INFINIFX NETWORK INC.

AML & SANCTIONS POLICY

Last updated: [27.Jan.2026]

Website: https://infinifx.io

This Anti-Money Laundering and Sanctions Policy (this **"Policy"**) describes the measures used by **INFINIFX NETWORK INC.** (Ontario Corporation Number **1001203825**), registered office at **1270 Central Parkway West, Unit 102, Mississauga, Ontario, L5C 4P4, Canada** (**"Infinifx"**, **"we"**, **"us"**, **"our"**) to help prevent, detect and respond to money laundering, terrorist financing, sanctions breaches and related financial crime risks in connection with our website, platform and services (the **"Services"**).

1. Definitions

In this Policy:

- **"AML/CTF"** means anti-money laundering and counter-terrorist financing.
- **"Business Day"** means a day other than Saturday, Sunday or a public holiday in Ontario, Canada.
- **"Customer"** means any applicant, customer or account holder (including business customers and their authorised users) using the Services.
- **"KYC/KYB"** means know-your-customer/know-your-business due diligence and verification.
- **"MLRO"** means the money laundering reporting officer or equivalent compliance officer role designated by Infinifx.
- **"PEP"** means a politically exposed person (including close associates and family members) as defined by applicable law and/or Infinifx risk procedures.
- **"Sanctions"** means applicable economic sanctions, restrictive measures, asset freezes and trade controls administered by competent authorities.
- **"Suspicious Activity"** includes activity that may be associated with money laundering, terrorist financing, fraud, sanctions evasion, proceeds of crime, or other unlawful conduct.

2. Purpose and scope

2.1 This Policy applies to:

(a) all Customers (including their beneficial owners, directors and authorised users);

(b) all Transactions and attempted Transactions processed through the Services; and

(c) Infinifx personnel, contractors and service providers involved in onboarding, customer support, payment operations, risk management and compliance.

2.2 This Policy is risk-based and is intended to support compliance with applicable AML/CTF and Sanctions requirements, including registration, screening, monitoring, reporting and recordkeeping obligations that apply to Infinifx based on the Services offered and jurisdictions served.

3. Governance and responsibilities

3.1 **Board/Director oversight.** Infinifx maintains oversight of AML/CTF and Sanctions compliance through senior management and the designated director(s).

3.2 **Compliance leadership.** Infinifx designates an **MLRO/Compliance Officer** responsible for:

(a) maintaining the compliance program and internal controls;

(b) overseeing KYC/KYB, sanctions screening and transaction monitoring;

(c) assessing and escalating Suspicious Activity;

(d) liaising with competent authorities, where required; and

(e) maintaining training and audit/testing processes.

Contact email: [info@infinifx.io]

Compliance postal address: INFINIFX NETWORK INC., 1270 Central Parkway West, Unit 102, Mississauga, Ontario, L5C 4P4, Canada

3.3 **Three lines of defence.** Infinifx applies a functional separation between: (i) customer-facing teams; (ii) compliance/risk; and (iii) independent review/testing (where appropriate for size and complexity).

4. Risk-based approach

4.1 Infinifx applies a risk-based approach that considers, among other things:

(a) customer type (individual vs. business), ownership/control structure, and beneficial owners;

(b) geography (Customer location, counterparties and payment corridors);

(c) products and features used (e.g., FX, transfers, wallet functionality);

(d) payment methods and funding sources; and

(e) transaction behaviour and velocity.

4.2 Infinifx maintains and periodically updates a documented risk assessment and calibrates controls (CDD/EDD, monitoring rules, limits, and review frequency) to the risk profile.

5. Customer due diligence (KYC/KYB)

5.1 **Minimum onboarding checks.** Before enabling Services, Infinifx may require and verify information such as:

(a) legal name, date of birth (for individuals), address and contact details;

(b) for businesses: incorporation/registration details, registered address, nature of business, operating address, directors/officers;

(c) beneficial ownership and control information (including UBOs);

(d) purpose and intended nature of the relationship;

(e) source of funds and/or source of wealth information, where appropriate; and

(f) any licences/registrations relevant to the Customer's activity.

