AML AND KYC COMPLIANCE POLICY
of Luminora Solutions Corp.

Last Updated Date: 1 June 2026

Luminora Solutions Corp., a company incorporated under the laws of the Republic of Panama under registration number 155782746, with its registered office at Torre Global Bank, 18th Floor, Office 1801, Calle 50, Panama City 0830, Republic of Panama (the ***"Company"***, ***"Luminora"***, ***"we"***, or ***"us"***), has adopted this AML and KYC Compliance Policy (the "***Policy***") as part of its internal compliance framework.

This Policy has been prepared with reference to the anti-money laundering and counter-terrorist financing laws and regulations of the Republic of Panama, including Law No. 23 of 27 April 2015, as amended by Law No. 254 of 11 November 2021 and as further regulated by Executive Decree No. 35 of 6 September 2022, and Law No. 129 of 17 March 2020, as well as relevant standards and guidance issued by the **Financial Action Task Force** (FATF), in each case to the extent relevant to the Company's business activities.

The Company maintains compliance controls designed to identify, assess, and mitigate risks related to anti-money laundering ("***AML***") and counter-terrorist financing ("***CTF***"). These controls apply to any person using or seeking to use the Company's services, including each customer or counterparty of the Company (each, a "***Customer***").

This Policy is intended to support the Company's lawful operations, protect the business from misuse, and establish a clear framework for customer due diligence, transaction monitoring, sanctions screening, escalation procedures, recordkeeping, and internal oversight. Any questions regarding this Policy may be directed to info@lumi-nora.com.

1. APPLICATION, PURPOSE AND CORE PRINCIPLES

1.1. This Policy applies to the Company's compliance operations relating to customer onboarding checks, transaction review, sanctions screening, internal reporting, document retention, and staff awareness measures.

1.2. The Company applies a control model in which **"Know Your Transaction"** (***"KYT"***) review is performed first. ***"Know Your Customer"*** (***"KYC"***) verification is applied on a triggered, risk-based, or discretionary basis where transaction behaviour, customer characteristics, sanctions exposure, regulatory considerations, or other relevant indicators justify additional scrutiny.

1.3. Nothing in this Policy requires the Company to proceed with any transaction, service, or customer relationship where the Company identifies compliance concerns, incomplete information, inconsistent data, or elevated AML/CTF or sanctions-related risks.

1.4. This Policy is intended to be read together with the Company's ***"Privacy Policy"***. Customer information obtained or processed under this Policy will be handled subject to the Privacy Policy and applicable legal requirements, including Law No. 81 of 26 March 2019 of the Republic of Panama on personal data protection and its regulations.

2. GOVERNANCE, ACCOUNTABILITY AND REGULATORY INTERFACE

2.1. The Company designates a ***"Compliance Officer"*** to oversee the practical implementation, maintenance, and enforcement of this Policy. For the purposes of this Policy**,** "**Compliance Officer**" means the person or persons designated internally by the Company to oversee AML/CTF compliance controls.

2.2. The Compliance Officer is responsible for directing and supervising the Company's AML/CTF control environment. This includes oversight of customer identification measures, transaction review procedures, internal policy updates, case handling, document retention arrangements, and periodic risk assessment activity.

2.3. The Compliance Officer also acts as the principal internal point of coordination for compliance escalations and, where appropriate, communications with competent authorities, including the **Unidad de Análisis Financiero** (UAF Panamá), the Ministerio Público of the Republic of Panama, and other relevant regulatory, supervisory, or law enforcement bodies.

2.4. The Compliance Officer may coordinate the provision of information to law enforcement or other competent bodies where disclosure is required under the regulatory framework applicable to the Company.

2.5. Personal and transaction-related information processed by the Company in connection with the application of this Policy may be obtained from one or more of the following sources:

(i) directly from the Customer in connection with an exchange request;

(ii) from partner aggregator services that route exchange requests to the Company, pursuant to the contractual arrangements between the Company and such partners; and

(iii) from third-party analytics, identity-verification, and sanctions-screening providers retained by the Company.

