Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy

“SOLUNEX” LLC

Year 2025

Chapter 1. Introduction

1.1. The management of *Solunex LLC* (hereinafter referred to as the "Company") is fully committed to preventing financial crime, money laundering, and the financing of terrorism (hereinafter "AML/CTF").

1.2. The Company's director(s) are responsible for establishing and maintaining an effective system for the assessment and management of AML/CTF risks, appropriate to the nature and scale of the Company's operations, and for appointing specialized and trained personnel to oversee its implementation.

1.3. To achieve these objectives, this Policy has been developed to set forth the fundamental guiding principles for the prevention of money laundering and terrorism financing.

1.4. The provisions of this document are based on the Law of Georgia *"On Facilitating the Prevention of Money Laundering and the Financing of Terrorism"* (hereinafter, the "Law"), the regulations issued by the Financial Monitoring Service of Georgia (hereinafter, "FMS"), the normative acts and guidance documents of the National Bank of Georgia, as well as the recommendations of the Financial Action Task Force (FATF) and other relevant international organizations, which establish the current standards for AML/CTF compliance.

Chapter 2. Definitions of Terms

- **Legalization of illicit income (Money laundering):** The legalization of illicit income, i.e., granting a legal form to illicit and/or unjustified property (use of assets, acquisition, possession, conversion, transfer, or other actions) for the purpose of concealing its illicit and/or unjustified origin or assisting another person in avoiding liability, as well as concealing or disguising its true nature, source, location, placement, movement, ownership, or other associated rights.
- **Terrorism financing:** The collection or provision of funds or other assets with prior knowledge that they will be used, in whole or in part, by a terrorist or terrorist organization, or for the execution of terrorist activities; or with prior knowledge, providing services, shelter, resources, or other material support to a terrorist or terrorist organization.
- **Linked transactions:** Transactions concluded within a reasonable time frame or determined as linked based on other criteria, which are associated with the same client.
- **Suspicious transaction:** A transaction for which there are reasonable grounds to suspect that it was prepared, executed, or conducted using illicitly obtained property or income derived from such property, and/or for the purpose of money laundering, or is related to terrorism financing.
- **Client:** A person who establishes a business relationship with the Company or conducts a one-off transaction to use its services.
- **Business relationship:** A continuous commercial or professional relationship between the Company and a client, involving the provision of services as defined by Georgian law.

- **One-off transaction:** A transaction (outside the scope of a business relationship) involving the provision of services by the Company to a client as defined by Georgian law.
- **Identification:** The process of obtaining identifying data about a person that allows for their verification and distinction from other individuals.
- **Verification:** Obtaining information or documents that enable the reporting entity to verify the accuracy of the identification data obtained about a person, and, in the case of a beneficial owner, to confirm their identity.
- **Confidential information:** Information or documents containing professional secrets, trade secrets, and/or personal data.
- **Person:** A natural person, legal entity, or unregistered organizational entity.
- **Sanctioned persons list:** A list of natural or legal persons subject to sanctions imposed by UN Security Council resolutions, the United States, the United Kingdom, the European Union, Russia, or Belarus.
- **Location:** The jurisdiction, country, or territory in which a person is registered and/or conducts activities.
- **Politically exposed person (PEP):** A natural person holding a prominent public or political function (excluding middle- and lower-level officials), including:
  a) Head of state, head of government, government member (minister), deputy, or head of a state institution;
  b) Member of a legislative body (parliament);
  c) Head of a political organization or member of its governing body;
  d) Member of the Supreme Court, Constitutional Court, or other high-level courts;
  e) Auditor general, deputy, or member of an audit institution;
  f) Member of the board of the national (central) bank;
  g) Ambassador or head of a diplomatic mission;
  h) Head of defense/military forces;
  i) Head or member of the governing body of a state-owned enterprise;
  j) Head, deputy, or member of the governing body of an international organization.
- **Family members of a politically exposed person:** Spouse or a person living in a joint household with the PEP, as well as parents, children, and the spouse of their children, who live together in the same household.
- **Associate of a politically exposed person:** A natural person who is a beneficial owner of a legal entity, unregistered organizational entity, trust, or trust-like structure together with a PEP, or has a close business, social, or political relationship with a PEP, or who is the beneficial owner of a legal entity or structure created for the benefit of a PEP.
- **PEP status persons:** Persons designated by the Company as having PEP status, including politically exposed persons, their family members, and associates.
- **International organization:** A permanent intergovernmental or supranational organization.

