NEXORA FINTECH LTD.

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

Effective Date: 01 July 2026
Version: 1.0
Approved by: Compliance Officer
Policy Owner: NEXORA FINTECH LTD. Compliance Function

---

1. GENERAL INFORMATION

The Anti-Money Laundering and Counter-Terrorist Financing Policy (the **"Policy"**) establishes the principles, standards and control framework adopted by **NEXORA FINTECH LTD.** (the **"Company"** or **"Nexora"**) to prevent, identify, assess, mitigate and report risks related to money laundering, terrorist financing and other forms of financial crime.

Nexora is committed to maintaining an effective and risk-based financial crime compliance framework proportionate to the nature, scale and complexity of its business activities, customers, products, services and geographic exposure.

The Company seeks to prevent its services, infrastructure, business relationships and distribution channels from being misused for:

- money laundering;
- terrorist financing;
- proliferation financing;
- sanctions evasion;
- fraud and other financial crimes;
- corruption and bribery;
- proceeds of criminal activity;
- human trafficking and modern slavery;
- drug trafficking;
- proliferation of weapons of mass destruction;
- illegal or unlicensed financial activities; and
- other unlawful activities.

For the purposes of this Policy, **Money Laundering ("ML")** means the process by which criminals seek to conceal, disguise, transfer, convert or otherwise use proceeds derived from criminal activity in order to make such proceeds appear legitimate.

Terrorist Financing ("TF") means the provision, collection, movement or use of funds or other assets, directly or indirectly, with the intention or knowledge that they may be used to finance terrorism or terrorist activities.

The Company applies a **Risk-Based Approach ("RBA")** to AML/CTF compliance. The level and intensity of controls applied to a customer, transaction, product or business relationship depend on the level of risk identified.

This Policy does not constitute a complete description of all AML/CTF policies, procedures and control measures implemented by the Company. Detailed operational requirements may be established through separate internal procedures, manuals, risk assessments and compliance instructions.

---

2. PURPOSE AND SCOPE

The purpose of this Policy is to establish the Company's framework for:

- preventing money laundering and terrorist financing;
- identifying and mitigating financial crime risks;
- conducting customer due diligence;
- identifying beneficial owners;
- assessing customer and geographic risk;
- identifying PEPs and sanctions exposure;
- monitoring customer and transaction activity;
- identifying and escalating suspicious activity;
- maintaining appropriate records;
- cooperating with competent authorities; and
- maintaining an effective financial crime compliance culture.

This Policy applies to:

- the Company;
- its directors and officers;
- employees;
- contractors, where relevant;
- business partners and counterparties, to the extent applicable;
- relevant outsourced service providers; and
- activities conducted through the Company's products, services and technology infrastructure.

The Policy applies proportionately according to the nature and level of risk associated with the relevant activity.

---

3. REGULATORY AND COMPLIANCE FRAMEWORK

Nexora maintains its AML/CTF framework with reference to applicable laws and internationally recognised standards in the jurisdictions in which it operates or provides services.

The Company's AML/CTF framework is informed, where applicable, by:

- applicable national AML/CFT legislation;
- applicable sanctions and financial crime legislation;
- Financial Action Task Force (**FATF**) Recommendations;
- applicable European Union AML/CFT requirements;
- applicable EU sanctions and restrictive measures;
- applicable United Nations sanctions;
- applicable requirements relating to beneficial ownership and customer identification;
- applicable requirements concerning transfers of funds and, where relevant, crypto-assets;
- applicable regulatory guidance issued by competent authorities;
- relevant European Banking Authority (**EBA**) guidelines and regulatory expectations; and
- other applicable international financial crime prevention standards.

Where mandatory local requirements impose a higher standard than this Policy, the Company shall apply the applicable mandatory requirement.

The Company periodically reviews its regulatory framework to ensure that material legislative and regulatory changes are reflected in its internal AML/CTF procedures.

---

4. COMPANY'S AML/CTF RESPONSIBILITIES

Nexora is responsible for establishing and maintaining the Company's AML/CTF control framework.

The Company's responsibilities include:

4.1 Customer Due Diligence

The Company shall:

- identify and verify customers;
- identify and verify Ultimate Beneficial Owners (“UBOs”);
- understand the purpose and intended nature of the business relationship;
- assess customer risk;
- identify Politically Exposed Persons (“PEPs”);
- conduct sanctions screening;
- assess adverse media and reputational risks where appropriate;
- establish and verify the source of funds (“SoF”) and source of wealth (“SoW”) where required; and
- apply Enhanced Due Diligence (“EDD”) where elevated risk is identified.

