AML Policy

MINT AML POLICY

Internal/External	External (Public)
Policy Owner	Legal, Risk and Compliance/Information Officer
Approved By	EXCO
Date	November 2025
Reviewed Date	January 2026
Next Review	March 2027

1. **PURPOSE AND SCOPE**

1.1. MINT is committed to the highest standards of integrity in its business operations. Its objective is to ensure that its platform is not used, directly or indirectly, to facilitate money-laundering, terrorist financing or proliferation financing (collectively "**ML/TF/PF**") and that it complies fully with applicable South African laws and regulations, including the FIC Act and its implementing regulations.

1.2. This policy applies to:

1.2.1. All employees, officers, directors, contractors and agents of MINT;
1.2.2. All customers (both individuals and legal entities) and those who seek to open accounts or transact via the platform;
1.2.3. All transactions in fiat currency and crypto-assets (and any other asset classes in which MINT operates now or in the future).

2. **LEGAL AND REGULATORY FRAMEWORK**

2.1. The FIC Act and its obligations:

2.1.1. The FIC Act requires accountable institutions to implement a risk-based approach (RBA) to ML/TF/PF risk.
2.1.2. Under the FIC Act, the institution must develop, document, maintain and implement a Risk Management and Compliance Programme ("**RMCP**") which includes, inter alia, customer due-diligence (CDD), transaction monitoring, targeted financial sanctions, risk assessment, record-keeping, training, internal controls.
2.1.3. The institution must conduct ongoing monitoring and keep appropriate records for at least five years from the termination of the relationship or transaction date.
2.1.4. The institution must screen against targeted financial sanctions lists (TFS), including those of the United Nations Security Council, and freeze assets where required.

2.2. Additional obligations and guidance (including the recently revised Guidance Note 7A, the Public Compliance Communications, etc) should be adhered to.

2.3. MINT will treat itself as an accountable institution under the FIC Act and ensure registration with the FIC, submission of required reports, and ongoing compliance. (Ensure registration with the FIC within 90 days of commencement of operations, etc.).

3. **GOVERNANCE & INTERNAL CONTROLS**

3.1. **Board or Senior Management Oversight:**
The board of directors (or equivalent senior management) must approve the RMCP and review it periodically, applying its mind to the adequacy of the programme relative to MINT's risk profile. This responsibility cannot be delegated away.

3.2. **Compliance Officer:**
MINT shall appoint a suitably qualified and senior-level Compliance Officer who is accountable for the design, implementation, maintenance and reporting of the Page 2AML/CTF framework. The Compliance Officer reports directly to senior management and the board (or its audit/risk committee) on compliance matters.

3.3. **Internal Policies & Procedures:**
MINT must document internal policies, procedures and controls covering CDD/EDD, monitoring, sanctions screening, record-keeping, internal reporting (including suspicious transaction reports), training, audits and vendor management.

3.4. **Outsourcing & Third-Party Providers:**
Where MINT outsources AML/CTF functions (for example, to provide automated sanctions screening and risk rating), it remains accountable for the performance of those functions and must conduct periodic due diligence and oversight of the third-

party provider.

3.5. **Independent Audit & Review:**
MINT shall arrange for periodic (at least annual) independent review or audit of its AML/CTF framework (internal or external) to test its effectiveness and compliance with regulatory obligations.

4. **RISK-BASED APPROACH**

4.1. MINT shall adopt a formal risk-based framework, in line with Guidance Note 7A, that identifies and assesses inherent and residual risk of ML/TF/PF in the context of its business (including crypto-assets, fiat, platform transactions, peer-to-peer flows, external exchanges).

4.2. The risk assessment must take into account:

4.2.1. Customer risk (e.g., individuals vs legal entities; politically exposed persons (PEPs); beneficial owners; high-risk jurisdictions);
4.2.2. Product/service risk (e.g., crypto-asset exchanges, high velocity trading, cross-border flows, externalisation of funds);
4.2.3. Delivery channel risk (e.g., remote onboarding, digital identity/verification, device/device-fingerprinting);
4.2.4. Geographic risk (e.g., customers or flows from high-risk jurisdictions);
4.2.5. External risks (e.g., evolving typologies of money-laundering, terrorist financing, proliferation financing).