- **Beneficial owner:** A natural person who ultimately owns or controls a client, or on whose behalf a transaction is conducted. For corporate entities (or other organizational entities under Georgian law), a beneficial owner is a natural person who directly or indirectly owns or controls 25% or more of the shares or voting rights, or otherwise exercises control over the entity.
- **Controlling person of a legal entity:** A natural person with the power to exercise significant influence over the management of a legal entity, directly or indirectly, individually or jointly, through ownership of voting rights or other means.
- **Legal entity:** Both resident and non-resident corporate entities, non-commercial (non-profit) legal entities, and other organizational entities recognized under law, including their branches and representative offices.
- **Non-commercial (non-profit) legal entity:** A private law non-commercial entity under Georgian law (e.g., NGO, unregistered association, political party, election bloc, voter initiative group, fund, federation, church).
- **Trust:** A fiduciary arrangement under which property belonging to the owner is transferred to a trustee (or custodian) under a trust declaration or agreement, who manages it to achieve the beneficiary's maximum benefit or according to the owner's instructions. The income generated is shared among income beneficiaries; the owner may also be a beneficiary. This includes legal relationships defined under the 1985 Hague Convention or similar structures.
- **High-risk jurisdiction:** Jurisdictions designated as high-risk by the President of the National Bank of Georgia.
- **Offshore zone:** Jurisdictions approved as offshore by the President of the National Bank of Georgia.
- **Ownership/founding structure:** The continuous chain of founders of a legal entity up to the ultimate beneficial owner.
- **Reasoned suspicion:** A set of information or circumstances that would lead an objective observer to conclude that a crime may have been committed.
- **Reasonable grounds:** Information, circumstances, or facts provided by competent authorities in Georgia or other jurisdictions that would lead an objective observer to reasonably suspect a person's involvement in terrorism financing or financing the proliferation of weapons of mass destruction, whether or not criminal proceedings have been initiated.
- **Suspicion:** A set of information, facts, or circumstances that objectively raises doubts for the reporting entity that a transaction involves illicit property or income, money laundering, or terrorism financing, and which cannot be dispelled through preventive measures.
- **Unusual transaction:** A complex, unusually large, or atypical set of transactions that appears to have no clear economic or lawful purpose.
- **Transfer of a convertible virtual asset:** A transaction resulting in the transfer of a virtual asset from one distributed ledger address, virtual asset account, or other device to another,

conducted via a virtual asset service provider or other financial institution authorized to provide such services. The sender and recipient of the virtual asset may be the same entity or use the same provider.

- **FMS:** Financial Monitoring Service of Georgia.
- **RBA:** Risk-Based Approach.
- **KYC (Know Your Customer):** Procedures for identifying and verifying clients.
- **KYCUB (Know Your Customer's Ultimate Beneficiary):** Procedures for identifying and verifying a client's beneficial owner.
- **EDD (Enhanced Due Diligence):** Enhanced preventive measures defined under the Company's KYC policy.
- **NBG:** National Bank of Georgia.
- **AMLO:** AML Officer responsible for the Company's AML/compliance function.
- **Note:** Other terms used in this Policy shall have the meaning defined by Georgian law and other normative acts.

Chapter 3. Assessment and Management of Money Laundering and Terrorism Financing Risks

3.1. The Company has implemented procedures for the identification and assessment of AML/CTF risks and carries out proportional measures to manage these risks using a risk-based approach.

3.2. The Company has established a unified risk-based approach for client assessment, which includes risk identification, analysis, implementation of preventive measures appropriate to the risk, and the development of an effective risk management strategy.

3.3. The Company ensures that risk-based approaches are applied both to prospective clients seeking to establish a business relationship and to existing clients engaged in ongoing business relationships, as well as to individuals conducting one-off operations or transactions.

3.4. The Company establishes appropriate criteria based on the level of risk, enabling effective assessment of potential and anticipated risks from individuals interested in its services.

3.5. The Company ensures that individuals interested in its services or existing clients are assigned an appropriate risk level in accordance with the Client Risk Assessment Policy.

3.6. The Company defines its organizational AML/CTF risk appetite, specifying which ML/TF risks it accepts in line with its strategic objectives and the types of controls or restrictions imposed to manage these risks.

3.7. Based on a risk-based approach, labor, time, and technological resources are allocated according to priorities, ensuring enhanced controls are applied to high ML/TF risks.

3.8. AML/CTF risk assessment is carried out considering the client and beneficial owner, the nature of their activities, the jurisdiction of their location, and other risk factors.

3.9. For clients, business sectors, jurisdictions, geographical areas, and each group of services/products, corresponding risk levels are defined.

3.10. Based on the risk levels, a client is assigned a high, medium, or low-risk category.

3.11. Risk management measures applied to clients depend on the assigned risk level. Specifically, standard preventive measures are applied to medium-risk clients, enhanced preventive measures to high-risk clients, and simplified preventive measures to low-risk clients.

3.12. Assessment of ML/TF risks related to clients and determination of their risk level is carried out prior to establishing a business relationship and periodically during the relationship, as well as when significant changes occur in circumstances related to the client.

3.13. The rules and procedures for client risk assessment are governed by this Policy and the Client Risk Assessment Policy.

3.14. Introduction of new technologies, products, services, or delivery methods, or other significant changes in business practices (hereinafter, "new product") is permissible only based on an assessment of the ML/TF risks associated with such changes.