4.2 Risk-Based Approach

Customers, transactions and business relationships are assessed according to relevant risk factors, including:

- customer risk;
- geographic risk;
- product and service risk;
- transaction risk;
- delivery channel risk;
- industry risk;
- ownership and control structure;
- sanctions exposure;
- PEP exposure;
- adverse media;
- source of funds and source of wealth; and
- other relevant financial crime indicators.

4.3 Monitoring

The Company maintains appropriate systems and procedures for:

- ongoing customer monitoring;
- transaction monitoring;
- sanctions screening;
- behavioural analysis;
- detection of unusual or suspicious activity;
- escalation of potential AML/CTF concerns; and
- investigation and disposition of alerts.

4.4 Record Keeping

The Company maintains appropriate records relating to:

- customer identification;
- verification;
- risk assessments;
- transaction activity;
- monitoring and screening;
- investigations;
- suspicious activity;
- decisions and approvals;
- compliance reviews; and
- relevant correspondence with competent authorities.

Records are retained for the period required by applicable law and internal retention requirements.

---

5. ROLE OF TECHNOLOGY PROVIDERS

Nexora may use third-party technology and software providers to support its operational and compliance infrastructure.

PayPilot / Pilot Innovation acts solely as a **technology and software provider**.

PayPilot may provide technical infrastructure, software functionality, APIs, interfaces, workflow tools, data processing capabilities or other technology services used by Nexora.

PayPilot does not act as Nexora's AML/CTF compliance function and does not assume Nexora's legal, regulatory or compliance responsibilities.

The use of a technology provider does not transfer Nexora's AML/CTF responsibilities to that provider.

Nexora remains responsible for:

- determining its AML/CTF requirements;
- approving its AML/CTF policies and procedures;
- customer acceptance decisions;
- customer risk classification;
- EDD decisions;
- sanctions and PEP escalation decisions;
- suspicious activity assessment;
- regulatory reporting where applicable; and
- maintaining appropriate oversight of outsourced or technology-supported processes.

Where technology is used for automated screening or monitoring, Nexora maintains appropriate human oversight and escalation procedures.

6. CUSTOMER DUE DILIGENCE

Customer Due Diligence (**CDD**) is a fundamental component of the Company's AML/CTF framework.

The Company conducts CDD:

- before establishing a business relationship;
- before performing relevant transactions where required;
- when there are doubts regarding previously obtained identification information;
- where customer circumstances materially change;
- where unusual or suspicious activity is detected; and
- at other intervals determined by the customer's risk level.

CDD may include:

1. identification of the customer;
2. verification of the customer's identity;
3. identification and verification of UBOs;
4. identification of directors and authorised representatives;
5. understanding the customer's business;
6. determining the purpose and intended nature of the relationship;
7. assessing geographic exposure;
8. identifying PEP status;
9. sanctions screening;
10. adverse media screening;
11. assessment of source of funds;
12. assessment of source of wealth where required; and
13. ongoing monitoring.

7. STANDARD DUE DILIGENCE

Standard Due Diligence (**SDD**) may be applied to customers presenting a standard or lower level of AML/CTF risk, where permitted by applicable law.

7.1 Individuals

Depending on the risk profile, the Company may request:

- valid passport or national identity card;
- proof of residential address;

- date of birth;
- nationality;
- tax or identification number where applicable;
- contact information;
- biometric or liveness verification for remote onboarding;
- information concerning the purpose of the relationship; and
- other information reasonably required for verification.

7.2 Corporate Customers

For legal entities, the Company may request:

- certificate of incorporation or equivalent;
- constitutional documents;
- company registration extract or equivalent;
- registered office information;
- directors and authorised representatives;
- UBO information;
- ownership structure;
- identification documents of relevant individuals;
- description of business activities;
- website and business presence;
- expected transaction volumes;
- expected countries and counterparties;
- source of funds;
- source of wealth where appropriate;
- relevant licences or registrations; and
- supporting commercial documentation where required.

The Company may use publicly available and reliable sources to independently verify information rather than requesting documents that can reasonably be obtained from authoritative public registers.