4.3. Based on that risk assessment, MINT shall apply appropriate controls and enhanced due diligence (EDD) for higher-risk customers and transactions (see Section 6).

4.4. The risk-based framework shall be reviewed at least annually or when there is a material change in the business or risk environment.

5. **CUSTOMER ON-BOARDING & KNOW YOUR CUSTOMER (KYC) / CUSTOMER DUE DILIGENCE (CDD)**

5.1. **Customer Classification:**
Upon account creation, customers will be classified (e.g., low, medium, high risk) based on identified risk criteria (jurisdiction, volume, product type, PEP status, beneficial ownership complexity, source of funds).

5.2. **On-boarding process (individuals and legal entities):**

5.2.1. Individuals

5.2.1.1. Customers shall provide personal information (full name, date of birth, identity number/passport number, residential address, contact details).
5.2.1.2. Verification of identity document (national ID or passport) using reliable, independent source(s).
5.2.1.3. Proof of address (e.g., utility bill, bank statement) not older than three months (or per policy) and verifying residence.
5.2.1.4. Verification of mobile number (device-linking, OTP) and any other identity proofing (e.g., biometric, facial match) as needed.
5.2.1.5. Source of funds/wealth information: At minimum for higher risk customers or large volumes, upload of bank statements or other evidence of source of funds.

5.2.2. **Legal Entities/Businesses**

5.2.2.1. Obtain corporate registration documents, beneficial ownership information (identify ultimate beneficial owners (UBOs) holding 25 % or more or other thresholds as defined in policy), proof of business address, nature of business, anticipated activity, expected transaction volumes.
5.2.2.2. Verification of those documents via independent reliable sources.
5.2.2.3. For entities domiciled outside South Africa, obtain certified copies of registration documents and verify via competent local authorities and consider country-risk.

5.3. **Enhanced Due Diligence (EDD):**
For high-risk customers (PEPs, high-volume or rapid transaction flows, complex ownership, high-risk jurisdictions, crypto to external exchanges) additional measures

will apply, including but not limited to:

5.3.1. further verification of source of funds/wealth;
5.3.2. ongoing monitoring at higher frequency;
5.3.3. senior management approval to onboard;
5.3.4. more stringent transaction limits; and
5.3.5. more frequent review of relationship.

5.4. **Timing of Verification:**
MINT may allow limited functionality (e.g., deposit, basic trading) pre-verification, but full access (withdrawal of fiat, large volumes, external transfers) shall only be permitted after full verification (KYC) and risk assessment (i.e., "**verified status**").

5.5. **Failure to Verify/Reject:**
If verification cannot be completed (or information appears false/misleading), MINT shall reject or terminate the account/dr relationship in line with the FIC Act section 21E (which prohibits entering into or maintaining relationships where CDD cannot be performed).

5.6. **Beneficial Ownership & Legal Entities:**
MINT shall maintain procedures to identify beneficial owners and control rights of legal entities/trusts. Where entities are high-risk or ownership unclear, additional steps shall be taken.

6. **TRANSACTION MONITORING, SANCTIONS & REPORTING**

6.1. **Ongoing Monitoring:**
MINT shall continuously monitor customer relationships and transactions, including:

6.1.1. Assessing whether transactions are consistent with the customer's known profile, business, risk classification and source of funds.
6.1.2. Monitoring transaction patterns, volumes, velocity (frequency of transactions and external flows) and geographies of counterparties.
6.1.3. Flagging unusual or suspicious transactions (e.g., rapid transfers to external exchanges, large fiat/crypto conversions, cross-border movements, layering).

6.2. **Sanctions & Watchlists:**

6.2.1. MINT shall screen prospective customers and existing customers regularly against the relevant sanctions lists (including UNSC TFS, domestic FIC lists, other jurisdictional lists) via its third-party sanctions-screening provider.
6.2.2. If a match is identified or a high-risk flag triggered, the account is to be locked/pending review and relevant processes (including asset freeze if required) are initiated.