3.15. The process for introducing a new product includes assessment of its associated risks, determination of necessary control mechanisms, the risk management process, risk mitigation strategy, evaluation of residual risk, and involvement of all relevant structural units (at minimum, AMLO, and where necessary, Information Security and others).

3.16. Prior to the introduction of a new product, the Company must ensure that it has the appropriate resources, infrastructure, and processes for risk management.

3.17. Any significant change in product characteristics requires reassessment. Risk assessments of new products are documented.

3.18. The organizational risk level is determined in accordance with the Company's "Organization-wide ML/TF Risk Assessment Methodology," which aims to assess money laundering and terrorism financing risks and improve risk mitigation mechanisms.

3.19. Organization-wide ML/TF risk assessments are conducted every two years or, if necessary, within one month upon identification of a significant change in the Company's risk profile (e.g., structural hierarchy changes within organizational units, merger with another company, etc.). In exceptional cases (e.g., as instructed by a supervisory authority), organizational risk assessments may be conducted within the timeframe or frequency determined by the supervisory authority.

3.20. The results of the organization-wide ML/TF risk assessment methodology are documented and, upon request, made available to the National Bank of Georgia.

Chapter 4. Control of International Financial Sanctions

4.1. "Solunex" LLC aims to conduct its activities in compliance with international and local sanctions. The Company's International Financial Sanctions Compliance and Screening Procedure defines the procedures, guiding principles, and control mechanisms that ensure the Company's activities comply with applicable laws and regulations on sanctions.

4.2. Sanctions risk management includes the processes of identifying, assessing, and managing potential risks of sanctions breaches within the scope of business relationships and executed transactions established by the Company.

4.3. Sanctions risk identification involves thorough review of client profiles, types of transactions, blockchain addresses, wallets, types of cryptocurrencies, geographical location, and service specifics during the establishment of a business relationship or execution of a one-off transaction to detect possible links to sanctioned persons or countries.

4.4. For blockchain analysis, the Company uses specialized software that determines the source and destination of virtual assets in a transaction, analyzes transaction flows, and identifies scenarios that may indicate suspicious activity.

4.5. The software has access to lists of sanctioned wallets and assigns a high-risk rating to any transaction with a match, forming the basis for enhanced preventive measures.

4.6. The principles defined in the International Financial Sanctions Compliance and Screening Procedure apply to all transactions, operations, business relationships, and one-off transactions.

4.7. To ensure compliance with international sanctions requirements, the Company screens all clients and transaction participants against sanctions lists issued by the United Nations, the European Union, the United States, and the United Kingdom.

4.8. The Company complies with sanctions regimes imposed on Russia and Belarus by the EU, the United States, and the UK, following the requirements of the National Bank of Georgia's Resolution No. 208/04 dated 4 August 2023, "Rules for Compliance with Sanctions Regimes by Reporting Entities Supervised by the National Bank of Georgia."

4.9. The Company uses automated software that provides automatic verification of clients against the following lists:

1. European Union consolidated list
2. OFAC Specially Designated Nationals & Blocked Persons
3. Denied Persons List
4. Federal Bureau of Investigation Most Wanted Terrorists & Seeking Information
5. Bank of England Sanctions List
6. HM Treasury
7. Non-Cooperative Countries and Territories
8. PEP List
9. EU Terrorism List
10. World Bank Ineligible Firms
11. Department of Foreign Affairs and Trade
12. Sanctions lists imposed on Russian and Belarusian nationals following developments in Ukraine

4.10. Ensuring compliance with sanctions includes:

- Refusing to establish or continue business relationships, or conduct one-off transactions, that may be associated with sanctions violations;

- Implementing effective control mechanisms to detect potential sanctions breaches;
- Clearly defining responsibilities for sanctions risk management and establishing a transparent organizational structure.

4.11. Sanctions risk management encompasses identification, assessment, and management of potential sanctions breach risks for all business relationships and executed transactions, including one-off transactions, in each operation.

4.12. Sanctions risk identification involves detailed examination of client profiles, transaction types, geographical locations, and service specifics during business relationship establishment or execution of one-off/multiple transactions to detect potential links to sanctioned persons, addresses, or countries.

4.13. The sanctions risk assessment process is dynamic, regularly reviewed, and updated when significant changes occur, such as amendments to sanctions regimes, legal requirements, or the Company's products and services.

4.14. The Company has implemented robust control mechanisms at various stages of client service to ensure timely detection and prevention of potential sanctions violations.

4.15. For sanctions compliance, daily automated screening (once every 24 hours) of existing clients and those in ongoing business relationships is conducted against lists published by the procedure, countries, and competent international organizations, comparing client identification data with sanctioned persons.

4.16. To detect clients' connections to sanctions, information on all transaction participants and sources of virtual assets is collected, and potential links to sanctioned addresses are checked for each operation, regardless of whether it is a one-off transaction or part of an ongoing business relationship.