---

8. ENHANCED DUE DILIGENCE

Enhanced Due Diligence (**EDD**) is applied where the customer, transaction, jurisdiction, product or other circumstances present elevated AML/CTF risk.

EDD may be triggered by:

- PEP status;
- high-risk jurisdiction exposure;
- sanctions concerns;
- complex or opaque ownership structures;

- unusual transaction activity;
- significant transaction volumes;
- high-risk industries;
- negative or adverse media;
- unexplained source of funds or wealth;
- use of high-risk financial instruments;
- significant exposure to virtual assets or crypto-assets where relevant;
- inconsistent business information;
- unexplained cross-border activity;
- use of nominee structures;
- unexplained third-party payments; or
- other relevant risk indicators.

EDD may include:

- obtaining additional identification documents;
- obtaining corporate and ownership documentation;
- obtaining additional information concerning the business model;
- verification of source of funds;
- verification of source of wealth;
- obtaining bank statements or equivalent financial records;
- obtaining contracts, invoices or other commercial evidence;
- enhanced adverse media screening;
- enhanced sanctions screening;
- senior management or Compliance approval;
- increased transaction monitoring;
- more frequent customer reviews; and
- other measures proportionate to the identified risk.

---

9. SOURCE OF FUNDS AND SOURCE OF WEALTH

The Company may request evidence to establish the legitimacy of funds or wealth where required by the customer's risk profile.

Potential evidence may include:

- bank statements;
- audited financial statements;
- employment or salary documentation;
- tax documentation;
- investment statements;
- loan documentation;
- sale and purchase agreements;

- inheritance documentation;
- business contracts;
- invoices;
- evidence of business revenues;
- evidence of asset sales; and
- other reliable supporting documentation.

The Company may use a combination of documentary evidence and independent verification.

The type and amount of evidence required will depend on the customer's risk profile, transaction size, business model and circumstances.

---

10. POLITICALLY EXPOSED PERSONS

The Company identifies customers and UBOs who are:

- Politically Exposed Persons (“PEPs”);
- family members of PEPs; or
- known close associates of PEPs.

PEP status does not automatically mean that a customer must be rejected.

However, where a customer is identified as a PEP, the Company applies appropriate EDD measures and obtains the required internal approval before or during the establishment of the relationship, as applicable.

PEP screening may cover domestic PEPs, foreign PEPs and individuals holding prominent positions in international organisations.

Examples include:

- heads of state or government;
- ministers and deputy ministers;
- senior government officials;
- members of national parliaments;
- senior judicial officials;
- senior military officials;
- ambassadors;
- senior executives of state-owned enterprises;
- senior officials of political parties;
- senior officials of international organisations; and
- other persons falling within the applicable legal definition of a PEP.

Family members and close associates are assessed in accordance with applicable AML requirements.

11. SANCTIONS SCREENING

The Company conducts sanctions screening of relevant customers, UBOs, directors, authorised representatives, counterparties and, where appropriate, transactions.

Screening may include relevant:

- United Nations sanctions lists;
- European Union sanctions lists;
- applicable national sanctions lists;
- UK sanctions lists where applicable;
- US sanctions lists where legally and operationally relevant; and
- other applicable sanctions or restrictive-measures databases.

Where a potential sanctions match is identified, the relevant relationship or transaction may be suspended or escalated until the alert has been reviewed and appropriately resolved.

The Company does not knowingly provide services where doing so would violate applicable sanctions or restrictive measures.

---

12. ONGOING MONITORING

The Company applies ongoing monitoring throughout the customer relationship.

Monitoring may include:

- review of transaction patterns;
- assessment of transaction frequency and value;
- identification of unusual transaction behaviour;
- review of geographic exposure;
- monitoring of changes in business activity;
- sanctions screening;
- PEP screening;
- adverse media screening;
- review of changes in ownership or management;
- review of source of funds where appropriate; and
- periodic refresh of customer information.

The frequency and depth of monitoring are determined by the customer's risk classification.

---

13. SUSPICIOUS ACTIVITY

The Company maintains procedures for identifying, escalating, investigating and documenting potentially suspicious activity.