5.2 **Verification methods.** Verification may be performed using documentary and/or non-documentary methods, including third-party identity verification providers, corporate registry checks, database checks and payment instrument verification.

5.3 **Ongoing KYC/KYB.** Infinifx may request refreshed information periodically and/or upon trigger events, including changes in ownership/control, business model, geographies, or unusual account activity.

5.4 **Failure to provide information.** If a Customer does not provide requested information within the timeframe specified by Infinifx, Infinifx may decline onboarding, restrict Services, suspend Transactions, or close the account/relationship.

6. Enhanced due diligence (EDD)

6.1 Infinifx may apply EDD measures for higher-risk Customers and scenarios, including where:

(a) the Customer or a beneficial owner is a PEP;

(b) the Customer operates in or transacts with higher-risk jurisdictions;

(c) there are complex ownership structures, nominee arrangements, trusts or opaque control;

(d) activity is inconsistent with stated business purpose;

(e) adverse media or derogatory information is identified; or

(f) higher-risk products, corridors or volumes are requested.

6.2 EDD measures may include: additional documentation, deeper source of funds/wealth review, senior approval, tighter limits, increased monitoring and periodic reviews.

7. Sanctions screening and controls

7.1 **Screening.** Infinifx screens (as appropriate to Services and risk) Customers, beneficial owners, directors, authorised users and relevant counterparties against sanctions and watchlists, including at onboarding and on an ongoing basis.

7.2 **Positive matches.** If screening identifies a potential or confirmed match, Infinifx may:

(a) delay onboarding or Transactions pending review;

(b) request additional information;

(c) block or freeze funds where required;

(d) suspend or terminate the relationship; and/or

(e) make notifications or reports to competent authorities where required.

7.3 **Restricted jurisdictions.** Infinifx may prohibit or restrict Services involving certain jurisdictions, persons, entities, currencies, corridors or transaction types as a matter of law and/or risk policy.

8. Transaction monitoring

8.1 Infinifx performs monitoring designed to detect unusual or suspicious patterns, which may include:

(a) rapid movement of funds, layering indicators, or circular transactions;

(b) transactions inconsistent with Customer's profile, stated purpose, or historical patterns;

(c) high-velocity activity, structuring, repeated small transactions, or unusual counterparties;

(d) mismatches between geolocation/device data and Customer information;

(e) repeated failed attempts, reversals, chargebacks, or suspicious refund behaviour; and

(f) transactions involving higher-risk jurisdictions or categories.

8.2 Infinifx may use automated and manual review processes and may apply thresholds, limits, velocity controls and holds.

9. Suspicious activity escalation and reporting

9.1 **Internal escalation.** Infinifx personnel must promptly escalate indicators of Suspicious Activity to compliance for assessment.

9.2 **External reporting.** Where required by applicable law, Infinifx will submit reports to competent authorities/financial intelligence units and respond to lawful information requests.

9.3 **No tipping off.** Infinifx may be restricted by law from informing a Customer that a report has been made or that an investigation is underway.

10. Recordkeeping

10.1 Infinifx maintains records of onboarding, verification, monitoring, investigations and Transactions in accordance with applicable law and internal retention schedules.

10.2 Records are retained for at least 5 years after account closure or the end of the relationship, or longer where required.

11. Training and awareness

Infinifx provides AML/CTF and Sanctions training to relevant personnel at onboarding and periodically thereafter, with role-specific refreshers where appropriate.

12. Third parties and outsourcing

Where Infinifx uses service providers for identity verification, sanctions screening, monitoring, payments or data hosting, Infinifx applies due diligence and contractual controls designed to support confidentiality, security, performance and compliance.

13. Enforcement, restrictions and outcomes

Infinifx may restrict, suspend or terminate Services (and/or hold or reject Transactions) where it reasonably believes this is necessary to:

(a) comply with applicable law or sanctions;

(b) manage fraud, AML/CTF or financial crime risk;

(c) protect Customers, Infinifx, counterparties or the financial system; or

(d) respond to requests/orders from authorities.

14. Changes to this Policy

We may update this Policy from time to time by posting an updated version on the Website. The “Last updated” date indicates when changes took effect.