Receipt and processing of such information is subject to the Company's ***"Privacy Policy"***.

2.6. The Compliance Officer may be contacted at info@lumi-nora.com.

3. RISK FRAMEWORK AND CATEGORISATION

3.1. The Company applies a ***"Risk-Based Approach"*** (***"RBA"***) to allocate its compliance resources proportionately and to focus enhanced scrutiny on matters presenting greater exposure. This framework is informed by **Article 40** of Law No. 23 of 27 April 2015 of the Republic of Panama.

3.2. In evaluating risk, the Company may consider a combination of factors, including customer profile, geographic nexus, transaction pattern, product or service type, delivery channel, asset type, use of third-party onboarding inputs, and technological developments relevant to the detection of **AML/CTF** risks.

3.3. Indicators of lower risk may include stable and predictable activity, smaller-value transactions, and customers associated with jurisdictions generally regarded as presenting lower AML/CTF exposure.

3.4. Indicators of moderate risk may include occasional larger-value transactions, use of products or services that require closer attention, or activity connected to jurisdictions with average or mixed AML/CTF control environments.

3.5. Indicators of elevated risk may include, among other things, **"Politically Exposed Persons"** (***"PEPs"***), sanctioned-country exposure, complex ownership structures, frequent high-value activity, the exchange of untraceable cryptocurrencies, involvement in higher-risk sectors, or patterns inconsistent with the Customer's expected profile.

3.6. Where a Customer or transaction presents elevated risk, the Company may intensify monitoring, require additional information, seek management-level review, restrict service access, or apply Enhanced Due Diligence (**"*EDD*"**).

4. TRANSACTION SURVEILLANCE AND SCREENING CONTROLS

4.1. The Company monitors transactions and related data in order to detect anomalies, patterns requiring review, potential sanctions concerns, and other indicators of **AML/CTF** risks.

4.2. Monitoring activities may include data capture, filtering, case creation, document handling, review workflows, internal communications, blacklist or sanctions-list screening, and preparation of internal or statutory reports where appropriate.

4.3. The Company conducts pre-execution blockchain analytics screening of deposit transactions through a third-party analytics provider at the Company's pre-deposit infrastructure layer before onward execution. That KYT monitoring is primarily performed through AMLBot, or such other reputable provider as the Company may select from time to time.

4.4. The Company may conduct periodic or ongoing screening checks against recognised blacklists and sanctions sources, including **OFAC**, **UN**, **HMT**, and **EU lists**, and may aggregate transfer data across multiple identifiers in order to identify linked activity or suspicious patterns.

4.5. Where a transaction raises compliance concerns, the Company may, at its discretion, request further information or documents, place the Customer under review, deny service, suspend access to services, restrict associated transaction flow, or escalate the matter internally.

5. CUSTOMER ONBOARDING CHECKS AND TRIGGERED VERIFICATION

5.1. The Company uses ***"customer due diligence"*** (***"CDD"***) measures that reflect the principles set out in **Articles 26** to **28** of Law No. 23 of 27 April 2015 of the Republic of Panama. Where a case presents increased concern, the Company may apply ***"Enhanced Due Diligence"*** as contemplated under **Article 34** of Law No. 23 of 27 April 2015 of the Republic of Panama.

5.2. The Company does not apply KYC verification as a universal first-step requirement for every transaction. Instead, the Company follows a KYT-first, KYC-on-trigger model.

5.3. KYC triggers are illustrative rather than exhaustive. They may include:

(i) the classification of a transaction as medium or high risk under the Company's RBA framework;

(ii) use of cryptocurrencies with privacy-enhancing or anonymity-enhancing features (including privacy coins or similar virtual assets with enhanced privacy functionality);

(iii) transaction values or flows that are unusual in light of the Customer profile or partner aggregator flow; or

(iv) any other factor giving rise to reasonable grounds for additional verification.

