AML POLICY

banqo

AML POLICY

Prime Money Services Group Inc., a company registered under corporate access number 2026726477, with a registered address at 1 Street SE, Calgary AB T2G5G3, Alberta, Canada. Prime Money Services Group Inc., operating under the brand name **banqo**, facilitates access between clients and IBAN accounts, establishing relationships between clients and the IBAN providers.

The following AML Policy shall govern the use of banqo's online website, http://www.banqo.ai/, as well as any services provided by the Company.

You can contact banqo at E-mail: support@banqo.ai, Address: 1 Street SE, Calgary AB T2G5G3, Alberta, Canada.

By availing yourself of any banqo services, you acknowledge your awareness of the associated risks. To the maximum extent allowed by mandatory provisions of applicable law, you absolve banqo.ai of any liability related to your use of the provided services.

1. DEFINITIONS

For the purpose of this policy, the following terms have the following meanings:

- AML: Anti-Money Laundering.
- Beneficial Owner: A natural person who, directly or indirectly, holds the final dominant influence over a natural or legal person.
- Business Relationship: A relationship established between the Company and its Customers for the provision of virtual currency services.
- CDD: Client due diligence
- CFT: Combating the Financing of Terrorism.
- Company: Prime Money Services Group Inc., operating under the brand name banqo.
- MLRO: The designated individual responsible for ensuring compliance with AML regulations.
- Customer or Clients: Refers to the corporate clients or users of the Company's services.
- EDD: Enhanced due diligence
- EEA: European Economic Area.
- ISA: International Sanctions Act.
- High-Risk Terrorism Country: A country or region associated with a higher risk of terrorist financing.

- HIO: Head of an international organization
- Management Board: The governing body of the Company responsible for its management and representation.
- Money Laundering: The process of concealing the origins of illegally obtained money.
- MLTFPA: Money Laundering and Terrorist Financing Prevention Act.
- PEP: Politically Exposed Person.
- Risk Appetite: The level of risk the Company is willing to accept for its strategic goals.
- RCA: Relatives and Close Associates of PEPs.
- Sanctions: Measures imposed to support international security, democracy and human rights.
- Subject of International Sanction: A person or entity directly specified in international sanction measures.
- Staff: Employees or individuals providing services to the Company.
- Terrorist Act: A terrorist act encompasses offenses defined under international treaties, including unlawful activities such as hijacking aircraft, compromising civil aviation safety, taking hostages, safeguarding nuclear materials, endangering maritime navigation, committing terrorist bombings and financing terrorism. Additionally, it includes any act aimed at causing death or serious injury to civilians or non-combatants, with the intent to intimidate a population or coerce a government or international organization into action or inaction.
- Terrorist Organization: A terrorist organization refers to any group that engages in terrorist acts, either directly or indirectly, including committing or attempting such acts, acting as an accomplice, organizing or directing others to carry out terrorist activities or intentionally contributing to these acts with knowledge of the group's intent to pursue terrorism.
- TF: Terrorist Financing.
- UBO: Ultimate Beneficiary Owner.
- Webpage: The online platform of the Company where Customers access their accounts.

2. REGULATORY FRAMEWORK- Proceeds of crime (money laundering) and terrorist financing act

In December 2001, Canada enacted the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA or "the Act"). The Act, along with its associated regulations (collectively referred to as "the Legislation"), aims to deter money laundering and terrorist financing (ML/TF) while supporting the identification, investigation and prosecution of ML/TF offenses.

The Legislation mandates that various individuals and entities, known as Reporting Entities, establish and maintain compliance programs that meet the requirements outlined within the Act. Additionally, the PCMLTFA established the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as the agency responsible for collecting, analyzing and disclosing information to detect, prevent and deter ML/TF activities in Canada and globally. FINTRAC serves as Canada's financial intelligence unit and fulfills its mandate through the following activities:

- Receiving financial transaction reports and voluntary disclosures in accordance with the PCMLTFA;
- Ensuring Reporting Entities comply with the PCMLTFA;
- Producing financial intelligence to support ML/TF investigations and threats to Canada's security;
- Researching and analyzing trends and patterns in ML/TF activities;
- Maintaining a registry of money services businesses in Canada; and
- Promoting public awareness and understanding of ML/TF issues.

As part of its compliance mandate, FINTRAC conducts periodic examinations of Reporting Entities. It has the authority to impose administrative monetary penalties on entities that fail to implement effective compliance programs and to recommend cases of criminal non-compliance for prosecution.

3. AML/KYC

3.1 Banqo's Anti-Money Laundering Policy, aimed at preventing the laundering of funds derived from criminal activities, is an essential component of the company's internal protocols. The anti-money laundering measures adhere to widely accepted standards and fulfil the regulatory obligations imposed on financial firms by governing authorities.

3.2 To prevent the concealment of illicit funds for their subsequent use as legitimate capital in financial transactions, banqo performs comprehensive client identification, including a review of business reputation and previous convictions in accordance with regulatory procedures. The Know Your Client (KYC) policy involves document verification, ensuring clients' compliance with the law and responsibility for their funds.

3.3 Utilizing modern technologies for personal identification, banqo monitors client activities and employs a record-keeping system to track suspicious transactions. The company promptly provides necessary information to relevant authorities overseeing anti-money laundering efforts.

3.4 Banqo retains the right to place fund transfers on hold if there are suspicions of criminal activity, obligating reporting of such transactions to supervisory authorities without client notification. banqo may adjust its Anti-Money Laundering Policy at its discretion.

3.5 The KYC Policy aims to prevent banqo from being utilized for money laundering or terrorist financing. Through KYC procedures, banqo seeks to understand its Clients and their financial dealings, enhancing risk management. Any fraudulent activity will result in immediate account closure.

Prevention:

- To ensure the integrity of sensitive data banqo obtains from the Client's account information and the transactions they make.
- To prevent criminal elements from using banqo for money laundering activities.
- To enable Company to know and understand its Clients and their financial dealings better which, in turn, would help the Company to manage risks prudently.
- To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- To comply with applicable laws and regulatory guidelines.

3.6 Banqo will conduct thorough inquiries to identify the ultimate owners and controllers of the company to the extent practicable. If any changes occur in the company's structure, ownership status or transactional nature that raises suspicions, additional inquiries will be conducted. It is essential to collect updated documentation and information to maintain the legal person's economic profile. Certified copies should be obtained from notaries, diplomatic officials, lawyers or equivalent professionals. Control standards will be closely scrutinized, considering the origin of the documents and the context in which they are presented.