Potential indicators may include:

- transactions inconsistent with the customer's stated business;
- unexplained rapid movement of funds;
- unusual third-party payments;
- transactions involving high-risk jurisdictions without an apparent business rationale;
- unexplained use of multiple accounts or payment instruments;
- attempts to avoid identification or verification requirements;
- inconsistent customer information;
- unexplained changes in transaction patterns;
- transactions involving sanctioned persons or jurisdictions;
- activity potentially associated with fraud or financial crime;
- unexplained crypto-asset exposure;
- use of complex structures without a legitimate economic rationale; and
- other behaviour inconsistent with the customer's known profile.

Where suspicious activity is identified, the matter is escalated to the appropriate Compliance/AML function for investigation.

Where legally required, the Company will submit reports or notifications to the relevant competent authority or Financial Intelligence Unit.

The Company does not disclose the existence or submission of a suspicious activity report where such disclosure is prohibited by applicable law.

---

14. RISK ASSESSMENT

The Company maintains an institution-wide AML/CTF risk assessment and updates it periodically and when material changes occur.

The risk assessment considers at least:

14.1 Customer Risk

- individual versus corporate customer;
- ownership structure;
- PEP status;
- sanctions exposure;
- adverse media;

- customer location;
- business activity;
- regulatory status; and
- customer profile.

14.2 Geographic Risk

- country of incorporation;
- residence;
- operating locations;
- customer base;
- counterparties;
- source and destination of funds;
- sanctions exposure; and
- FATF or other competent authority risk classifications.

14.3 Product and Service Risk

- payment services;
- account-related services;
- card-related services;
- cross-border transactions;
- digital financial services;
- virtual asset or crypto-related activity where applicable;
- technology-enabled financial services; and
- other products offered or supported by the Company.

14.4 Transaction Risk

- value;
- frequency;
- velocity;
- complexity;
- geographic routing;
- counterparties;
- unusual behaviour; and
- consistency with the customer's expected activity.

---

15. CUSTOMER RISK CLASSIFICATION

Customers may be classified as:

- **Low Risk**

- **Medium Risk**
- **High Risk**
- **Prohibited / Unacceptable Risk**

The risk classification determines the level of CDD, monitoring and review required.

High-risk customers may only be accepted where the Company determines that the identified risks can be effectively mitigated and the relationship falls within the Company's risk appetite.

The Company reserves the right to reject or terminate a relationship where the identified risk cannot be adequately mitigated.

---

16. PROHIBITED AND UNACCEPTABLE CUSTOMERS

The Company does not knowingly establish or maintain relationships with persons or entities that:

- refuse to provide required information;
- provide false, misleading or materially inconsistent information;
- cannot satisfactorily establish their identity or ownership;
- are subject to applicable sanctions prohibiting the relationship;
- are involved in money laundering or terrorist financing;
- are involved in organised criminal activity;
- are involved in human trafficking or modern slavery;
- are involved in the production or trafficking of illegal drugs;
- operate as shell banks;
- conduct unlicensed financial services where licensing is required;
- engage in fraud or other serious financial crime;
- use structures designed to conceal beneficial ownership;
- present an unacceptable sanctions risk;
- are involved in prohibited weapons activities;
- are involved in child sexual exploitation or illegal exploitative content;
- are involved in counterfeit or serious intellectual property infringement;
- operate Ponzi or pyramid schemes;
- operate unregulated investment schemes;
- conduct illegal gambling or unlicensed betting activities;
- use anonymous ownership structures that cannot be satisfactorily verified; or
- otherwise fall outside the Company's risk appetite.

The Company may also restrict specific products, services, transaction types or jurisdictions where the associated risk cannot be adequately controlled.

17. HIGH-RISK JURISDICTIONS

The Company applies enhanced controls to customers and counterparties connected with jurisdictions identified as high risk by:

- FATF;
- the European Commission;
- the United Nations;
- applicable national competent authorities; or
- other recognised regulatory or governmental bodies.

The Company does not rely exclusively on a static country list.

Country risk is reviewed periodically and updated when relevant international sanctions, FATF statements, EU measures or other authoritative classifications change.

Customers from high-risk jurisdictions may only be accepted following appropriate EDD and approval in accordance with the Company's internal procedures.

---

18. PROHIBITED JURISDICTIONS

The Company may maintain a list of prohibited jurisdictions based on:

- applicable sanctions;
- regulatory restrictions;
- AML/CTF risk;
- terrorism financing risk;
- geopolitical considerations;
- inability to perform adequate CDD;
- legal restrictions;
- inability to provide services lawfully; or
- the Company's internal risk appetite.