6.3. **Internal Reporting:**
MINT shall maintain internal procedures for employees and relevant stakeholders to report suspected ML/TF/PF to the Compliance Officer or designated desk; records of these internal reports shall be maintained.

6.4. **External Reporting:**
MINT shall file reports to the FIC as required by the FIC Act and regulations, including:

6.4.1. Suspicious and unusual transaction reports (STRs) when MINT knows or suspects that funds or property may be proceeds of unlawful activity, or are linked to terrorist financing.
6.4.2. Cash Threshold Reports (CTRs) and Terrorist Property Reports (TPRs), as applicable under the regulations.

6.5. **Record Keeping:**
MINT shall maintain customer due-diligence, transaction and reporting records for a minimum of five years from termination of the relationship, transaction date or date of report submission.

6.6. **Account Freezing/Blocking:**
When suspicious behaviour is detected, MINT will place the account on hold (withdrawals/trading/externals disabled) pending investigation. If necessary, funds or transactions will be frozen, and regulatory authorities will be notified where required.

7. **EXCHANGE CONTROL, FIAT/FOREIGN INVESTMENT ALLOWANCES AND CRYPTO EXTERNALISATION**

7.1. **Exchange Control Compliance:**
MINT will implement controls to ensure compliance with South African exchange control rules (externalisation of funds, foreign investment allowances, etc.) as they relate to fiat deposits/withdrawals, transfers in and out of South Africa, and crypto flows to external exchanges.

7.2. **Limits & Notifications:**
MINT shall apply system limits reflecting user foreign allowances (for example, Single Discretionary Allowance, Foreign Investment Allowance) and provide notifications at the time of deposit/withdrawal that such allowance has been used/affected.

7.3. **Beneficiary/External Transfer Controls:**
Page 8No user may externalise funds or transfer to an external exchange (crypto or fiat) without prior verification of the beneficiary account, bank verification check, and AML/CTF risk review.

7.4. **Reporting & Audit Trail:**
All external transfers relating to cross-border flows, crypto externalisation or fiat withdrawals must be logged, traceable, and subject to internal audit and possibly regulatory reporting if thresholds or suspicions arise.

8. **TECHNOLOGY, AUTOMATION & THIRD-PARTY SERVICE PROVIDER INTEGRATION**

8.1. **Third-Party Screening and Risk Rating Provider:**
MINT has engaged a third-party provider for sanctions screening, identity verification, risk rating and ongoing watch-list monitoring. MINT remains responsible for oversight of that provider, ensuring service-levels, accuracy, update frequency, audit trails, contractual obligations (including data protection/POPIA compliance) are met.

8.2. **System Alerts and Automated Controls:**
MINT's platform will incorporate business intelligence tools in transaction monitoring (volume alerts, velocity alerts, anomalous flows, high risk pairings) as part of the AML/CTF toolkit.

8.3. **Integration with Architecture and APIs:**
All API calls and platform functionalities shall have appropriate AML/CTF checks (e.g., new beneficiary creation, external transfers, account-level limits), and any suspicious action triggers an account lock/pending review.

8.4. **Data Protection & Privacy:**
Page 9While performing identity verification and monitoring, MINT must ensure compliance with the Protection of Personal Information Act, 2013 ("**POPIA**"), safeguarding client data, and fully documenting processing activities.

9. **TRAINING, AWARENESS AND CULTURE**

9.1. All relevant employees, directors, agents and service providers must receive AML/CTF training (at onboarding and periodically, at least annually) that covers: regulatory requirements (FIC Act, Guidance Notes), internal policies/procedures, typologies of ML/TF/PF, red-flags, internal reporting obligations, sanctions screening, exchange control considerations.

9.2. Compliance culture: Senior management and the board must actively foster a culture of compliance, integrity and zero tolerance for financial crime, ensuring the AML/CTF policy is clearly communicated, enforced and monitored.

9.3. Records of training: MINT must keep verifiable records of training attendance, content delivered and updates in policy or regulation.