3.7 KYC and KYT Monitoring:

3.7.1 The Client acknowledges and agrees that banqo, will utilize an Automated Transaction Monitoring system. Through this system, banqo examines transactions to identify links to various illicit activities. This screening is essential

for ensuring compliance with regulatory obligations and safeguarding banqo and its customers from accepting transactions associated with illegal or illicit funds.

3.7.2 Banqo is linked to the KYT Automated Vendor through an API to facilitate automated screening. Whenever a deposit is received, the system automatically assesses each deposit transaction to establish a risk score for the related funds and bank/EMI accounts. banqo's platform systematically tracks the sender's bank account, submitting an API request to the KYT Automated Vendor with this information to conduct a Basic Check on the incoming transaction.

3.7.3 The Client, consents to the use of the KYT Automated Vendor by banqo for monitoring transactions involving the exchange of foreign currencies. The KYT Automated Vendor may assess transaction patterns, amounts, frequency and other relevant factors to identify and mitigate potential risks associated with money laundering, terrorist financing and other illicit activities.

3.7.4 Banqo will use the KYT Automated Vendor to conduct transaction monitoring in accordance with applicable laws and regulations. If the KYT Automated Vendor detects transactions that raise suspicions of illegal activities or non-compliance with AML regulations, banqo reserves the right to take appropriate actions, including but not limited to placing transactions on hold, freezing accounts and reporting the suspicious activities to relevant authorities.

3.7.5 The Client acknowledges the importance of transaction monitoring for regulatory compliance and agrees to cooperate with banqo in providing any necessary information or documentation required for AML checks. The Client further understands that the KYT Automated Vendor monitoring activities aim to maintain the integrity of the financial system and protect against unlawful activities.

4. CLIENT'S RIGHTS, RESPONSIBILITIES AND PROHIBITED ACTIVITIES

4.1 Requirement to Update Information by the Client:

The Client commits to promptly, within a maximum of three calendar days, notify banqo of any modifications to the information or documents previously supplied by the Client. This includes details provided during System registration, as well as information linked to the Client's contacts, business operations, customer portfolio, financial status, legal position, corporate arrangement, beneficial ownership, etc. This holds true regardless of whether this information has been shared with public registers/authorities.

4.2 Supplementary Information upon Demand:

Throughout the ongoing business relationship, at banqo's request, the Client must furnish additional information and/or documents concerning the Client, its business undertakings and the provision of Services. This is essential for effectively managing Anti-Money Laundering (AML) risks.

4.3 Regular Updates of KYC Information:

The Client will be periodically prompted by banqo to revise the Questionnaire and supply additional documents, data and information linked to Know Your Customer (KYC) procedures. This is done to adhere to relevant legal regulations. Banqo will inform the Client of the request and allocate a timeframe for submitting the required materials.

4.4 Verification of Payment Transactions:

The Client must periodically (at least once a month) review the Account Statements to authenticate Payment transactions. If the Client identifies improper or unauthorized Payment operations, they are obliged to inform banqo within three months of becoming aware of such issues.

4.5 Reporting Unsanctioned Activities:

The Client must furnish banqo with all accessible information regarding any unauthorized access to the Account or any illicit activities conducted by third parties as a result of such unauthorized entry, as outlined in Clause 9.5.1 of the Terms and Conditions.

4.6 Assistance in Investigating Unauthorized Transactions:

The Client agrees to assist in the inquiry of unapproved or inaccurately executed Payment operations.

4.7 Engagement of Third Parties:

Banqo retains the authority to involve third parties, either partially or completely, in executing the Client's Payment order if the nature of the order demands it. If another Payment Service Provider (PSP) places the Payment order on hold, banqo isn't accountable for this action but will endeavour to comprehend the underlying causes.

4.8 Prohibited Activities While Using banqo Services:

- Failing to adhere to the terms of the Agreement, Supplements and legal regulations, including but not limited to Anti-Money Laundering (AML) laws.

- Infringing upon banqo's and third parties' rights to trademarks, copyrights, trade secrets and other intellectual property rights.

- Providing untrue, deceptive or inaccurate information to banqo or refusing to supply information or fulfill reasonable requests from banqo.

- Disseminating false, deceptive or inaccurate information about banqo and collaborative endeavors with banqo to third parties.

- Executing or accepting transfers of unlawfully obtained funds, when the Client is aware of or should be aware of their illegitimate source.

- Utilizing banqo's services in a manner that results in losses, liability, adverse legal consequences or harm to banqo's business reputation or associated third parties.

- Accessing banqo's Services from countries not approved by banqo.

- Spreading computer viruses and engaging in activities that could disrupt the functioning of the System, damage information or harm banqo's equipment.

- Taking deliberate actions that disrupt the provision of banqo's Services to the Client or others or impede the proper operation of the System.

- Organizing illegal gambling, illicit trading of commodities, currency (e.g., Forex), stocks, indices, options, exchange-traded funds (ETFs) and engaging in prohibited trades of restricted goods as stipulated by the law.

- Providing financial services or engaging in legally regulated trading activities in stocks, indices, commodities, currencies (e.g., Forex), options and ETFs without banqo's prior written consent. If such services are intended, the Client must hold a valid license from an EU member state or equivalent third country, monitored by competent authorities for adherence to these criteria.

- Conducting legal gambling, lotteries or other licensed activities without prior written consent from banqo. In case of such services, the Client must possess a valid license from an EU member state, monitored for compliance by competent authorities.

- Enrolling with fictitious or unauthorized names, using anonymous phone numbers or email addresses from third parties or external websites.

- Providing services that contravene the law or ethical standards.

- Accessing the System as an anonymous user (e.g., via proxy servers).

- Disclosing Account Security credentials and/or Payment instrument details to third parties or allowing others to use Services under the Client's identity.

4.9 Ramifications of Violation:

In the event of a client's breach or if banqo suspects potential breach of the aforementioned prohibitions or involvement in the activities listed in the Prohibited Activities clause, banqo reserves the right, at its complete discretion, to take various measures. These actions may include reversing Payment transactions, placing on hold or closing the Account, notifying relevant parties, initiating legal proceedings and pursuing damages.

4.10 Compensation for Losses:

The Client is obligated to compensate banqo for direct damages, penalties and other monetary penalties incurred due to the Client's failure to adhere to or violation of the terms, including clause 9.8 of the Terms and Conditions, resulting from the Client's fault.