The current prohibited-jurisdiction list is maintained separately and is reviewed periodically.

The Company may refuse customers or transactions connected with prohibited jurisdictions even where no statutory prohibition applies, where the associated risk exceeds the Company's risk appetite.

---

19. HIGH-RISK BUSINESS ACTIVITIES

Depending on the circumstances and applicable risk appetite, enhanced controls may apply to customers operating in sectors such as:

- virtual assets and crypto-assets;
- gambling and betting;
- adult entertainment;
- high-risk financial services;
- foreign exchange;
- money transmission;
- investment services;
- unregulated financial activities;
- online marketplaces;
- high-value goods;
- precious metals and stones;
- weapons and defence-related industries;
- pharmaceuticals;
- industries involving significant cash flows; and
- other sectors identified as presenting elevated AML/CTF risk.

A high-risk industry does not automatically result in rejection. The Company assesses whether the risk can be appropriately mitigated.

---

20. VIRTUAL ASSETS AND CRYPTO-ASSET ACTIVITIES

Where customers or transactions involve virtual assets or crypto-assets, the Company applies additional risk-based controls where appropriate.

Such controls may include:

- verification of the customer's regulatory status;
- assessment of the business model;
- wallet screening;
- blockchain analytics;
- assessment of transaction history;
- source of crypto-assets;
- destination wallet assessment;
- sanctions screening;
- identification of exposure to darknet markets, ransomware, scams or illicit services;
- identification of exposure to mixers or tumblers where relevant;
- assessment of anonymity-enhanced technologies; and

- enhanced transaction monitoring.

The Company may reject or restrict transactions where the source or destination of funds presents unacceptable financial crime risk.

---

21. USE OF TECHNOLOGY

Nexora may use automated and technology-supported systems to assist with AML/CTF controls.

Such systems may include:

- automated customer screening;
- sanctions screening;
- PEP screening;
- adverse media screening;
- transaction monitoring;
- behavioural analysis;
- blockchain analytics;
- risk scoring;
- identity verification;
- document verification;
- fraud detection; and
- case management systems.

Technology is used to support, rather than replace, appropriate compliance oversight.

Where automated systems generate alerts or risk indicators, appropriate human review and escalation procedures shall be maintained.

The Company remains responsible for the final compliance decisions required under its internal policies and applicable law.

---

22. COMPLIANCE OFFICER / AML OFFICER

Nexora shall designate an appropriately qualified **Compliance Officer / AML Officer** responsible for AML/CTF oversight, where required by applicable law and the Company's regulatory framework.

The Compliance Officer may be responsible for:

- maintaining the AML/CTF framework;
- overseeing KYC/CDD procedures;
- supervising transaction monitoring;
- reviewing suspicious activity;
- coordinating regulatory reporting;
- maintaining AML/CTF records;
- conducting risk assessments;
- overseeing sanctions and PEP controls;
- providing compliance advice to management;
- coordinating AML/CTF training;
- monitoring regulatory developments;
- supporting regulatory inspections and information requests; and
- reporting material AML/CTF matters to senior management.

The Compliance Officer shall have appropriate independence, authority and access to relevant information necessary to perform the role effectively.

---

23. EMPLOYEE TRAINING

Employees and relevant contractors receive AML/CTF training appropriate to their responsibilities.

Training may cover:

- AML/CTF principles;
- customer identification;
- KYC/CDD;
- EDD;
- sanctions;
- PEPs;
- transaction monitoring;
- suspicious activity indicators;
- escalation procedures;
- fraud risks;
- data protection requirements; and
- changes in applicable laws and internal procedures.

Training is conducted periodically and whenever material changes to the Company's AML/CTF framework occur.

---

24. OUTSOURCING AND THIRD-PARTY SERVICE PROVIDERS

The Company may use third-party providers to support AML/CTF and operational processes.

Before engaging relevant providers, the Company may conduct appropriate due diligence covering:

- corporate existence;
- ownership and management;
- regulatory status;
- reputation;
- information security;
- AML/CTF framework where relevant;
- sanctions exposure;
- service scope;
- data protection;
- subcontracting arrangements; and
- operational resilience.

Outsourcing or use of technology does not remove the Company's responsibility for appropriate oversight.

The Company maintains appropriate contractual, operational and monitoring controls over material outsourced activities.

