctions and PEP Screening

As part of AML risk assessment, the Company must conduct sanctions and PEP checks on:

- All individual clients;
- Individuals associated with legal entities (e.g., directors, beneficial owners, controllers, authorized signatories);

The following actions apply:

- If a client appears on a sanctions list, the Company must refuse to establish or continue the relationship;
- If a client is identified as a PEP, Enhanced Due Diligence procedures must be applied;

- The Company must maintain internal controls to prevent engagement with sanctioned individuals;

Jurisdiction Risk

The classification of jurisdictions as “equivalent” or “high-risk” is based on guidance from recognized bodies such as the Joint Money Laundering Steering Group (JMLSG) and international standards (e.g., FATF).

Generally:

- European Economic Area (EEA) countries are considered lower risk due to aligned regulatory frameworks;
- High-risk jurisdictions require additional scrutiny and enhanced due diligence measures;

Austria	Belgium	Denmark	Finland
France	Germany	Greece	Ireland
Italy	Luxembourg	Netherlands	Portugal
Spain	Sweden	Bulgaria	Cyprus

Jurisdictions outside of the European Economic Area (EEA) that are considered to have equivalent AML/CTF frameworks, and may therefore be classified as **lower risk**, include the following:

Argentina	China	New Zealand	Turkey
Australia	Brazil	Hong Kong	
India	Japan	South Korea	Mexico
Singapore	Switzerland	South Africa	

These classifications are based on available regulatory guidance and international assessments.

For the most up-to-date information on equivalent jurisdictions, please refer to official sources such as the Joint Money Laundering Steering Group (JMLSG).

Additionally, guidance on high-risk jurisdictions may be obtained from Transparency International, including:

- Corruption Perceptions Index (CPI)
- Research and analytical reports

5. Record Keeping Requirements

Client Record Keeping

All documentation obtained for the purpose of verifying a client's identity and fulfilling Customer Due Diligence (CDD) requirements must be retained for a minimum of **five (5) years** after the end of the client relationship.

- Copies of all documentation must be stored electronically to allow efficient retrieval;
- Where paper documents are received, copies must be created and securely stored;
- Transaction records must be retained for at least **five (5) years** from the date of the transaction;

Internal and External Reports

Where applicable, records must be maintained for:

- Internal and external suspicious activity reports (SARs);
- Actions taken in relation to such reports;
- Decisions made by the MLRO, including cases where no external report was submitted;
- Clients refused due to high risk, sanctions, or other compliance concerns;

Training Record Keeping

The Company must maintain records of all AML training provided to staff, including:

- Dates of training sessions;
- Content and nature of the training;
- Names of attendees;
- Confirmation that staff understood the training;
- Results of any assessments, where applicable;

MLRO Annual Reports

The MLRO shall prepare an annual report assessing the effectiveness of AML systems and controls. These reports must be retained for at least **five (5) years**.

6. MLRO and Reporting of Suspicious Transactions

MLRO Responsibilities

The MLRO is responsible for:

- Receiving and reviewing internal reports of suspicious activity;
- Determining whether external reporting is required;
- Overseeing AML systems and controls;
- Reporting to senior management on AML/CTF effectiveness;
- Ensuring compliance with applicable regulations;

Reporting Suspicious Activity

All staff must:

- Report suspicions of money laundering or terrorist financing to the MLRO as soon as reasonably practicable;
- Submit internal reports when there are reasonable grounds for suspicion;

The MLRO must:

- Review all internal reports;
- Submit reports to the National Crime Agency (NCA) where appropriate;
- Seek consent from authorities before proceeding with suspicious transactions when required;

It is a criminal offence to **“tip off”** a client or third party that a report has been made or that an investigation is underway.

Reporting Procedures (Summary)

- All suspicions must be reported internally;
- The MLRO must evaluate all reports;
- External reporting must be made where required;
- Funds must be frozen if a client appears on sanctions lists;
- Suspicious attempts to engage in business must also be reported;

7. Customer Due Diligence (CDD) Documentation

General Requirements

All due diligence documentation must be:

- Accurate and complete;
- Properly recorded and stored;
- Reviewed and approved by relevant staff;

Documents in Foreign Languages

Documents provided in a foreign language must be accompanied by a certified English translation.

Original Documents and Copies

- Copies of original documents must be clearly marked, dated, and signed by the staff member verifying them;
- Both physical and electronic copies must be securely stored;

Politically Exposed Persons (PEPs)

A PEP is an individual entrusted with prominent public functions, including close associates and family members.

Examples include:

- Heads of state or government officials;
- Senior judicial or military officials;

- Central bank officials;
- Executives of state-owned enterprises;

Where a PEP is identified:

- Senior management approval is required;
- Enhanced Due Diligence (EDD) must be applied;
- Source of wealth and funds must be verified;
- Ongoing monitoring must be increased;

Ongoing Due Diligence and Monitoring

The Company must continuously monitor client relationships, including:

- Reviewing transaction patterns;
- Ensuring client information remains up to date;
- Adjusting monitoring frequency based on risk level;

Indicators requiring attention include:

- Unusual transaction size or frequency;
- Transactions involving high-risk jurisdictions;
- Dealings with sanctioned or suspicious parties;

Enhanced Due Diligence (EDD) – Individuals

EDD must be applied in higher-risk situations, including:

- PEPs;
- Non-face-to-face clients;
- Complex or unusual transactions;
- Clients from high-risk jurisdictions;

Required documentation may include:

- Government-issued ID (passport or driver's license);
- Proof of address (utility bill, bank statement, etc.);
- Source of funds and wealth;
- Employment or business details;

Due Diligence – Legal Entities

For corporate clients, the Company must:

- Verify company registration and legal status;
- Identify beneficial owners (≥25% ownership/control);
- Verify directors and authorized signatories;

Documentation may include:

- Certificate of Incorporation;
- Memorandum and Articles of Association;
- Financial statements;
- List of authorized signatories;

Enhanced Due Diligence must be applied where risk factors are identified, including complex ownership structures or links to high-risk jurisdictions.