4.17. If there is suspicion of a sanctions regime breach regarding a client or their transaction, the system automatically blocks the client's profile/account (including electronic wallet accounts within the Company) and registration/transaction. The AML Officer is notified, who analyzes the information and performs appropriate actions in accordance with this document and legal requirements.

4.18. Responsibility for sanctions compliance control lies with the person responsible for the functioning of the compliance system, represented by the Company's AML Officer. Ultimate responsibility for the effective functioning of the system rests with the Company's director.

Chapter 5. Preventive Measures

5.1. The foundation of the Company's compliance control system for the prevention of money laundering (ML) and terrorist financing (TF) is the principle of "Know Your Customer" (KYC).

5.2. KYC approaches and standards are regulated by this Policy and the "Know Your Customer (KYC) and Preventive Measures Policy."

5.3. For the purposes of this Policy, the Company implements legally required preventive measures, which include:

- Identifying the client and verifying their identity using reliable and independent sources;
- Identifying the beneficial owner, the person responsible for representation/authority, and legal entities within the ownership structure, and taking reasonable measures to verify them using reliable sources;
- Determining the purpose and intended nature of the business relationship;
- Assessing ML/TF risks arising from a person in a one-off transaction or within a business relationship, and assigning the appropriate risk level to the person seeking to establish a business relationship;
- Monitoring the business relationship.

5.4. Implementation of preventive measures is mandatory under the following circumstances:

- Establishment of a business relationship;
- Conducting a one-off transaction;
- Regardless of the amount, establishing a business relationship is mandatory if the service is received by a legal entity or an individual entrepreneur;
- Establishing a business relationship is mandatory if the amount of a one-off transaction involving convertible virtual assets exceeds 3,000 GEL, 1,000 EUR/USD, or if the total volume of related transactions conducted by the person with the Company (including split transactions) exceeds 3,000 GEL/1,000 EUR/USD;
- Doubts about the accuracy of the client's identification data or compliance with legal requirements;
- If a one-off transaction does not exceed 3,000 GEL, 1,000 EUR/USD, or the total volume of related transactions conducted by the person with the Company does not exceed 3,000 GEL/1,000 EUR/USD, after the client's identification/verification, the following identification data shall be obtained and recorded:
- Full name;
- Personal identification number (if available);
- Date of birth;
- Date of issue and validity period of identity and/or citizenship document.

5.5. Preventive measures must be implemented according to the client's risk level before conducting a one-off transaction or establishing a business relationship, as well as periodically during the course of the business relationship or when material circumstances related to the client change.

5.6. Anonymous or fictitious client registration and service provision are strictly prohibited.

5.7. For clients classified as high-risk, or in other high-risk scenarios defined in this Policy, the following enhanced preventive measures must be implemented:

- Obtaining additional information/documentation about the client's and/or beneficial owner's assets and business activities (including current activity and location, sources of convertible virtual assets, income, and property, business history, reputation, etc.);
- Obtaining additional information about the intended nature of the business relationship, including the purpose of past, current, and expected transactions (e.g., description of client's business operations, information on contractors, suppliers, customers, client's residential, workplace, or business location);

- Obtaining authorization from the Director to establish or continue the business relationship;
- Taking reasonable measures to determine the source of the client's assets, convertible virtual assets, and funds;
- In certain cases, access to specific products may be restricted, or transaction limits imposed for risk mitigation.

5.8. Enhanced monitoring of the business relationship, which includes at a minimum:

- Reviewing/updating client information/documentation at least once a year to verify whether the client's risk level has changed and remains manageable;
- Reviewing the basis (purpose and intended nature) of the client's transactions, the participants involved, and the source of funds or convertible virtual assets;
- Ongoing monitoring to ensure that the client's declared information aligns with actual activity, aiming to identify unusual, suspicious, or unexpected transactions or patterns.

5.9. A high-risk jurisdiction is a country or territory with significant deficiencies in its system for preventing money laundering or terrorist financing.

5.10. The National Bank of Georgia approves the list of high-risk jurisdictions and offshore zones.

5.11. The Company applies enhanced preventive measures if:

- The client is a legal entity registered in a high-risk jurisdiction/offshore zone or a branch of such a legal entity in Georgia;
- The client is a natural person with registration or actual residence in a high-risk jurisdiction/offshore zone;
- The client's main source of income is a high-risk jurisdiction/offshore zone;
- The client's place of birth is a high-risk jurisdiction (see Client Risk Assessment Policy).

5.12. When implementing preventive measures, before entering into a business relationship or conducting a one-off transaction, it is determined whether the client or beneficial owner is a politically exposed person (PEP), a family member of a PEP, or associated with a PEP, based on verification against relevant lists.

5.13. If the client or beneficial owner is a PEP, a PEP's family member, or associated with a PEP, the following enhanced preventive measures must be implemented:

- Obtain authorization from management to establish or continue the business relationship as an unconditionally high-risk client;
- Take reasonable measures to determine the source of the PEP's assets, convertible virtual assets, and funds;
- Conduct enhanced monitoring of the business relationship;
- After the client or beneficial owner ceases to hold significant public or political functions, the Company considers ongoing risks associated with PEP connections.