---

25. MANAGEMENT INFORMATION AND INTERNAL OVERSIGHT

Management receives appropriate information concerning the Company's AML/CTF framework and risk exposure.

Depending on the Company's size, activities and regulatory obligations, management information may include:

- AML/CTF risk assessment results;
- customer risk classification;
- high-risk customers;
- EDD cases;
- sanctions alerts;
- PEP cases;

- suspicious activity investigations;
- rejected or terminated relationships;
- transaction monitoring alerts;
- regulatory requests;
- material compliance breaches;
- remediation activities;
- training completion;
- internal review findings;
- outsourced AML/CTF activities;
- changes in applicable legislation; and
- recommendations for improving the AML/CTF framework.

Material AML/CTF issues are escalated to senior management in a timely manner.

---

26. INTERNAL CONTROLS AND REVIEW

The Company periodically assesses the effectiveness of its AML/CTF framework.

Reviews may consider:

- adequacy of customer due diligence;
- effectiveness of transaction monitoring;
- sanctions screening performance;
- PEP screening;
- risk classification;
- effectiveness of EDD;
- quality of suspicious activity investigations;
- record keeping;
- employee training;
- third-party providers;
- regulatory changes; and
- identified deficiencies.

Where weaknesses are identified, appropriate corrective actions shall be implemented and monitored.

---

27. RECORD KEEPING

The Company maintains adequate records to demonstrate compliance with applicable AML/CTF requirements.

Records may include:

- customer identification information;
- verification evidence;
- UBO information;
- risk assessments;
- transaction records;
- monitoring results;
- screening results;
- investigation records;
- EDD documentation;
- source of funds and wealth evidence;
- internal approvals;
- suspicious activity documentation;
- regulatory correspondence; and
- training records.

Records are retained for the period required by applicable law and internal record-retention procedures.

---

28. REFUSAL, SUSPENSION AND TERMINATION

The Company reserves the right to:

- refuse onboarding;
- delay or suspend a transaction;
- restrict access to services;
- request additional information;
- apply EDD;
- terminate a business relationship; or
- take other appropriate measures

where the Company determines that AML/CTF, sanctions, fraud or other financial crime risks cannot be adequately mitigated.

The Company is not required to disclose internal AML/CTF controls, monitoring logic or suspicious activity investigation details where disclosure is prohibited or would compromise the effectiveness of the Company's controls.

---

29. COOPERATION WITH AUTHORITIES

Nexora cooperates with competent regulatory, law-enforcement, financial intelligence and other governmental authorities where required by applicable law.

The Company may provide information, records and documentation in response to valid legal or regulatory requests.

Such cooperation may include:

- customer information;
- transaction information;
- corporate documentation;
- identification records;
- suspicious activity information;
- compliance records; and
- other information required by law.

The Company shall ensure that information is disclosed only through appropriate and legally authorised channels.

---

30. CONFIDENTIALITY AND DATA PROTECTION

AML/CTF activities involve the processing of personal and corporate information.

The Company processes such information in accordance with applicable data protection and privacy laws.

Access to AML/CTF information is restricted to personnel and service providers with a legitimate business or legal need to access such information.

Confidential information relating to suspicious activity investigations and regulatory reporting shall be handled in accordance with applicable confidentiality and anti-tipping-off requirements.

---

31. POLICY REVIEW

This Policy shall be reviewed periodically and whenever material changes occur to:

- the Company's business model;
- products or services;
- customer base;

- geographic footprint;
- regulatory status;
- applicable legislation;
- AML/CTF risk exposure;
- sanctions environment; or
- relevant international standards.

The Company may amend this Policy whenever necessary to maintain an effective AML/CTF framework.

---

32. FINAL PROVISIONS

This Policy forms part of Nexora's overall financial crime compliance framework.

All employees, officers, contractors and relevant service providers involved in activities subject to this Policy are expected to comply with its requirements and applicable internal procedures.

Nothing in this Policy shall be interpreted as limiting any obligation imposed on the Company by applicable law, regulation, regulatory guidance, sanctions regime or competent authority.

Where a conflict exists between this Policy and mandatory applicable law, the mandatory legal requirement shall prevail.

ANNEX 1 — ACCEPTED IDENTIFICATION DOCUMENTS

1. Natural Persons

Depending on the customer's risk profile, the Company may accept:

- passport;
- national identity card;
- residence permit;
- other government-issued identification document recognised under applicable law.