4.11 Liability for Losses:

The Client assumes responsibility and agrees to indemnify banqo, fellow banqo Clients and third parties for losses sustained due to the utilization of banqo's Services and violations of the Agreement or its supplements.

4.12 Notice of Breach Actions:

Banqo will inform about actions taken or consequences imposed against the Client or banqo due to the Client's breach of the prohibitions mentioned in this agreement, unless legally restricted from doing so.

5. RISK ASSESSMENT AND RISK APPETITE

5.1 Risk Assessment Process

During the risk assessment process, the Company maps the risks of ML, TF and sanctions breaches related to the provision of virtual currency services. This involves:

- Identifying risk categories and factors contributing to higher or lower risks.
- Assessing the effects of mapped risks on the Company's activities.
- Analyzing potential risk-mitigating countermeasures, their feasibility and applicability.
- The risk assessment process is tailored to the nature, size and complexity of the Company's economic and professional activities. Proportionality and relevance are key principles guiding the selection of risk management measures.

5.2 Establishing Risk Appetite

Based on the risk assessment, the Company establishes its risk appetite, which includes:

- Determining lower and higher risk fields related to ML, TF and sanctions breaches.
- Defining the volume and scope of products and services provided.
- Developing a risk management model, including simplified and enhanced due diligence measures.
  The risk appetite considers risks the Company is willing to assume or avoid, qualitative and quantitative compensation mechanisms, planned revenue, capital reserves, reputation risks and legal implications arising from ML, TF or other unethical activities.

5.3 Documentation and Updates

The establishment of risk assessment and risk appetite is documented and may be submitted to regulatory authorities, upon request. These documents are periodically updated based on changes in the Company's activities, with updates occurring at least once every six months. Staff members are required to familiarize themselves with and adhere to these documents in their daily responsibilities.

5.4 Separate Documentation

The risk assessment and risk appetite are documented in separate documents to ensure

clarity and transparency in the Company's risk management practices.

6. DETERMINATION OF THE RISK PROFILE

6.1 Determination of Risk Categories and Factors

Prime Money Services Group Inc., operating under the brand name banqo (hereinafter referred to as the "Company"), assesses the risk profile of its Customers by considering various risk categories and factors that may increase or decrease these risks. These risk categories include:

a) Customer Risk:

Factors contributing to customer risk include:

- Legal form and management structure of the Customer.
- Status as a Politically Exposed Person (PEP) or Relative or Close Associate (RCA) of a PEP.
- Presence on international sanctions lists.
- Prior suspicions of money laundering or terrorist financing.
- Engagement in cash-intensive businesses.
- Provision of services to anonymous customers.
- Complexity of ownership structures hindering the identification of Ultimate Beneficial Owners (UBOs).

b) Geographic Area / Jurisdiction Risk:

Factors affecting geographic risk include:

- Compliance with international standards on anti-money laundering (AML) and combating terrorist financing (CFT).
- Crime rates and levels of corruption in the jurisdiction.
- Existence of sanctions or embargoes against the jurisdiction.
- Involvement in terrorist activities or support for terrorist organizations.
- The company recognizes geographic risk and actively addresses it by tracing the IPs of clients and cross-referencing this data with the KYC process. If a client originates from a country on a prohibited list or flagged as high risk based on the factors above, they undergo heightened scrutiny. This approach aligns with international AML/CFT standards and enhances the company's ability to mitigate potential risks associated with clients from high-risk jurisdictions.

c) Product, Transaction and Service Risk:

Factors influencing product/service risk include:

- Nature of services provided, such as virtual currency exchange or gambling services.
- Complexity and volume of transactions.
- Countries involved in transactions.
- Use of new payment methods or emerging technologies.

d) Communication or Mediation Channels Risk:

Risk associated with communication channels is affected by:

- Constant communication via various channels without consistent contact details.
- Lack of physical verification of customers.
- Use of representatives authorized by customers.
- Use of IP addresses and VPNs.

e) Systems and Technology Risk:

Factors related to systems and technology may increase or decrease overall risk, depending on the effectiveness of technological solutions in detecting and preventing suspicious activities.

6.2 Determination of the Customer's Risk Profile

Upon assessing the risk profile of our corporate Customers, the Company considers various risk categories and factors that contribute to increasing or decreasing risk levels. The risk profile is determined based on the information gathered through the application of due diligence measures. Customers are categorized into the following risk tiers:

1) Low (Tier 1) Risk:

- Customers Incorporated and operating in EU and EEA
- Low risk industries, such as retail, health care etc.
- Companies holding a License or Legal opinion or which do not require a License.
- Monthly transactions which fall within the financial means of the client.
- A long term Contractual agreement.
- Residence and citizenship of the UBOs and Directors in EU and EEA

- UBO and Directors are not PEPs
- Neither the Customer nor its UBOs and Directors are sanctioned.

2) Medium (Tier 2) Risk:

- Customers Incorporated and operating in countries which are outside the EU and EEA but are not high risk or prohibited jurisdictions.
- Medium risk industries, such as Forex etc.
- Companies not holding a License or Legal opinion.
- Monthly transactions which fall within the financial means of the client but are close to the limit of what the client is processing.
- A long-term Contractual agreement.
- Residence and citizenship of the UBOs and Directors in countries which are outside the EU and EEA but are not high risk or prohibited jurisdictions.
- UBO and Directors are not PEPs
- Neither the Customer nor its UBOs and Directors are sanctioned.

3) High (Tier 3) Risk:

- Customers Incorporated and operating in countries which are high risk but not Prohibited.
- High risk industries, such as Real Estate etc.
- Companies not holding a License or Legal opinion.
- Monthly transactions which do not fall within the financial means of the client, they are slightly excessive compared to the company's activity.
- A long-term Contractual agreement.
- Residence and citizenship of the UBOs and Directors in countries which are high risk but not Prohibited.
- UBO and Directors are not PEPs
- Neither the Customer nor its UBOs and Directors are sanctioned.

4) Forbidden/Restricted:

- Customers Incorporated and operating in countries which are Prohibited.
- Prohibited industries, such as Illegal Activities, Weapons, Shell, Cannabis products, Adult Entertainment and Services etc.
- Companies not holding a License or Legal opinion.
- Monthly transactions which do not make financial sense.
- A onetime transaction.
- Residence and citizenship of the UBOs and Directors in countries which are

Prohibited.

- UBO and/or Directors are PEPs
- Either the Customer or its UBOs and/or Directors are sanctioned.