10. **AUDIT, REVIEW AND REPORTING TO GOVERNANCE**

10.1. The Compliance Officer shall report to the board (or risk/audit committee) at least annually (and more frequently if material issues) on:

10.1.1. The status of MINT's RMCP;
10.1.2. Summary of customer risk profile, volume of onboarding, number of high-risk customers, number of EDD cases;
10.1.3. Key AML/CTF metrics (transaction volumes, external flows, blocked accounts, suspicious reports filed);
10.1.4. Findings from internal/external audits or reviews;

10.1.5. Proposed updates to policy/procedure.

10.2. Internal audit (or third-party) shall conduct periodic effectiveness reviews of the AML/CTF framework and recommend enhancements.

10.3. MINT shall update the AML/CTF policy (and supporting procedures) at least annually or sooner if there is a material change in law, business model, service offering, or risk assessment.

11. **SANCTIONS, VIOLATIONS AND ENFORCEMENT**

11.1. **Disciplinary Measures:**
Any employee, director, agent or contractor who fails to comply with this policy may be subject to disciplinary action (including termination) in line with MINT's broader human resources disciplinary procedures.

11.2. **Customer Sanctions:**
If a customer is found to be in breach of MINT's AML/CTF policy, or aligned with financial crime sanctions or flagged high risk, MINT has the right to restrict activities, freeze or block accounts, cease the business relationship and report to regulatory authorities.

11.3. **Regulatory Sanctions:**
Non-compliance with the FIC Act can result in administrative sanctions, fines (for example, up to R10 million for failing to register with the FIC) and reputational damage.

12. **DOCUMENTATION AND RECORD-KEEPING**

12.1. All documentation obtained for customer due-diligence (identity documents, proof of address, corporate registration, beneficial ownership charts, source of funds/wealth documentation) shall be retained in electronic or physical form in a retrievable manner.

12.2. Transaction records shall include sufficient detail for reconstruction of the transaction (date, amount, currency, parties, account details, business correspondence) and must be retained for at least five years from the conclusion of the relationship or transaction.

12.3. Record-keeping systems must permit timely retrieval and secure storage and will account for the destruction of records only in compliance with retention periods.

13. **SPECIAL CONSIDERATIONS FOR CRYPTO-ASSETS, EXTERNAL EXCHANGES & HIGH-RISK FLOWS**

Given that MINT's business includes crypto-asset transactions and externalisation to other exchanges, the policy should explicitly address the following:

13.1. Risk of crypto-asset-based laundering, anonymity features, cross-jurisdiction flows, conversion into fiat and vice-versa.

13.2. Enhanced due diligence on crypto-asset flows, especially where funds are sent to or received from external exchanges, peer-to-peer network interfaces or high-risk jurisdictions.

13.3. Monitoring of crypto-asset-to-fiat conversions, fiat-to-crypto on-boarding and external exchange transfers with stronger controls and higher thresholds for red-flags.

13.4. Beneficiary creation and external address whitelisting prior to transfers to external crypto addresses or exchanges, verification and risk-assessment of the beneficiary/exchange must occur.

13.5. Consideration of geo-location, device-fingerprinting and behavioural analytics to detect masquerading, layering or structuring via crypto channels.

14. **COMMUNICATION AND CUSTOMER DISCLOSURE**

14.1. At account opening, and on relevant transactions, MINT shall provide customers with clear disclosures regarding AML/CTF obligations, including that transactions may be monitored, reported, and that verification may be requested.

14.2. Customers shall be informed about their obligations to maintain and update their personal information, to respond to verification requests and the consequences of non-compliance (account restriction, termination, reporting).

14.3. With respect to South African resident customers, MINT shall notify users when their foreign investment allowance or exchange-control limit is impacted (e.g., "Your Single Discretionary Allowance has been used – go to your profile to view status"). As

you have included, MINT shall integrate such notification and provide user access to allowance-status information.

15. **POLICY REVIEW AND UPDATE**
This Policy shall be formally reviewed at least annually, or more frequently if:

15.1. There is a change in MINT's business model, product offering or risk profile;
15.2. There is a material regulatory change (including by the FIC or other supervisory body);
15.3. There is a significant control failure or a major suspicious-activity incident.
15.4. Any update must be approved by the board (or senior management) and communicated to all staff and relevant third-party providers.