5.14. A local or foreign person is considered a politically exposed person for 1 (one) year following the termination of the aforementioned position.

5.15. For clients classified as low-risk, simplified preventive measures are applied, which include:
5.15.1. Updating identification data of the client and/or beneficial owner once every five years;
5.15.2. Determining the purpose and intended nature of the business relationship or transactions based on their type;
5.15.3. Simplified preventive measures must not be applied if there is suspicion of money laundering or terrorist financing;
5.15.4. Simplified or any type of preventive measures cannot be implemented without identifying/verifying the client and/or beneficial owner. The Company does not exercise the legal right to complete identification/verification within 30 days after establishing the business relationship;
5.15.5. Establishing a business relationship or conducting a one-off transaction is prohibited if:

- Appropriate risk-based preventive measures have not been implemented;
- There is a reasonable suspicion that the client, the client's beneficial owner, a person within the ownership structure, or any other transaction participant is listed as a sanctioned person under UN Security Council resolutions, EU, US, UK, Russia, or Belarus sanctions;
- The Company is not confident it can effectively manage risks associated with the business relationship or one-off transaction;
- The client is a terrorist or suspected of financing terrorism or a terrorist organization;
- Other cases as defined by the Company's policies and procedures;
- The business relationship with an existing client must be terminated if any of the above circumstances arise.

Chapter 6. Client Identification and Verification

6.1. Before establishing a business relationship or executing a one-off transaction, client identification and verification of identification data must be performed based on reliable and independent sources.

6.2. Client verification includes the identification of any person acting on behalf of the client, verification of such person based on reliable and independent sources, and obtaining a properly certified document confirming their representation authority.

6.3. Identification, verification, or updating of a client, a person acting on behalf of the client, or a beneficial owner can be performed without the client's consent through systems integrated with the electronic databases of the Public Service Development Agency.

6.4. The identification data, information, and documents to be obtained for client and representative verification, as well as the procedures for verification, recording, storage, and updating, are defined by the applicable laws of Georgia.

6.5. Establishing or continuing a business relationship, or executing a one-off transaction, is prohibited if client identification, verification, or updating of identification data cannot be completed.

6.6. Before establishing a business relationship or executing a one-off transaction, the Company performs client identification and verification based on reliable and independent sources.

6.7. For natural persons, identification must be performed using original documents.

6.8. A document used to verify the identity of a natural person must:

- Contain the standard features of that document type (number, issue and expiry dates, security features, etc.);
- Not be significantly damaged;
- Include a photograph allowing the identification of the document holder;
- Be valid at the time of presentation.

6.9. For the identification of resident or non-resident natural persons, the Company collects:
a) Full name;
b) Date of birth;
c) Personal identification number (if available);
d) Identity or citizenship document number, issue date, issuing country, issuing authority, and expiry date;
e) Gender;
f) Citizenship, including dual citizenship;
g) Place of birth (country and city if available);
h) Registration address;
i) Actual residence address.

6.10. For natural persons legitimately residing in the Autonomous Republic of Abkhazia or the Tskhinvali region (former South Ossetian Autonomous District), the following data is collected:
a) Full name;
b) Date of birth;
c) Personal identification number;
d) Neutral certificate or neutral travel document number, issue date, issuing country, issuing authority, and validity period (if available);
e) Gender;
f) Place of birth (country and city if available);
g) Address.

6.11. If the client is a natural person registered as an individual entrepreneur, the following additional data is collected:
a) Taxpayer identification number;
b) Legal address;
c) Registration date;
d) Field of activity.

6.12. Verification of natural persons is performed using valid documents appropriate to their citizenship and residency.

6.13. For residents of Abkhazia or the Tskhinvali region, verification uses a neutral identity certificate or neutral travel document. If only a personal number is assigned, verification is performed using the Public Service Development Agency database.

6.14. For foreign citizens, verification uses:

- Residence permit issued by the Public Service Development Agency;
- Temporary identification certificate issued by the Public Service Development Agency;

- International passport;
- Other documents allowed by Georgian law or international agreements for border crossing;
- Certificate for Georgian citizens residing abroad.

6.15. For stateless persons, verification uses:

- Residence permit issued by the Public Service Development Agency;
- Temporary identification certificate or travel document issued by the Public Service Development Agency.

6.17. For individual entrepreneurs who are Georgian citizens, verification uses passports, identity cards, driver's licenses, or certificates for Georgians residing abroad.

6.18. For foreign individual entrepreneurs, verification uses residence permits, temporary identification certificates, passports, or other legally permitted documents for border crossing.

6.19. The Company does not provide services to minors under 14 years old.

6.20. Verification documents for natural persons must include a photograph (except birth certificates and extracts from the Public Registry) and be valid.

6.21. If a document does not allow verification of data accuracy, other reliable and independent sources must be used.

6.22. The Company may obtain identification data and photographs from the Public Service Development Agency without the data subject's consent.