7. DUE DILIGENCE MEASURES

To mitigate the risks associated with money laundering (ML), terrorist financing (TF) and breaching sanctions, the Company implements a multi-level limit structure for incoming, outgoing and exchangeable funds for Customers. The Onboarding Team and Compliance Officer apply due diligence measures in several circumstances:

- Establishment of a business relationship
- Suspicion of ML, TF or breaching sanctions
- Doubts regarding the truthfulness or sufficiency of information/documents
- Verification of information or documents gathered earlier

The due diligence measures applied by the Onboarding team and overseen and verified by the Compliance Officer, include:

- Identification and verification of the Customer's identity
- Identification and verification of the Directors' identity
- Identification of the Ultimate Beneficial Owners (UBOs)
- Identification of the UBOs' Source of Wealth
- Acquisition of information about the purpose and nature of the business relationship and transactions
- Identifying whether the Directors or UBOs are Politically Exposed Persons (PEPs)
- Understanding the business relationship
- Identifying whether the Customer, Directors or UBOs are subject to sanctions
- Constant monitoring of the business relationship and transactions
- Identification of the source and origin of funds used in transactions

These measures are divided into two categories based on when they are applied:

- Before accepting a Customer and establishing a customer relationship (Category A)
- During a Customer relationship (Category B)
- The purpose of Category A measures is to establish a customer relationship based on the Customer's risk profile. Category B measures focus on monitoring transactions to ensure they correspond to reasonable expectations and assumptions concerning the Customer and their activities and updating Customer information.

The Onboarding team must pay special attention to transactions indicative of ML and TF, including complex, high-value and unusual transactions. The due diligence measures depend on the Customer's risk profile, which is determined based on information provided by the Customer and other factors. The Know Your Customer (KYC) principle is crucial, requiring the gathering of relevant information and data on the Customer to assess transaction patterns and identify suspicious activities.

The Company updates Customer data regularly, with higher-risk Customers requiring more frequent updates. The Know Your Customer principle is applied by providing Customers with questionnaires to collect additional data and analysing the submitted data to assess changes in activities and adjust risk profiles accordingly. The Onboarding team and Compliance Officer play key roles in applying these measures and ensuring compliance with regulations.

7.1 Identification of a Legal Entity

After a potential Customer expresses their intention to engage with the Company, the Onboarding team sends them the necessary information and data required for onboarding. When identifying a Customer, it's crucial to identify both the legal entity itself and its representative(s).

The Company handles the identification and verification of the Customer internally.

The following KYB data and information must be submitted to the Company via questionnaire by the Customer:

- Company name
- Country and Date of Registration
- Registration Number
- License number (if applicable)
- Tax Number
- Website
- Business Activity
- Company contact details
- Registered and Operational Address (if different to Registered Address)
- 'Names and contact details of Directors, UBOs and the Signatory (as described previously)
- Information on whether the Customer's Directors or Ultimate Beneficial Owner (UBO) is a Politically Exposed Person (PEP)
- Purpose of establishing the business relationship
- Operation details, such as turnover, customer details, countries of operation
- Transaction details

,

The following documents must be provided, recent (issued less than three months ago) or recently notarized/apostilled (within the last three months):

- Articles of Incorporation
- Business Registry Certificate
- Company License (If applicable)
- Certificate of Incumbency
- Shareholders & Directors Certificate
- Company Structure
- Business Proof of Address
- Proof of Domain Ownership (This doesn't require notarization)
- KYC/AML Policy (This doesn't require notarization – the document must be the most recent version)

In the event of Shareholders or Directors of the Customer being Legal Persons, the same documentation and information are required and the same procedures (KYB and KYC checks) are applied to them. This process continues for all Legal Persons in the structure.

7.2 Identification of a Natural Person

The Company utilizes the KYC services of an Automated Vendor for identifying and verifying the identity of Directors, UBOs and Signatory. The Company does not conduct face-to-face identification, instead conductions live verifications through the KYC Automated Vendor. If the information gathered during identification cannot be verified by the KYC Automated Vendor the Company prohibits the establishment of a business relationship. Cooperation with Customers unwilling to update their required identification data may not be continued.

To identify a natural person, the following data and information must be provided by the Customer:

- Name
- Date of Birth
- Place of residence
- Nationality
- Contact details (email address, phone number)
- ID or Passport information
- Information on whether the Customer is a Politically Exposed Person (PEP)
- Source of Wealth information (only applicable for UBOs)

- % of ownership (only applicable for UBOs)

Identification and verification of a natural person's identity are based on an identity document. The Company utilizes the services of a KYC Automated Vendor for this process. The following valid documents are requested:

- Photo of a Valid Passport or ID, taken with a mobile phone
- Proof of Address (e.g. Utility Bill, Bank Statement, Tax Declaration etc) Less than 3 months old

The Onboarding team is responsible for updating the Customer's personal data and operation profile, ensuring they are up-to-date. Updates are required at least twice a year for all Customers, starting from the Customer onboarding. The Onboarding team receives notifications in the System for updating deadlines.

7.2.1 Process of Verification of a Natural Person through KYC Automated Vendor

The Directors, UBOs and Signatory are identified using information technology means by KYC Automated Vendor. The KYC Automated Vendor adheres to relevant laws related to privacy and data processing, such as GDPR.

For all Customers, the following must be submitted for identification and identity verification:

- A liveness check is requested. This includes a Biometric analysis of an Applicant's facial movements compared with photographs on the submitted identity documents in order to ensure that the Applicant is alive and present at the time of the identity verification.
- A clear copy or digital copy of a recent Utility Bill (less than three months old)

For medium-risk (Tier 2) or high-risk (Tier 3) Customers, all the requested documents must be provided notarized and dated within the last three months within the scope of Enhanced Due Diligence.

With the questionnaire sent to a Customer by the Onboarding team, the legal representative/signatory declares:

- Accuracy and completeness of the data provided, acknowledging the consequences of providing false or misleading information.

- That they will provide any requested documents and information as required for the safe onboarding.
- That the Customer or associated companies or UBOs, Directors, Secretaries or Shareholders have not been sanctioned, negatively listed, declared bankruptcy etc

The KYC Automated Vendor screens against the below lists:

- OFAC Economic Sanctions Program
- EU Sanctions List
- FATF (Financial Action Task Force)
- UK/HMT Sanctions & OFSI (Office of Financial Sanctions Implementation)
- UN Consolidated Sanctions List
- US/US Treasury Sanction Lists
- Any other lists that the Vendor screens against.

