AML/CFT Policy

Compliance Policy | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to “the Company” with your organisation’s name.

Document Control

Document name	AML/CFT Policy
Document type	Compliance Policy
Jurisdiction	Global
Owner	Chief Compliance Officer / AML/CFT Compliance Officer
Approved by	Board of Directors
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose

This Policy sets out the principles, minimum requirements and accountabilities through which the Company identifies, assesses, manages, mitigates and reports the money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks arising from its business. It gives effect to the FATF 40 Recommendations, the Basel Committee's guidelines on the sound management of ML/TF risks, Wolfsberg Group standards, and the Company's AML/CFT obligations under applicable law in each operating jurisdiction.

The Policy is the governing document of the Company's financial crime framework. It is implemented through the Company's AML/CFT Program — the business-wide ML/TF/PF risk assessment, customer due diligence procedures, and monitoring and reporting arrangements — and through supporting procedures and system controls. Where this Policy and the Programme conflict, this Policy prevails and the conflict must be reported to the AML/CFT Compliance Officer (AMLCO) within [5] business days of identification. The AMLCO must resolve it and report the resolution to the [Board Risk Committee] at its next meeting. Where the conflict concerns a requirement the AMLCO personally operates or approves, it must be referred instead to the Chair of that Committee, who must determine the resolution.

The Board of Directors has approved this Policy and has no appetite for wilful or negligent breaches of AML/CFT laws. Compliance failures expose the Company to civil and criminal penalties, licence revocation, exclusion from correspondent relationships and serious reputational damage, and expose the community to harm from crime and terrorism.

2. Scope

This Policy applies to the Company and each of its subsidiaries and branches, and to all directors, employees, contractors, secondees and agents (together, staff), wherever located. It applies to every product and service the Company provides, across all customer segments, delivery channels (branch, broker, digital and third-party) and jurisdictions in which the Company operates. Consistent with FATF Recommendation 18, the Programme applies group-wide, and foreign branches and subsidiaries must apply the higher of local requirements and this Policy to the extent local law permits.

Where the Company outsources activities connected with its products and services — including onboarding, identity verification, transaction processing, screening or monitoring — the third party must comply with the relevant requirements of this Policy and the Programme, and the arrangement must satisfy the Outsourcing Policy. Reliance on third parties for elements of CDD is permitted only where FATF Recommendation 17 and applicable law allow; ultimate responsibility for CDD remains with the Company at all times.

This Policy addresses AML/CFT obligations. Sanctions screening and asset freezing are governed in detail by the Sanctions Policy; fraud and anti-bribery matters by the Fraud Risk Management Policy and the Anti-Bribery and Corruption Policy. Those documents must be read alongside this Policy, whose tipping-off and reporting requirements prevail in any interaction between them.

Jurisdictional application. This Policy states international best practice, anchored to the FATF 40 Recommendations and related standards. The AMLCO must map this Policy's requirements to the AML/CFT laws, regulations and FIU rules of each jurisdiction in which the Company operates, and document that mapping in the obligation register, which the [Chief Compliance Officer] owns and must refresh at least annually and within [20] business days of any material change in an operating jurisdiction's AML/CFT law or FIU guidance. Where local law imposes a stricter or additional requirement, local law prevails.

3. Definitions

Term	Definition
AML/CFT	Anti-money laundering and countering the financing of terrorism, including countering proliferation financing, as framed by the FATF 40 Recommendations and applicable law in the Company's operating jurisdiction(s).
AML/CFT Program	The documented programme of ML/TF/PF risk assessment, policies, procedures, systems and controls the Company maintains to prevent, detect and report money laundering, terrorism financing and proliferation financing.
AML/CFT Compliance Officer (AMLCO)	The senior officer appointed at management level to oversee the Company's AML/CFT compliance, act as its contact point with the FIU and relevant authorities, and decide suspicious transaction reporting. In some jurisdictions this role is designated the Money Laundering Reporting Officer (MLRO).
Beneficial Owner	The natural person or persons who ultimately own or control a customer, directly or indirectly, including through holding [25]% or more of the ownership interests or voting rights (or any lower threshold prescribed by applicable local law), any person who otherwise exercises ultimate effective control over the customer, and any person on whose behalf a transaction is conducted.
Correspondent banking	The provision of banking services by one bank (the correspondent) to another bank (the respondent), including cash management, international wire transfers,

	payable-through accounts and foreign exchange services.
Customer	A natural person, legal person or legal arrangement to whom the Company provides, or proposes to provide, a financial product or service, whether through a business relationship or an occasional transaction, including account holders, signatories, borrowers, depositors, and parties to payment, remittance or value transfer transactions.
Customer Due Diligence (CDD)	The measures by which the Company identifies a customer and verifies its identity using reliable and independent sources, identifies and takes reasonable measures to verify beneficial owners, understands the ownership and control structure and the purpose and intended nature of the business relationship, and keeps that understanding current through ongoing monitoring, consistent with FATF Recommendation 10.
Enhanced Due Diligence (EDD)	More intensive due diligence measures applied beyond the standard requirements where the money laundering, terrorism financing or proliferation financing risk of a customer, counterparty, transaction, relationship or other party is assessed as high, or where a mandatory trigger arises, including additional verification, establishment of source of funds and source of wealth, senior management approval and enhanced ongoing monitoring.
Financial Intelligence Unit (FIU)	The national agency in each jurisdiction in which the Company operates that acts as the central authority for receiving, analysing and disseminating suspicious transaction reports and other information relevant to money laundering, associated predicate offences, terrorism financing and proliferation financing, consistent with the FATF Recommendations.
ML/TF/PF Risk	The risk that the Company may reasonably face that the provision of its products and services might, whether inadvertently or otherwise, involve or facilitate money laundering, terrorism financing or proliferation financing.
Ongoing CDD	The ongoing process of scrutinising transactions and reviewing and updating

	customer information and risk ratings, so that CDD information remains accurate and appropriate to the customer's ML/TF/PF risk throughout the relationship.
Politically Exposed Person (PEP)	An individual who is or has been entrusted with a prominent public function, whether domestically, in a foreign country or by an international organisation, together with that individual's immediate family members and close associates, classified as domestic, foreign or international organisation PEPs consistent with the FATF standards.
Shell Bank	A bank that has no physical presence in the country in which it is incorporated and licensed, and that is not affiliated with a regulated financial group subject to effective consolidated supervision.
Source of Funds	The origin of the particular funds or other assets involved in a business relationship or transaction with the customer, including the activity that generated them and the means by which they were transferred.
Source of Wealth	The origin of the entire body of wealth of a customer or beneficial owner, including how that wealth was acquired and whether its volume is consistent with the person's known profile and with what could reasonably be expected of that person.
Suspicious Transaction Report (STR)	A report submitted to the FIU, however styled in the relevant jurisdiction and including a suspicious activity report (SAR), where the Company suspects or has reasonable grounds to suspect that funds or activity are the proceeds of criminal conduct, including fraud, or are related to terrorism or proliferation financing, consistent with FATF Recommendation 20.
Targeted Financial Sanctions	Asset-freezing measures and prohibitions on making funds or other assets available, directly or indirectly, to or for the benefit of specifically designated persons and entities, as required by United Nations Security Council resolutions, reflected in FATF Recommendations 6 and 7, and imposed under applicable autonomous sanctions regimes.
Tipping Off	The prohibited disclosure to a customer or

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.