6.23. If a one-off transaction does not exceed GEL 3,000 / EUR/USD 1,000, or related transactions remain under this threshold, the Company collects at minimum:

- Name and surname;
- Personal number (if unavailable, leave blank);
- Date of birth;
- Identity/citizenship document number.

6.24. Establishing a business relationship is mandatory if the client is a legal entity or individual entrepreneur, regardless of transaction amount. For natural persons exceeding GEL 3,000 / EUR/USD 1,000, the Company must establish a business relationship, which includes obtaining verified copies of identification documents, complete KYC information (citizenship, dual citizenship, activity, purpose, expected transactions, volumes, and risk assessment).

6.25. If a natural person is registered as an individual entrepreneur, the Company establishes a business relationship regardless of transaction amount and additionally collects:

- Identification number;
- Registration date;
- Field of activity;
- Number of employees;
- Legal address;
- Actual address;

- Registering authority;
- Business partner information if required by risk assessment.

6.26. For legal entities, the Company collects, verifies, and records:

- Name;
- Registration date;
- Registration country;
- Legal address;
- Identification data if available;
- Registration number if available;
- Legal form;
- Actual address.

6.27. Legal entities must comply with applicable law and have properly executed founding documentation, supported by a registration certificate or other founding documents issued by the relevant authority.

6.28. Founding and other documents of foreign legal entities must be legalized or apostilled according to Georgian law.

6.29. Required documents for registration and establishing a business relationship vary by jurisdiction and organizational-legal form.

6.30. Ownership and control structures (major shareholders, founders, beneficial owners) must be examined. Certified extracts or share certificates for each entity in the ownership chain must be presented.

6.31. Identification of directors and authorized representatives of legal entities uses all identification data as outlined for natural and legal persons.

6.32. Beneficial owner identification follows procedures for examining ownership and control structures.

6.33. For branches, the parent organization's and its directors' and authorized representatives' data must be obtained.

6.34. For administrative bodies, international organizations, financial institutions, or diplomatic missions, the Company collects the client's name, legal address, and directors' identification data.

6.35. Verification is based on official extracts or other documents confirming registration, existence, and current data.

6.36. For legal entities registered in Georgia: extracts from the Public Registry of Entrepreneurs and Non-Entrepreneurial Legal Entities.

6.37. For foreign legal entities: extracts from relevant registries or other documents issued by the registration authority.

6.38. Documents used for verification must contain current identification data and be no older than 12 months unless verification is conducted directly via a registry.

6.39. If a document does not allow verification of accuracy, other reliable sources must be used.

6.40. For branches, verification of the parent organization and its authorized representatives must be performed.

6.41. For administrative bodies, international organizations, financial institutions, or diplomatic missions, verification uses publicly available or other reliable sources.

6.42. The Company may obtain identification data of directors, authorized representatives, or beneficial owners from the Public Service Development Agency without consent.

6.43. For unregistered organizational entities, the Company collects:

- Name;
- Date of establishment;
- Legal address;
- Actual local address;
- Taxpayer identification number if available.

6.44. For identifying directors or authorized representatives of unregistered entities:

- If natural persons, collect identification data as per this chapter;
- If legal persons, collect identification data as per this chapter.

6.45. Verification of unregistered entities uses:

- Founding document (agreement, general meeting resolution);
- Tax registration document if available.

6.46. Verification documents must contain identification data current at the time of verification. If not, other reliable sources are used.

6.47. The Company may access the Public Service Development Agency database without consent to verify directors or authorized representatives of unregistered entities.

Chapter 7. Beneficial Owner Identification

7.1. During the implementation of preventive measures, it is mandatory to determine, identify, verify, and validate the identity of the client's beneficial owner.

7.2. A beneficial owner is a natural person who is the ultimate owner or ultimate controller of the client and/or on whose behalf a transaction is prepared, conducted, or executed.

7.3. When identifying the beneficial owner of a legal entity, unregistered organizational entity, trust, or trust-like legal structure, it is necessary to examine the client's ownership and control (management) structure. (The Company is prohibited from registering legal entities that are structured as a trust or trust-like legal entity.)

7.4. The beneficial owner of a legal entity is a natural person who directly or indirectly owns 25% or more of the legal entity's shares or voting rights, or otherwise exercises ultimate control over the legal entity.

7.5. Direct ownership of shares or voting rights is considered the holding of 25% or more of the shares or voting rights of a business legal entity by a natural person. Indirect ownership is considered the holding of 25% or more of the shares or voting rights of a business legal entity by a legal entity controlled by the natural person(s), or by multiple legal entities controlled by the same natural person(s).

7.6. If, after all possible measures, the Company determines that no beneficial owner holds 25% or more, identification and verification procedures must be performed for the person(s) with management authority in the client organization.