7.3 Identification of the Ultimate Beneficial Owner (UBO)

- Direct Ownership: A natural person holds at least 25% or an ownership interest in a company.
- Indirect Ownership: A company controlled by a natural person holds at least 25% in another company.
- If no natural person holds or identifiably controls more than 25%, information about shareholders, partners or other persons exercising control must be requested.

Identification Process for UBO of Legal Entities:

- Customer submits a valid legal document of the company with shareholder/UBO data, notarized where necessary.
- The Onboarding team verifies the submitted documents/data.
- If necessary, supporting documents are requested.
- If submitted documents don't explicitly indicate the UBO, relevant information is registered based on documents.
- The Onboarding team verifies the submitted data through reasonable measures, such as checking registers or requesting annual reports.
- The Onboarding team must know the UBO and understand the ownership/control structure. The UBO's identification must be verified by the Compliance Officer before establishing a business relationship.

It is prohibited to begin a Business Relationship with a Customer if:

- UBO cannot be identified.
- Ownership/control structure is complex/incomprehensible.
- UBO is a PEP.

In addition to the previous, all UBOs who have been identified must provide Source of Wealth information in the form of a questionnaire.

Information requested in the Source of Wealth Questionnaire is:

- Source of Wealth (Employment, Loan, Company profits etc)
- Total Net Worth
- Companies in which they hold over 25% interest.

In addition, the UBOs must declare in writing on the Questionnaires that:

- They have not been convicted, bankrupt, investigated, connected to sanctioned entities, they are not PEPs.
- They confirm the accuracy of the information.
- That they will provide any requested documents and information as required for the safe onboarding, etc.

For high-risk (Tier 3) Customers further proof of Wealth is requested in the form of Bank statements, employment agreements, tax declarations etc within the scope of Enhanced Due Diligence.

Further to the previous, the Customer must provide information in the form of a questionnaire regarding their own AML/TF Policies and procedures. The most recent AML Policy document is requested and further information may be requested as necessary.

8. ENHANCED DUE DILIGENCE MEASURES

Enhanced due diligence measures are implemented to effectively manage and mitigate the higher risk of money laundering (ML) and terrorist financing (TF). These measures are applied to High Risk Customers (Tier 3). Enhanced Due Diligence is applied for all high-risk customers but can also be applied even for low-risk or medium risk customers if there are indications of being high-risk.

8.1 Documents and information requested from Tier 3 (High-Risk) Customers:

In addition to the documents and information requested for Tier 1 and 2 (Low and Medium Risk) Customers (KYB and KYC), the documentation provided will require to be recently notarized/apostilled (within 3 months) and further information and documentation will be required for the Source of Wealth of a UBO or the Company.

Further information may be requested as necessary.

Approval from the MLRO is required before onboarding High Risk – Tier 3 clients. This ensures that the decision to onboard such clients follows the regulations of the responsible compliance authority.

For any High Risk – Tier 3 clients that are onboarded, they are subject to ongoing Enhanced monitoring, which includes ongoing transaction monitoring, daily re-checks of risk scores via KYC Automated Vendor and immediate notifications if risk levels increase or if the client is listed in any blacklists. The monitoring system is customizable and can be adjusted based on the individual client's risk profile and activity.

8.2 Factors Triggering Enhanced Due Diligence Measures:

EDD triggers are any factors contributing to the customer being classified as Tier 3 – High Risk. These can be geographic location, high risk industry etc.

Also, transactions flagged as suspicious are triggers for EDD.

9. APPROVAL – REJECTION OF CUSTOMERS

Following the examination of all provided documents and information, the Onboarding Specialist fills out a Customer Acceptance Form where he summarizes in key information of the Customer.

Information included is:

- Company Name
- Country of Registration
- Countries of Operations
- Industry
- Whether all questionnaires and documents were sent and were valid
- Whether the KYC Automated Vendor checks were clear
- The existence of risk factors
- The subsequent Customers Risk Level – Tier
- Comments and Mitigating Factors

The Onboarding Specialist then provides the form to the MLRO who is responsible for examining it and ultimately approving or rejecting the Customer in writing on the form.

- Only the MLRO can provide approval to onboard High Risk -Tier 3 Customers. This ensures that the decision to onboard such clients follows the regulations of the responsible Compliance authority.

- Any High Risk - Tier 3 clients that are onboarded, are subject to ongoing Enhanced monitoring, which includes ongoing transaction monitoring, daily re-checks of risk scores via the KYC Automated Vendor and immediate notifications if risk levels increase or if the client is listed in any blacklists.

10. ONGOING MONITORING AND REASSESSMENT

The KYC Automated Vendor conducts daily automated checks for the reassessment of customer risk profiles and informs the Company immediately if risk levels increase or if the client is listed in any blacklists.

Customer's KYB and KYC information is requested and reassessed no later than six months after establishing the business relationship. For High Risk – Tier 3 Customers, review periods may be shortened.

To update data, the Onboarding team follows these steps:

- Sends the Customer a questionnaire via email and reviews the answers received.
- Verifies data on the KYC Automated Vendor.
- Contacts the Customer to request a valid document upon document expiry.

11. PERSONS SUBJECT TO INTERNATIONAL SANCTIONS & PEPs

The KYC Automated Vendor is used to identify Customers, Directors, UBOs and Signatories subject to sanctions and Directors, UBOs and Signatories who are Politically Exposed Persons (PEPs). If identified, the Company will not establish a business relationship with the Customer.

If the KYC Automated Vendor, during the Ongoing KYC monitoring, identifies a sanctioned person or PEP in the structure or a transaction of an already onboarded Customer, then the MLRO must collect additional information, terminate the business relationship and, if necessary, report to Authorities.

12. TRANSACTION MONITORING

12.1 Identifying the Purpose of a Business Relationship and Transaction

The Onboarding team identifies the purpose and nature of a business relationship and transaction using the following data:

- Warranties given by the Customer upon establishment of the business relationship or making of the transaction.
- Data received on the Customer's operation profile and field of activity.

12.2 Monitoring a Business Relationship

The Onboarding Team and Compliance Officer regularly monitor the business relationship with the Customer to ensure transactions correspond to the Customer's risk profile. Monitoring includes:

- Monitoring transaction size and frequency, identifying the origin of assets used in the business relationship or transactions when necessary.
- Verifying that the Volume of Monthly Transactions falls within the financial means of the Customer.
- Checking the Customer's legal status, financial situation and field of activity when necessary.
- Verifying ownership information.