Documents must generally be:

- valid;
- legible;

- authentic or reasonably verifiable;
- issued by a competent authority; and
- sufficient to establish the identity of the customer.

For remote onboarding, the Company may additionally require:

- liveness verification;
- biometric verification;
- video identification;
- document authenticity verification; or
- other appropriate electronic identification measures.

2. Legal Entities

The Company may accept:

- certificate of incorporation;
- certificate of registration;
- official company registry extract;
- articles of association;
- constitutional documents;
- shareholder or ownership information;
- director information;
- UBO information;
- proof of registered address;
- business licence, where applicable; and
- other reliable corporate documentation.

Where information can be independently verified through reliable public sources, the Company may use such sources instead of requesting duplicate documents from the customer.

3. Document Requirements

Documents must be sufficiently clear and complete to allow reasonable verification.

Documents issued in a language that cannot reasonably be reviewed by the Company may be accompanied by a translation where required.

The Company reserves the right to request additional documentation where the customer's risk profile or circumstances require Enhanced Due Diligence.

ANNEX 2 — PEP CATEGORIES

For AML/CTF purposes, the Company considers the following categories when identifying PEPs:

Heads of State and Government

- presidents;
- prime ministers;
- heads of government;
- ministers and equivalent senior officials.

Legislative and Political Officials

- members of national parliaments;
- senior officials of political parties;
- other persons holding prominent public functions.

Judicial and Law-Enforcement Officials

- senior judges;
- members of supreme or constitutional courts;
- senior prosecutors;
- other senior judicial or law-enforcement officials where covered by applicable law.

Central Banks and Public Financial Institutions

- senior officials of central banks;
- senior officials of state-owned financial institutions;
- other senior public financial officials.

Military and Diplomatic Officials

- senior military officers;
- ambassadors;
- senior diplomatic representatives.

State-Owned Enterprises

- senior management and board members of state-owned enterprises.

International Organisations

Senior officials of international organisations, including organisations such as:

- United Nations;

- World Bank;
- International Monetary Fund;
- NATO;
- OECD;
- European Union institutions; and
- other comparable international organisations.

Family Members

The Company considers, where applicable:

- spouses or equivalent partners;
- children and their spouses or equivalent partners; and
- parents.

Close Associates

Close associates may include persons known to:

- have joint beneficial ownership of legal entities or arrangements with a PEP;
- maintain close business relationships with a PEP; or
- own a legal entity or arrangement known to have been established for the benefit of a PEP.

PEP classification shall be determined in accordance with applicable law.

ANNEX 3 — RISK CATEGORIES

Low Risk

Generally characterised by:

- transparent ownership;
- regulated or well-established business;
- reputable jurisdiction;
- straightforward business model;
- transparent source of funds;
- no material adverse media;
- no sanctions concerns; and
- no material PEP exposure.

Standard Due Diligence may be appropriate where legally permitted.

Medium Risk

May include:

- moderate geographic exposure;
- more complex business structures;
- international activity;
- higher transaction volumes;
- moderate industry risk;
- limited adverse media concerns; or
- other circumstances requiring additional monitoring.

Enhanced monitoring or additional verification may be applied.

High Risk

May include:

- high-risk jurisdictions;
- PEP exposure;
- complex ownership;
- significant crypto exposure;
- high-risk industries;
- significant transaction volumes;
- unexplained source of funds or wealth;
- sanctions concerns requiring further investigation;
- material adverse media; or
- other significant AML/CTF risk factors.

EDD and appropriate approval are required.

Prohibited / Unacceptable Risk

Includes circumstances where:

- the customer cannot be satisfactorily identified;
- UBO cannot be established;
- sanctions prohibit the relationship;
- the customer is involved in serious criminal activity;
- the source of funds cannot be reasonably established where required;
- the relationship presents an unmanageable financial crime risk; or
- the relationship otherwise falls outside the Company's risk appetite.

Such customers shall be rejected or the relationship terminated, subject to applicable legal requirements.

ANNEX 4 — CONTACT

For AML/CTF and compliance-related matters:

NEXORA FINTECH LTD.
Compliance / AML Department
Email: compliance@nexorafintech.com
Registered Office: 128 City Road, London, United Kingdom, EC1V 2NX

PayPilot / Pilot Innovation acts solely as a technology and software provider and is not the designated AML/CTF compliance contact for NEXORA FINTECH LTD.