7.7. Examination of the client's ownership and control structure and identification and verification of the beneficial owner is carried out in accordance with the procedure established by Georgian law (see "Policy on Examination of Client Ownership and Control Structure and Identification and Verification of Beneficial Owner").

Chapter 8. Determination of the Purpose and Intended Nature of the Business Relationship

8.1. To determine the purpose and intended nature of the business relationship, the Company collects and systematically records the following information about the client during the service process:

- Information related to the client's business activity;
- Information regarding the client's sources of income;
- Information about the purpose of the business relationship and the role of any third party in the client-related transaction (if applicable);
- Information regarding the intended nature of the business relationship, specifically which products or services the client intends to use;
- Information about the expected volume, type, frequency, currency, geographical scope, period, counterparties' identities, and residency of operations/transactions.

8.2. Before establishing a business relationship and prior to each transaction, whether it is a one-off transaction or part of an ongoing business relationship, the Company additionally checks the client (including the beneficial owner and/or other relevant persons) against politically exposed persons (PEPs) and sanctioned persons databases (see International Financial Sanctions Compliance and Screening Procedure).

Chapter 9. Monitoring of the Business Relationship

9.1. Throughout the entire duration of the business relationship with the client, the Company conducts ongoing risk-based monitoring, which includes the following measures:

- Maintaining updated records of the client's (including the beneficial owner's) identification data and documents, as well as records regarding the purpose and intended nature of the business relationship, and reviewing the assigned risk level in accordance with the client's executed transactions and updated information.
- Examining executed transactions and verifying their consistency with the information available regarding the client, their business activity, risk profile, and sources of funds or convertible virtual assets.

- Proactively identifying unusual and suspicious transactions (see Suspicious Transaction Detection Procedure).

9.2. Information related to the client is regularly verified, and records and relevant documentation are updated as changes occur; the client's risk level is also reassessed.

9.3. The frequency of reviewing/updating information/documents about the client depends on the assigned risk level:

- Low risk – at least once every 5 years;
- Standard risk – at least once every 3 years;
- High risk – at least once a year.

9.4. In the event of changes in the beneficial owners and/or persons authorized to manage or represent the client, or persons within the founding structure, the client may receive services only after identification/verification of the changed persons, regardless of the predetermined record update period.

9.5. During the ongoing monitoring of transactions, the Company reviews the transactions executed by the client and verifies whether they correspond to the information available to the Company regarding the client. This includes reviewing records about the client's profession, commercial activity, business history, financial condition, risk level, and sources of funds or convertible virtual assets. In case of discrepancies, the client's information/documents are updated and the client's risk is reassessed if necessary.

9.6. During ongoing monitoring, the Company records and examines unusual transactions.

9.7. An unusual transaction is a complex, unusually large transaction or an unusual combination of transactions that lacks an apparent economic (commercial) or lawful purpose.

9.8. A transaction is considered unusual if:

- The transaction is larger than the Company would normally expect based on the client's data, the purpose and intended nature of the business relationship, or the client's characteristics; or
- The transaction or combination of transactions has an unexpected structure or frequency compared to the client's normal activity or the activity of a similar client group; or
- The transaction is highly complex compared to other similar clients' transactions.

9.9. The Company reviews the unusual transaction, its purpose and basis, and, if necessary, conducts enhanced monitoring of the business relationship to detect suspicious transactions.

9.10. The results of the review of an unusual transaction are justified, documented, and stored in a manner that allows immediate presentation to the National Bank of Georgia upon request.

Chapter 10. Politically Exposed Person (PEP)

10.1. A politically exposed person (PEP) is an individual who holds or has held a prominent public or political position (excluding middle- and low-ranking officials), including:

- Head of state, head of government, government member (minister), deputy, or head of a state institution;

- Member of the legislative body (parliament);
- Leader or governing body member of a political organization;
- Member of the Supreme Court, Constitutional Court, or other high-level judicial bodies whose decisions are appealable only in exceptional cases;
- General auditor, deputy, or member of the audit court;
- Member of the board of the national (central) bank;
- Ambassador or head of a diplomatic mission;
- Head of defense or military forces;
- Head or governing body member of a state-owned enterprise;
- Head, deputy, or governing body member of an international organization.

10.2. Family members of a politically exposed person include:

- Spouse or person with whom the PEP permanently shares a joint household;
- Siblings;
- Parents;
- Children and grandchildren;
- Spouse or partner of a child/grandchild with whom they permanently share a joint household.

10.3. Persons associated with a politically exposed person include:

- An individual who, together with the PEP, is a beneficial owner of a legal entity, unregistered organizational structure, trust, or trust-like structure;
- An individual having a close business, social, or political relationship with the PEP;
- An individual who is a beneficial owner of a legal entity, unregistered organizational structure, trust, or trust-like structure effectively created for the benefit of the PEP.