During the ongoing KYC and KYB monitoring the Customer is sent a questionnaire at least every six months for all Customers.

The questionnaire verifies changes in risk data (e.g., geographic risk, field of activity) and updates the Customer's risk profile.

If the Customer doesn't provide required information or refuses, the Company terminates the client agreement and notifies the Authorities.

12.3 KYC and KYT monitoring

KYC and KYT monitoring aims to identify suspicious/unusual transactions, transactions exceeding limits, PEPs, subjects of international sanctions and adverse media coverage. The Company's Automated KYC and KYT Vendor tools are used for monitoring.

Ongoing Automated KYC Monitoring Parameters:

- Changes in Customer's status regarding PEP.
- Changes in the status regarding international sanctions.
- Changes in the status regarding Adverse media coverage.
- Screening is done daily and alerts are generated for further investigation. The Compliance Officer investigates alerts, coordinating next steps with the MLRO.

The Company does not allow any crypto or fiat transactions without first fully verifying the identity of the Customers through the KYC Automated Vendor tool, in addition to having completed the rest of the onboarding procedure.

All transactions are monitored and assessed in real time using the KYT Automated Vendor. If a transaction is flagged as pending in the system then the account of the customer will be frozen until the appropriate EDD has been conducted. The MLRO conducts the examination and if necessary, the account is closed and he reports to the Authorities.

Enhanced Due Diligence conducted will include the examination of source of funds, as well as any other information and documents are required.

Specifically:

- Source: Reason, explanation and legal relationship basis for transferring funds.
- Origin: Activity with which funds were earned or received.
  Identification of source and origin depends on various factors including transaction size, correspondence with known Customer information and suspicion of criminal activities.

12.4 Transactions with Politically Exposed Persons (PEPs)

The Company shall not establish a Business Relationship with a Customer found to be a PEP and/or related to a PEP during the KYC checks.

The KYC Automated Vendor is used to identify PEPs.

The Company shall terminate the Business Relationship with a Customer found to be a PEP and/or related to a PEP during ongoing KYC monitoring.

If, during KYC monitoring, a Customer involved in a transaction is found to be a PEP

and/or related to a PEP, the transaction is placed on hold – unless in extreme situations it's objectively impossible. If placing a transaction on hold is impossible, we promptly notify the Authorities.

12.5 Ongoing Transaction Monitoring

Banqo uses a KYT Automated Vendor tool for ongoing, real-time transaction monitoring. All transactions are continuously monitored and as soon as a suspicious transaction is identified, it is placed on hold and reported to the MLRO. The MLRO then examines the case, requests EDD and fills out an Internal Suspicious Activity Report and, if necessary, reports the incident to the Authorities.

12.5.1 Transactions Monitoring Systems

The KYT Automated Vendor tool has systems and practices in place to monitor transactions in real time.

- Transaction Monitoring: They monitor transactions to estimate associated risks. This involves checking a wide range of currencies and setting corresponding alerts for certain transactions.

- Custom Rules: They provide the capability to implement custom business logic, allowing us to create fraud prevention rules tailored to our specific business needs. These rules are automatically applied to transactions to determine if they match the rule parameters.

The Automated KYT Vendor includes advanced IP address checks. The Fraud Network Detection tool employs AI and machine learning to monitor and control various forms of financial crime.

Key features include:

- Network Analysis:

  - Prevent Multi-Accounting: Detects multiple accounts from the same IP or device.
  - Deepfake and Mule Detection: Identifies deepfakes and mule accounts through network analysis.

- Traffic Monitoring and Bot Detection: Assesses geographical patterns, device fingerprints and behavioural nuances to distinguish genuine users from fraudulent activities, including bot farms.

➢ Advanced IP Check:

- IP Risk Assessment: Checks the IP address for risk factors, revealing the applicant's location and whether a VPN, proxy or TOR is used.
- Risk Labels: IP addresses are labelled as safe (green), suspicious (yellow) or risky (red) based on the detected risk.

➢ Implementation and Monitoring:

- Networks are calculated daily for active clients and results are accessible via API and Dashboard, showing detailed fraud network information.

The KYT Automated Vendor screens against the below lists:

➢ OFAC Economic Sanctions Program
➢ EU Sanctions List
➢ FATF (Financial Action Task Force)
➢ UK/HMT Sanctions & OFSI (Office of Financial Sanctions Implementation)
➢ UN Consolidated Sanctions List
➢ US/US Treasury Sanction Lists
➢ Any other lists that the Automated KYT Vendor screens against.

12.5.2 Transaction Monitoring Process

The automated KYT Vendor monitors and verifies transactions and provides advanced IP analysis.

1. Geolocation Analysis:

- Advanced IP Analysis: The Automated KYT Vendor provides advanced IP analysis to determine the geographic location of users, identifying if access is from sanctioned or prohibited areas. This includes detecting the use of VPNs or proxies to mask true locations.
- The risk level associated with transactions is assessed based on the involved countries, ensuring no links to high-risk jurisdictions.

2. Machine Learning and AI Integration:

- AI-driven anomaly detection identifies patterns that may indicate attempts to evade sanctions or conduct illicit activities.
- Pattern recognition algorithms enhance the overall effectiveness of compliance checks.

12.5.3 Rules

The KYT Automated Vendor, facilitates automated rule-setting to monitor and assess transactions in real time. This ensures compliance with regulatory obligations and helps identify any links to illicit activities.

The KYT Automated Vendor implements the following rules:

- Large Amount Trigger: Transactions exceeding 2,000 EUR automatically add 30 points to the risk score.
- High-Risk Countries: Transactions involving high-risk countries add 30 points to the risk score.
- Frequent Transactions: If the same remitter or beneficiary conducts more than 7 transactions within 7 days, an additional 30 points are added to the risk score.
- Recurring Payments: When more than 2 outbound transactions to the same beneficiary within 30 days, each exceeding 2,000 EUR, are identified with identical payment details, 30 points are added.
- Duplicate Payment Methods: Transactions using duplicate payment methods are automatically rejected.
- Multiple Payment Methods: Transactions involving more than 4 different payment methods are rejected.
- On-Hold Transactions: Any transaction that reaches or exceeds a total risk score of 30 is put on hold for further review by the compliance team.