5.4. Where KYC is triggered, identity verification services are performed through **KYCAID** (**operated by KYCAID Limited, UK, Company No. 11670407**), or such other reputable provider as the Company may select.

5.5. When verification is required, the Company may request information and documentation from the Customer, including:

FOR INDIVIDUALS

(i) national ID;

(ii) international passport;

(iii) bank statement or utility bill; and

(iv) source of funds information and any other documents reasonably requested by the Company.

FOR BUSINESS

(i) registry certificate and proof of legal existence;

(ii) identification of ultimate beneficial owners holding 25% or more of shares or otherwise exercising control, as understood under **Article 1** of Law No. 254 of 11 November 2021 amending **Article 4** of Law No. 23 of 2015, and under the framework established by Law No. 129 of 17 March 2020;

(iii) proof of business activity, such as a licence, operation permit, or equivalent document;

(iv) financial statements or source of funds evidence where appropriate; and

(v) tax identification number and fiscal residence details.

5.6. As part of identity assurance, the Company may assess whether the information received is coherent, sufficient to support a reasonable belief that the Customer's true identity is known, and supported by documentation that appears valid. The Company may also review whether the Customer or submitted materials indicate sanctions exposure.

5.7. The Company may contact the Customer for clarification, request updated materials, investigate discrepancies, or refuse to proceed where additional information is requested but not provided.

6. ENHANCED REVIEW MEASURES

6.1. ***"Enhanced Due Diligence"*** may be applied to Customers presenting elevated risk. This may include PEPs, customers connected to high-risk jurisdictions, customers associated with jurisdictions presenting elevated AML/CTF, sanctions, transparency, or tax-related risk, or cases involving other substantial risk indicators.

6.2. Enhanced Due Diligence measures may include one or more of the following:

(i) obtaining supplementary identification documentation;

(ii) reviewing source of wealth and source of funds through bank records, tax documentation, property records, or business financial statements;

(iii) carrying out adverse media checks;

(iv) requiring enhanced internal review or senior-level approval; and

(v) applying closer ongoing monitoring with more frequent transaction review and periodic refresh of customer information.

6.3. The Company may use any lawful and reasonable method to verify documents and information supplied by the Customer and may conduct further inquiry into any Customer or transaction the Company considers **higher-risk, anomalous, suspicious, or otherwise requiring additional review**.

7. TRAINING

7.1. The Company may provide AML/KYC training and compliance guidance to relevant team members at onboarding and on a recurring basis thereafter.

7.2. Personnel working in higher-risk functions receive role-specific and enhanced training aligned to their responsibilities.

7.3. Team members are regularly tested to ensure understanding and retention of training materials. Training programmes are continuously updated based on team feedback, regulatory changes, and industry best practices.

7.4. Comprehensive records of all training sessions, materials, and team participation are maintained and reviewed regularly.

8. STATUTORY REPORTING, SANCTIONS, AND CONFIDENTIALITY

8.1. ***Suspicious transaction reporting***. Where reasonable grounds for suspicion arise that any transaction may be related to money laundering, terrorist financing or the financing of the proliferation of weapons of mass destruction, the following framework applies:

(i) Internal escalation. The matter shall be escalated to the Compliance Officer within twenty-four (24) hours of detection;

(ii) Statutory reporting. The Company may submit a suspicious transaction report to the **Unidad de Análisis Financiero (UAF Panamá)** within the timeframes established by **Article 54** of Law No. 23 of 27 April 2015 of the Republic of Panama, which provides for a reporting period of fifteen (**15**) calendar days from detection; and

(iii) Voluntary internal target. As an internal standard **adopted by the Company for compliance and risk-management purposes**, the Company aims to submit such reports within seventy-two (**72**) hours of detection where operationally feasible.

