AML & CFT COMPLIANCE POLICY

DOCUMENT REFERENCE	EFFECTIVE DATE	TARGET AUDIENCE	STATUS
POL-AML-2026-V1	**August 2026**	**Regulators & Payment Partners**	**Auditable / Active**

1. STATUTORY COMMITMENT & LEGAL STANDARD

WilteX Direct (Pty) Ltd maintains zero tolerance for money laundering, terrorist financing, proliferation financing, and financial crime. This Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) Policy complies with the *Financial Intelligence Centre Act (FICA) 38 of 2001*, the *Prevention of Organised Crime Act (POCA) 121 of 1998*, and South African banking partner compliance directives.

2. RISK-BASED CUSTOMER DUE DILIGENCE (CDD)

All platform actors undergo strict risk-based identity screening linked to transaction thresholds and activity profiles:

- **Individual & Corporate Verification:** Mandatory identity, registration, and banking validation prior to enabling transaction capabilities (as defined in our published KYC Policy).
- **Politically Exposed Persons (PEP) Screening:** Automated batch matching of platform users and company directors against global PEP and targeted financial sanctions watchlists.
- **Sanction Check Filters:** Immediate blocking of individuals or entities listed on UN, OFAC, or South African FIC sanctions registers.

3. TRANSACTION MONITORING & SUSPICIOUS ACTIVITY REPORTING

WilteX Direct's automated transaction monitoring engines analyze real-time platform payment velocity and routing patterns. Suspicious indicators include:

Red Flag Indicator	Operational Trigger	Compliance Action
Rapid Payout Velocity	Multiple high-value bookings cancelled immediately after payment to force refund dispatches.	Immediate payment freeze + AML investigation.
Structured Transactions (Structuring)	Splitting large freight invoices into micro-payments to evade monitoring thresholds.	System auto-flagging and aggregation audit.
Third-Party Bank Payout Attempts	Driver requesting payout settlement to a bank account not registered in their verified name.	Strict account lock and AVS verification.

Regulatory Reporting Obligation (FICA Sec 29): Any transaction or activity suspected of involving money laundering or terrorist financing will be reported directly to the South African Financial Intelligence Centre (FIC) via formal Suspicious Transaction Reports (STR) or Suspicious Activity Reports (SAR).

4. RECORD KEEPING & EMPLOYEE TRAINING

All KYC documentation, transaction metadata, driver logs, and payment audit trails are securely retained in encrypted storage for a statutory minimum period of **5 years** post-account termination. Compliance personnel receive annual mandatory training on AML/CFT regulatory updates.

Issued By:

WilteX Direct (Pty) Ltd

Anti-Money Laundering Compliance Officer
Email: aml-compliance@wiltexdirect.co.za

Regulatory Alignment:

Financial Intelligence Centre Act (FICA)

Johannesburg, South Africa