

GCB FINTECH — AML/CTF POLICY

DOCUMENT CONTROL & METADATA

Platform: GCB Fintech — <https://gcbfintech.digital>
Version: 1.26 | Effective Date: October 20, 2026
Contact: compliance@gcbfintech.digital

3. AML/CTF Policy

3.1 Governance and responsibility

Each entity is responsible for the compliance obligations applicable to its own business. GC Global Finance Ltd. maintains the AML/CTF programme applicable to its Canadian MSB activities. GC Trust KB maintains the AML/CFT controls applicable to its Swedish trust and foundation management activities and any related activity undertaken under a trust arrangement.

The entities maintain appropriate compliance responsibility, internal controls, documented procedures, training, record keeping, risk assessment and escalation arrangements. Staff, contractors and relevant service providers must follow the procedures applicable to their role and report suspected financial crime through the designated internal channels.

3.2 Risk-based approach

Risk is assessed using relevant customer, product, service, transaction, delivery-channel, geographic and counterparty factors. Higher-risk indicators may include complex or opaque ownership, unexplained wealth, high-risk jurisdictions, unusual virtual-asset activity, rapid movement of value, use of mixers or tumblers, inconsistent customer explanations, adverse media, PEP exposure, sanctions concerns, fraud indicators, high-risk trust structures, unexplained third-party payments and activity inconsistent with the stated purpose of the relationship.

Risk ratings are not permanent. They may change as new information, transactions, adverse information, regulatory guidance or typologies emerge.

3.3 Transaction monitoring

We may monitor transactions and account activity for unusual, inconsistent or suspicious patterns. Monitoring may consider transaction size and frequency, counterparties, wallet addresses, geographic exposure, funding and withdrawal patterns, use of intermediaries, source and destination of funds, asset type and the relationship's stated purpose.

Where activity cannot be reasonably understood or supported, we may seek additional evidence, apply enhanced controls, refuse the activity or escalate it for investigation and reporting.

3.4 Reporting and non-disclosure

Where required, the responsible entity may make reports or disclosures to FINTRAC, the Swedish authorities, law-enforcement bodies, financial-intelligence units, sanctions authorities, courts, correspondent institutions or other competent authorities. We may not notify a customer that a suspicious-transaction report or equivalent confidential report has been made where prohibited by law.

3.5 Record keeping

We retain KYC, transaction, trust, screening, investigation, communication and compliance records for the period required by applicable law and our documented retention schedule. Records may be held in Canada, Sweden, the European Economic Area or other jurisdictions through approved service providers, subject to applicable privacy and transfer safeguards.

3.6 Training and review

Relevant personnel receive role-appropriate AML/CTF training. Policies, risk assessments and controls are reviewed periodically and when there is a material change to law, regulation, products, technology, delivery channels or risk exposure.