10.4. Screening of clients, their persons authorized to manage or represent them, and beneficial owners is carried out in PEP lists (covering PEPs, PEP family members, and PEP-associated persons):

- Before establishing a business relationship (any person assigned PEP status is automatically considered high-risk and subject to enhanced preventive measures, and written consent from the Company's director is obtained for engagement);
- Before executing a one-time transaction;
- During the business relationship:
- When the client's risk level changes;
- When identification data of the client, their authorized representatives, or beneficial owners changes;
- When there are changes in the client's ownership or control structure;
- When the client conducts suspicious or unusual transactions;
- Immediately upon PEP list updates (within 24 hours);
- Screening of the person and all participants in a transaction is performed for every transaction, whether one-time or within a business relationship;
- Existing clients assigned PEP status have their risk level reassessed, are assigned unconditional high risk, enhanced preventive measures are applied, and written consent from the Company's director is obtained to continue the business relationship.

10.5. If a client or beneficial owner is a PEP, a PEP-associated person, or a family member, the Company applies the following enhanced preventive measures:

- Takes reasonable measures to verify the source of the client's wealth, funds, and virtual assets to ensure they are not derived from criminal activity. Verification must rely on reliable, independent sources, information, or documentation;
- As a high-risk client, establishing or continuing a business relationship requires the Company director's approval. The director must review information obtained through preventive measures and the AMLO's substantiated assessment of client-related risks to make a fully informed and reasoned decision;
- The Company conducts enhanced monitoring of both the client's transactions and business relationship-related risks.

10.6. A client's PEP status (assigned if the person is a PEP, a family member, or associated with a PEP) may also be identified during the update of client information using public sources.

10.7. A client, authorized representative, or beneficial owner may have their PEP status removed after reasonable analysis, if it is determined that the person no longer holds a relevant position under the law, no longer performs prominent public or political functions, or no longer meets the circumstances that initially conferred PEP status.

10.8. After the cessation of significant public or political functions by the client or beneficial owner, the Company continues to consider ongoing risks associated with the client.

10.9. For one year following changes in circumstances that initially led to PEP status, the enhanced preventive measures defined in this document continue to apply. This decision is documented and stored in the client's profile.

Chapter 11. Virtual Asset Address Screening Process

11.1. The Company conducts screening of virtual asset addresses/e-wallets:

- For every transaction performed by the client, whether one-time or within the scope of an ongoing business relationship;
- During scheduled reviews of the client database (at least once per year).

11.2. For virtual asset address screening, the Company uses automated software that analyzes the source of convertible virtual assets associated with the addresses based on the following criteria.

11.3. High-Risk Circumstances:

- Persons linked to sexual violence, coercion, or child exploitation;
- Virtual assets associated with illegal activity (dark markets);
- Virtual assets related to child abuse, terrorism financing, or trade in prohibited substances (dark services);
- Legal proceedings against the organization (enforcement actions);
- Exchanges involved in fraud (fraudulent exchanges);
- Virtual assets linked to unlicensed online gambling;
- Virtual assets linked to illegal activities (illegal services);

- Virtual assets received through mixers;
- Virtual assets obtained through threats or extortion (ransom);
- Virtual assets from sanctioned addresses or persons;
- Virtual assets obtained via scam, fraud, or phishing;
- Virtual assets forcibly obtained from victims (stolen coins/hacked wallets/funds);
- Virtual assets from persons associated with terrorism financing.

11.4. Suspicious Sources:

- Virtual assets obtained via self-service kiosks (ATMs);
- Exchanges that do not implement verification procedures (high-risk exchanges);
- P2P exchanges allowing daily withdrawals over $1,000 without KYC/AML procedures (high-risk P2P exchanges);
- Exchanges allowing daily withdrawals over $2,000 without KYC/AML procedures (moderate-risk exchanges);
- Smart contracts where tokens are locked to provide liquidity (liquidity pools);
- Crypto ATMs;
- Virtual assets associated with unlicensed online gambling/gaming;
- Virtual assets from VASPs not registered or licensed in Georgia or any other jurisdiction;
- Virtual assets associated with large-scale cryptocurrency purchases or sales without a centralized exchange (OTC desks);
- Smart contracts where tokens are locked for financial services (e.g., lending, borrowing, insurance) (decentralized services including coin swap services and DeFi platforms).

11.5. To assess and categorize the risk of a virtual asset address (or transaction), the software evaluates the probability that the operation or address is linked to illegal activity and assigns a risk level as follows:

- Low risk – probability up to 30%;
- Medium risk – probability 30% to 60%;
- High risk – probability 60% to 80%;
- Unacceptable risk – probability over 80%.

11.6. During virtual asset address screening, if high or unacceptable risk or high-risk factors (hazardous, suspicious, or sanctions/terrorism-related) are detected, the client's transaction/service is halted or delayed in real time, regardless of the amount. In such cases, the AML Officer undertakes the following actions:

- Conducts enhanced due diligence and reviews the client and transaction;
- Decides whether to provide or deny service to the client;
- If necessary, provides information to the Financial Monitoring Service (FMS) the same day;
- Reassesses the client's risk level if needed and obtains the Company Director's consent to continue the business relationship.