A transaction is automatically rejected in the following cases:

- It involves a PEP, a sanctioned individual or entity
- It involves a prohibited/sanctioned geographic area

12.5.4 Risk Parameters

The transaction risk parameters align with the Company's business risk assessment and risk appetite by considering various risk categories, such as geographic risk, industry risk and size of transaction risk among others. If a transaction is made which alters the risk score in any of the above categories, then the customers entire risk scoring is reassessed.

The KYT Automated Vendor shows the transaction address and estimates the risk level and risk score for a particular transaction. The Risk level and Risk score values are shown as follows:

- A score from 0 to 0.25 indicates the Low value in the Risk level field.
- A score from 0.25 to 0.6 indicates the Medium value in the Risk level field.
- A score from 0.6 indicates the High value in the Risk level field.

The following information illustrates the response types that can be provided in the results:

- Child Exploration: An organization which operates via darknets and is suspected of child abuse and exploitation.
- Enforcement Action: An entity is subject to legal proceedings. Jurisdiction will be annotated as a subtype.
- Exchange Fraudulent: Exchange that was involved in illegal activity.
- Exchange Licensed: An organization that is licensed to provide exchange services.
- Exchange Unlicensed: An organization that is not licensed to provide exchange services.
- Gambling: An online resource offering gambling services.
- Illegal Service: A resource offering illegal services or engaged in illegal activities.
- Marketplace: An entity offering legal services/trading goods.
- Payment Processor: A service which acts as an intermediary between customers and the company which provides services for making a payment.
- Ransom Extortioner: Extortioners demand payment.
- Sanctions: An organization that is found in sanctions lists.
- Terrorism Financing: An organization which operates via darknets.
- Other: None of the specified entities above. It may include a subtype.

12.6 Internal Suspicious Activity Report (SAR) Procedure

The Internal Suspicious Activity Report (SAR) procedure is a crucial component of the Company's compliance framework. This procedure ensures that suspicious activities are identified, documented and reported in accordance with regulatory requirements. Below is a step-by-step guide to the SAR procedure:

1. Identification of Suspicious Transactions

Banqo uses a KYT Automated Vendor tool. Monitoring of transactions through the above vendor is ongoing and in real time.

Once a suspicious transaction is flagged by the KYT Automated Vendor tool, the transaction is immediately placed on hold. The Compliance Officer notifies the MLRO.

2. Investigation

Enhanced Due Diligence is performed. A thorough investigation is conducted by the MLRO to gather more information about the suspicious activity. This includes requesting Source of Funds documentation, reviewing transaction logs, customer profiles and KYC, communication records etc.

3. Reporting

An Internal SAR is prepared. This report includes all relevant details such as customer information, the nature of the suspicious activity, findings from the investigation and recommended actions.

The internal SAR is signed by the MLRO.

- If the outcome of the EDD and the Investigation clears the transaction from ML/TF suspicions, the MLRO will permit the transaction to continue and note it on the Internal SAR.

- If the outcome of the EDD and the Investigation confirms the ML/TF suspicions or remains inconclusive, the MLRO proceeds to note it in the Internal SAR, instruct the transaction to be rejected (funds will be returned), the account to be frozen, cease the business relationship with the Customer and submit a report to the Authorities.

A suspicious transaction is automatically rejected in the following cases:

- It involves high risk and blacklisted bank/EMI accounts
- It involves a PEP, a sanctioned individual or entity
- It involves a prohibited/sanctioned geographic area

In these events, the MLRO will prepare the Internal SAR and report to the Authorities, without the investigation and EDD step. The account will be frozen, funds will be returned and the business relationship will be ceased.

In the extreme event that the transaction cannot be placed on hold, for reasons outside the Company's control, the MLRO must promptly notify the Authorities.

The SAR procedure is periodically reviewed and updated to reflect changes in regulations, emerging risks and lessons learned from past cases.

Information to be noted by the MLRO in the Internal SAR includes the following:

- Customer Name;
- Contact Info;
- Details of suspicious transaction;
- Automated KYT Vendor report;
- Recommendations for Action (freezing account, EDD etc);
- Results of EDD and Investigation;
- Final recommendations after the EDD and Investigation (Reporting to the Authorities or Release of account and continuation of Transaction) etc

12.7 Reporting to the Authorities

The MLRO must fill in seven information areas when submitting reports to the Authorities:

1. Author of the report
2. Report
3. Parties
4. Transaction
5. Documents
6. Submission

The MLRO retains all reports received from the Onboarding team and Compliance Officer about suspicious and unusual transactions, along with any information collected for analysis and forwards these reports to the Authorities along with information about the time of forwarding.

It is strictly prohibited to notify a Customer or a person participating in a transaction about whom a suspicion is being communicated to Authorities.

13. COLLECTION, VERIFICATION AND RETENTION OF DATA

The Company diligently collects and retains data on customers gathered during the performance of due diligence measures. The data is registered and stored on the Company's Cloud Server.

The Company retains digital copies of documents used for identification and verification, as well as documents establishing a business relationship, for five years after the termination of the business relationship. This allows for immediate responses to inquiries from the Authorities regarding past business relationships.

Data and documents on customers and their transactions are stored in a folder system,

categorized by natural and legal persons and then by name, ensuring efficient organization and retrieval of information.

Staff members are required to retain various documents and data, including identity documents, responses to database queries, customer questionnaires and reports on suspected ML. This information is stored securely on a virtual server leased from Microsoft Azure, with strict adherence to GDPR regulations.

Personal and financial data, including sensitive information such as passport details, account numbers and authentication data, are treated as confidential. The Company ensures the protection of personal data and limits access to relevant staff members authorized by the Management Board.

We retain personal data only for as long as necessary in order to deliver the services you request, fulfil legal, accounting or reporting obligations and provide you with reasonable access to your data. The personal data we collect is used for various purposes, each governed by specific standards and regulations and various factors are evaluated to determine their retention period.

Before establishing a business relationship, customers are informed about the processing of their personal data and sign declarations to this effect which are included in the questionnaires provided during the onboarding process.

Principles adhered to during data collection, processing and retention include lawfulness, minimalism, data quality, limited retention and security. Any questions regarding data collection, retention, processing or deletion should be addressed to the MLRO.

The business relationship may be commenced only where all risks of ML and TF correspond to the Company's risk appetite or can be reduced to an acceptable level by applying countermeasures. The Risk Scoring Forms and Customer Acceptance Forms are documented and kept on Company's server.

14. ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS

The purpose of the Risk Assessment is to identify, assess and analyse the exposure of the Company to the money laundering and terrorist financing risks in its business activities or for any new services, products or sales channels or emerging technologies they might adopt in the future.

As a result of the Risk Assessment, the Company establishes fields of lower and higher risk of money laundering and terrorist financing; the risk appetite, including the volume and scope of products and services provided in the course of business activities; and the risk

management model, including regular and enhanced due diligence measures, in order to mitigate identified risks.

Before introducing new services, products or sales channels or adopting emerging technologies, the Management Board conducts a thorough assessment of related risks concerning money laundering (ML) and terrorist financing (TF).

The methodology used in the Risk Assessment is developed taking into account the size, the number of clients and products offered and also the business structure of the Company. The methodology used in the Risk Assessment enables to first identify and categorise the ML/TF risks and second, classify the ML/TF risk in the Company for the specific risk factor on the scale of low, medium and high risk.

By following this structured approach, the Company ensures that new services, products or technologies are introduced responsibly, with careful consideration given to mitigating ML and TF risks in line with its risk appetite.

The main risk factors of the Company have been identified taking into consideration the FATF guidance for a risk based approach and the high risk factors in the Canadian AML Act, EFSA Guidance, other Regulations as stated in the Internal rules for preventing of ML/FT as well as any relevant information that the Company would be aware of. In the Risk Assessment ML/TF risk is only assessed for the risk factors which are relevant to the business model and products of the Company.

The ML/TF risks that have been currently identified by the Company have been classified under one of the following categories:

- Risks factors relating to the characteristics of the clients of the Company; Risks factors relating to the characteristics of the Company's products and services: including the level of transparency of the services offered, the complexity and the value or size of the transactions;
- Risks factors relating to the countries and geographic areas involved in the Company's activities;
- Risks factors relating to the distribution channels: including the free services and the potential use of intermediaries such as agents.

The Company takes into account the factors of higher ML/TF risks, for example:

- Customers: unusual circumstances surrounding the business relationship, forged documents; Product and distribution channel: products or transactions that might favour anonymity, non-face-to-face business relationships or transactions, without

certain safeguards, such as electronic signatures, payment received from unknown or non-associated third parties, new products and new business practices, including new delivery mechanism and the use of new or developing technologies for both new and pre-existing products;

- Countries or Geographical area: Countries identified as not having effective AML systems, countries identified as having a high level of risk of corruption or criminal activity, countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations, countries designated by FATF as high-risk, countries providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country.

The relevant risk factors for the Company are:

Geographic risks:

- cross-border activity and global reach; (including transactions in high-risk areas);
- complications with identifying the origin of funds.

Risks related to products, services, transactions and channels:

- online service provision (including transactions in the dark web);
- speed and volume of the transactions;
- problems with the monitoring systems (unable to detect flows of funds which have criminal background).

Risks related to Clients:

- non-face-to-face identification;
- politically exposed persons (PEPs) or Related person of PEP;
- non-residents;
- business relationship foundations based on unusual factors.

Risks related to the regulative environment, including the ability to carry out supervision:

- under-regulation of the area (the development of the area is ahead of the regulatory environment);
- global fragmentation of the regulations (different requirements and definitions worldwide);
- cooperation between service providers and regulators (service providers would prefer further cooperation with the regulators and more efficient trainings).

The Company employs stringent measures of KYC and KYT monitoring to counter the abovementioned risks.

15. RESPONSIBILITIES AND RIGHTS OF THE MLRO

The MLRO must:

1. Analyse suspicious transactions and Customer activities reported by the first line of defence.
2. Act as a liaison between the Company and the Authorities regarding compliance with ML and TF prevention requirements.
3. Prepare and sign off on the Internal SAR.
4. Report to the Authorities when necessary.
5. Exercise the right to examine, place on hold (freeze) or close any Customer account.
6. Implement the Rules.
7. Supervise Staff, assess their performance and take appropriate actions based on assessments (e.g., arrange additional training, redistribute responsibilities, terminate contracts, etc.).
8. Maintain records of Staff supervision activities.
9. Provide training to Staff or new members as requested by the Management Board.
10. Report directly to the Management Board on risk management or compliance issues and inform them of other emerging situations during Company operations (e.g. suspicious transaction reports, unusual activities, fraudulent accounts, etc.).

The MLRO has the right to:

1. Propose amendments to the Rules to the Management Board.
2. Request that Staff rectify identified deficiencies in Rule implementation within a reasonable timeframe.
3. Receive necessary data and information for fulfilling duties.
4. Receive training.
5. Examine, place on hold (freeze) or close any Customer account without explicit prior approval from the Management Board if necessary.

16. TRAINING REQUIREMENT

All Staff members whose job responsibilities involve interacting with Customers, establishing and monitoring business relationships, analysing and reporting to the Authorities, executing transactions and retaining data must adhere to the Rules.

The Management Board ensures that Staff responsible for due diligence receive regular training covering:

1. Company obligations under the Regulation.
2. Modern identification methods.
3. Monitoring and screening of business relationships.
4. Identification of individuals subject to sanctions, PEPs and RCAs.
5. Data collection and retention.
6. Risk assessment.

Training sessions are conducted at least annually or more frequently if needed. The MLRO maintains records of training sessions, including the date, participants, topic, duration, trainer and materials used.

New Staff members must complete training before commencing duties related to due diligence and Customer identification, within one month of starting employment. The Management Board or another qualified person introduces the Rules to new employees within one week of their start date and employees confirm their understanding by signing.

When amendments are made to the Rules, they are communicated to relevant Staff within two weeks. Staff members affected by the amendments confirm their understanding by signing. The MLRO ensures that all new Staff and those affected by Rule amendments have confirmed their understanding and follows up with those who have not.

17. OVERSIGHT AND INTERNAL CONTROL MEASURES

The Management Board member responsible for AML, the MLRO and the internal auditor are tasked with ensuring compliance with the Rules. The MLRO reviews the AML Policy annually and updates it as needed. The Management Board notes the deadline for the next review when making amendments. The Management Board is responsible for analysing monitoring results, ensuring compliance and assessing Staff training needs.

17.1 Staff Screening Procedure

The MLRO conducts ongoing screening of Staff involved in customer communication, business relationship establishment, transactions and due diligence measures. At least 8 hours per month are allocated for screening.

For first-line defence employees, the MLRO assesses Rule application efficiency by reviewing activities related to a selected group of Customers monthly. Screening includes:

1. