

RANVOL LTD.

Anti-Money Laundering Policy

Anti-money laundering, counter-terrorist financing and sanctions compliance

Version 1.0 · Effective from 30 September 2026 · Public summary of the Company's internal AML/CFT & KYC Policy

Ranvol Ltd. · International Business Company · Registration No. 2026-00670 · Ground Floor, The Sotheby Building, Rodney Village, Rodney Bay, Gros-Islet, Saint Lucia · www.ranvol.com

1. Our commitment

- 1.1 Ranvol Ltd. ("Ranvol", "we", "us") does not permit its trading platform, accounts or payment channels to be used for money laundering, terrorist financing, sanctions evasion, fraud or any other financial crime. We apply the measures described in this Policy to every client, every account and every transaction, regardless of size.
- 1.2 This document is a public summary of our internal Anti-Money Laundering, Counter-Terrorist Financing and Know-Your-Customer Policy, which is approved by our Board of Directors and binding on everyone who acts for the Company. The practical requirements for verifying your identity are set out in our separate KYC Policy.
- 1.3 This Policy forms part of the Contractual Documents listed in the Client Agreement. By opening an Account you agree to comply with it and to provide the information and documents it requires.

2. Legal framework

- 2.1 Ranvol is an International Business Company incorporated in Saint Lucia. We apply the standards of:
 - the Money Laundering (Prevention) Act, Cap. 12.20 of the Laws of Saint Lucia, and regulations made under it;
 - the Anti-Terrorism Act of Saint Lucia and the guidance of the Financial Intelligence Authority of Saint Lucia (the "FIA");
 - the Recommendations of the Financial Action Task Force ("FATF");
 - the sanctions regimes of the United Nations Security Council, the United States (OFAC), the European Union and the United Kingdom.
- 2.2 Ranvol is not licensed or supervised by a financial services regulator. This does not reduce our anti-money laundering obligations: we apply the full standard described here, and we are also bound by the anti-money laundering requirements of our banking, payment, technology and liquidity providers.

3. Compliance Officer

- 3.1 The Board has appointed a Compliance Officer and Money Laundering Reporting Officer who is responsible for implementing this Policy, approving higher-risk clients, reviewing unusual activity and reporting to the FIA. The Compliance Officer has authority to restrict any account, hold any transaction and refuse or end any client relationship. Contact: compliance@ranvol.com.

4. Risk-based approach

- 4.1 We assess the money-laundering and terrorist-financing risk of each client at onboarding and throughout the relationship, taking into account the client's country of residence and nationality, occupation and source of funds, expected activity, payment methods, the way the client came to us, and the results of screening. The depth of our checks and monitoring depends on that assessment. We do not disclose a client's risk rating.

5. Who we do not accept

We do not open or maintain accounts for:

- persons under 18 or without full legal capacity;
- citizens or residents of the United States of America, wherever they are located;
- persons originating from, resident in, domiciled in, incorporated in or operating within Iran, the Democratic People's Republic of Korea, Myanmar or the Russian Federation, or any territory subject to comprehensive international sanctions, including the Crimea, Donetsk, Luhansk, Kherson and Zaporizhzhia regions, subject only to the exception in section 5.2;
- persons designated on a sanctions list of the UN, US, EU or UK, and entities owned or controlled by them;
- shell banks, anonymous accounts, accounts in fictitious names, and accounts held on behalf of undisclosed third parties;
- legal entities whose beneficial owners cannot be identified and verified;
- persons who do not provide the information and documents we request.

5.1 "Originating from" a jurisdiction means holding its citizenship or being resident in it.

5.2 A citizen of Iran, Myanmar or the Russian Federation who does not live in, and does not operate from, any of the jurisdictions listed above may be accepted if they prove that they have lived permanently in another country for at least two continuous years immediately before applying. Acceptance is at our discretion, requires Compliance Officer approval, and is subject to enhanced due diligence. The exception does not apply to citizens of North Korea or to US persons. The documents required are listed in our KYC Policy.

5.3 Clients connected to jurisdictions on the FATF list of jurisdictions under increased monitoring, or subject to targeted sanctions programmes, are accepted only after enhanced due diligence.

6. Customer due diligence

6.1 Before you can deposit funds or trade on a live account, we identify you and verify your identity, residential address and other information as described in our KYC Policy. You may register and use a demo account before verification.

6.2 For corporate clients we verify the company, its directors, the persons authorised to operate the account, and every natural person who ultimately owns or controls 25% or more of it.

6.3 We carry out enhanced due diligence for higher-risk clients, including politically exposed persons, clients connected to higher-risk jurisdictions, clients using the exception in section 5.2, and clients whose deposits exceed certain levels or do not match their profile. Enhanced due diligence may include evidence of the source of the funds deposited and of the source of the client's overall wealth, additional documents, a video call, and Compliance Officer approval.

6.4 We do not rely on introducing brokers, affiliates or other third parties to verify clients on our behalf. Every client is verified by us.

- 6.5 We may ask for updated or additional information at any time, including when documents expire, when your circumstances change, or when your activity changes.

7. Sanctions and PEP screening

- 7.1 Every client, and every director and beneficial owner of a corporate client, is screened before acceptance and on an ongoing basis against the sanctions lists of the UN, OFAC, the EU and the UK, and against databases of politically exposed persons and adverse media.
- 7.2 Cryptocurrency deposits are screened using blockchain analytics. Deposits from addresses linked to sanctioned persons, mixers, darknet markets, ransomware, hacks or fraud may be held, rejected or reported, and are not credited to your account until reviewed.
- 7.3 Where we identify a sanctions match, we freeze the account and the funds and act as required by law.

8. Deposits and withdrawals

- 8.1 **Own-name funds only.** We accept deposits only from bank accounts, cards and cryptocurrency wallets held in your own name or proven to be owned and controlled by you. We do not accept cash or third-party payments. A payment from a third party is returned to its source and is not credited to your account.
- 8.2 **Return to source.** Withdrawals are paid to the account, card or wallet from which you deposited, in the same currency or asset, up to the amount deposited from that source. Profits above your deposits may be paid to another account or wallet verified as yours. We do not make payments to third parties.
- 8.3 Client funds are held separately from the Company's operating funds. They are not held on trust and are not covered by any compensation scheme, as explained in the Client Agreement and the Risk Disclosure Statement.

9. Monitoring and reporting

- 9.1 We monitor deposits, withdrawals and trading activity for consistency with what we know about each client. Examples of activity we review include deposits followed by withdrawals with little or no trading, deposits inconsistent with a client's declared income, multiple accounts sharing devices or payment sources, trading with no economic purpose, and requests to change withdrawal destinations.
- 9.2 Where activity cannot be explained, we may request information, apply enhanced due diligence, hold transactions, restrict or close the account, and report to the FIA. The law prohibits us from telling a client that a report has been made or is being considered, and we will not do so.
- 9.3 We cooperate with lawful requests from the FIA, law-enforcement authorities and courts, and with anti-money laundering enquiries from our service providers to the extent the law permits.

10. Restriction and closure of accounts

- 10.1 We may, without giving reasons where the law prevents us: refuse an application; refuse a deposit or withdrawal; hold funds while enquiries are completed or while we await the consent of an authority; restrict an account to closing positions only; or close an account. Where a relationship ends for anti-money laundering reasons, funds are returned only to their verified source, and only where the law allows.

11. Record keeping, training and review

- 11.1 We keep identification documents, account records, transaction records and related correspondence for at least seven years after the end of the relationship or the transaction, whichever is later.
- 11.2 Everyone acting for the Company who deals with clients, payments or trading receives anti-money laundering training on joining and at least annually.
- 11.3 The internal policy is reviewed at least annually and whenever the law, FATF guidance, our products or our providers change. The operation of the policy is reviewed each year by a person independent of the Compliance Officer function. This public Policy is updated when the internal policy changes.

12. Your personal data

- 12.1 Information collected under this Policy is processed to meet our legal obligations and is handled in accordance with our Privacy Policy. It is shared only with our verification, screening, payment, technology and liquidity providers, and with authorities and courts where the law requires.

13. Contact

- 13.1 Questions about this Policy: compliance@ranvol.com. Questions about verifying your account: support@ranvol.com.