8.2. Sanctions freezing. Where the Company identifies funds or other assets that **may be subject to restrictive measures under** United Nations Security Council resolutions or implementing instruments of the Republic of Panama, the Company may apply appropriate restrictive measures, including temporary transaction blocking, service restriction, or preventive freezing measures, established under **Articles 49** to **52** of Law No. 23 of 27 April 2015 and Executive Decree No. 587 of 4 August 2015, and shall report the matter without delay through the Compliance Officer.

8.3. Confidentiality. The internal handling of suspicious transaction reports, related investigations and freezing measures is subject to confidentiality and reserve in accordance with **Article 55** of Law No. 23 of 27 April 2015. Team members involved in the relevant processes are bound by these confidentiality obligations.

9. RESTRICTED JURISDICTIONS

9.1. Designated jurisdictions. The Company does not provide services to Customers from jurisdictions and territories designated in this Policy as ***"Restricted Jurisdictions"***. For the purposes of this Policy, Restricted Jurisdictions comprise: Afghanistan, Belarus, the Central African Republic, Crimea, Sevastopol and the Donetsk, Luhansk, Kherson and Zaporizhzhia regions of Ukraine, Cuba, the Democratic Republic of the Congo, Eritrea, Guinea-Bissau, Iran, Iraq, Lebanon, Libya, Mali, Myanmar, North Korea, the Republic of Panama, the Russian Federation, Somalia, South Sudan, Sudan, Syria, the United Kingdom, the United States of America, the member states of the European Union, Venezuela, and Yemen.

9.2. Additional restrictions. Restricted Jurisdictions also include any other country or territory subject to comprehensive sanctions imposed by the United Nations Security Council, the Office of Foreign Assets Control of the United States Department of the Treasury, the European Union, or His Majesty's Treasury of the United Kingdom, or designated by the **FATF** as a jurisdiction subject to a call for action, increased monitoring, or other enhanced countermeasure recommendations.

10. RECORDS, RETENTION AND INTERNAL AUDIT

10.1. Retention period. The Company maintains records relating to AML/KYC compliance activities for a period of five (**5**) **years**. This includes customer identification materials, due diligence records, monitoring outputs, case documentation, and records of suspicious activity reporting. The five-year retention period is aligned with **Article 29** of Law No. 23 of 27 April 2015 of the Republic of Panama and **Article 60** of the Tax Code of the Republic of Panama.

10.2. STR records. The Company maintains records of STRs filed with competent authorities, together with the basis for filing and supporting materials, where applicable. The Company may prepare periodic compliance reports for authorities where required by law or considered appropriate by the Company's compliance function.

10.3. Internal audits. The Company conducts internal audits or periodic reviews of its AML/KYC framework at intervals it considers appropriate, taking into account risk exposure and regulatory expectations. Areas presenting higher risk may be reviewed more frequently. Audit activity may include review of customer files, transaction surveillance tools, onboarding checks, escalation procedures, staff preparedness, and the practical functioning of the Company's RBA controls.

10.4. Process reviews. The Company reviews its record management and compliance control arrangements on a regular basis and updates them where necessary to preserve effectiveness and consistency with legal or operational developments.

11. POLICY ADMINISTRATION AND RESERVATIONS

11.1. This Policy forms part of the Company's internal compliance arrangements and may be reviewed, supplemented, or updated from time to time to reflect changes in the Company's operations, compliance practices, provider arrangements, or the legal, regulatory, or compliance environment relevant to the Company's activities.

11.2. The Company may, at its discretion, request additional information, decline to process a transaction, suspend or terminate access to services, or maintain restrictions where this is considered appropriate in light of the Company's AML, CTF, sanctions, or related compliance policies, risk-management considerations, or legal requirements.

11.3. This Policy supports the Company's internal risk management processes. It does not limit any right of the Company to take stricter action in a specific case where the facts, the applicable legal framework, or competent authority guidance reasonably support such action.

* * *