8. Miscellaneous Due Diligence

Trusts

For trusts, the identity of relevant parties must be verified in accordance with individual Due Diligence procedures. This includes:

- The settlor (person providing the funds);
- Trustees;
- Any individuals exercising control or influence over the trust;

The following information must also be obtained:

- Full name of the trust;
- Nature and purpose of the trust;
- Country of establishment;
- Names of all trustees;
- Names of beneficial owners;
- Name and address of any protector or controller;
- List of authorised signatories;

This information is typically available from the trust deed or relevant official register.

Partnerships and Unincorporated Entities

All beneficial owners must be identified. A beneficial owner is any individual who:

- Owns or controls more than 25% of capital or profits;

- Holds more than 25% of voting rights;
- Exercises control over management;

Required information includes:

- Full legal name;
- Business address;
- Names of partners or controlling individuals;
- Names of beneficial owners;
- List of authorised signatories;

Verification must be based on reliable and independent sources. Smaller entities should be treated similarly to individuals, while larger entities may rely on professional or trade association verification, supported by additional documentation.

Public Sector Bodies and Government Entities

Simplified Due Diligence may be applied to public authorities where:

- The entity performs public functions;
- Its identity is publicly available and verifiable;
- It is subject to appropriate oversight;

Required information includes:

- Full name and legal status;
- Address;
- Nature of the entity;

- Supervisory authority;
- Directors or equivalent কর্মকর্ত
- Authorised signatories;

Pension Schemes

Where pension schemes are registered with HMRC or the relevant regulatory authority, such registration may be sufficient for verification purposes.

If registration cannot be confirmed, the scheme must be assessed according to its legal structure, and standard Due Diligence procedures must be applied.

Non-Face-to-Face Identification

Non-face-to-face onboarding presents higher risks and requires additional verification measures, such as:

- Verifying payments from an account in the client's name with a regulated institution;
- Conducting additional identity checks or reviewing electronic footprints;
- Performing verification calls;
- Sending confirmation to a verified address;
- Using secure authentication methods (e.g., tokens, codes);
- Requiring certified copies of documents;

Source of Funds

In certain low-risk scenarios, the source of funds may be used as supporting evidence of identity, provided:

- The funds originate from a regulated financial institution;
- The account is in the name of the client;
- The rationale is documented and justified;

---

9. Appendix 1 (Definitions)

Conflict-Affected and High-Risk Areas

Regions characterized by armed conflict, political instability, violence, or systemic legal and institutional weaknesses, which increase the risk of financial crime and human rights violations.

Due Diligence

An ongoing process through which a company identifies, assesses, and mitigates risks related to financial crime, ensuring compliance with applicable laws and international standards.

Management System

A structured framework of policies, procedures, and controls designed to ensure consistent and effective compliance with regulatory requirements and continuous improvement.

Regulated Market

A multilateral trading system operated by a market operator that brings together multiple buyers and sellers of financial instruments under defined rules, in accordance with applicable regulations such as MiFID.

10. Appendix 2 – Due Diligence Documents List

Group 1 – Primary Identification Documents

- Passport (valid and current)
- Biometric Residence Permit (UK)
- Driving Licence (UK, Isle of Man, Channel Islands)
- Birth Certificate (issued at time of birth – UK or Channel Islands)

Group 2a – Secondary Identification Documents

- Driving Licence (UK or non-UK, valid up to 12 months)
- Birth Certificate (UK or Channel Islands)
- Marriage or Civil Partnership Certificate (UK or Channel Islands)
- Adoption Certificate (UK or Channel Islands)
- HM Forces ID Card (UK)
- Firearms Licence (UK or Channel Islands)

Group 2b – Supporting Documents (Proof of Address / Financial)

- Mortgage Statement (UK or EEA)
- Bank or Building Society Statement (UK, Channel Islands, or EEA)
- Bank Account Opening Confirmation Letter (UK)

- Credit Card Statement (UK or EEA)
- Financial Statement (e.g., pension or endowment – UK)
- P45 or P60 Statement (UK or Channel Islands)
- Council Tax Statement (UK or Channel Islands)
- Work Permit or Visa (UK, valid)
- Letter of Sponsorship (non-UK applicants only)
- Utility Bill (UK, excluding mobile phone bills)
- Benefit Statement (e.g., Child Benefit, Pension – UK)
- Government-issued letters (central or local authority – UK or EEA)
- EU National ID Card
- PASS-accredited ID card (UK or Channel Islands)

Verification Routes

Route 1 (Standard)

The client must provide:

- **1 document from Group 1**, and
- **2 additional documents** from Group 1, 2a, or 2b

At least **one document must confirm the client's current address**.

Route 2 (Alternative)

If the client cannot provide a Group 1 document:

- **1 document from Group 2a**, and
- **2 additional documents** from Group 2a or 2b

At least **one document must confirm the client's current address**.

Route 3 (Exceptional)

Used only if Routes 1 and 2 are not possible:

- Birth Certificate (issued after birth – UK or Channel Islands),
- **1 document from Group 2a**, and
- **3 additional documents** from Group 2a or 2b

At least **one document must confirm the client's current address**.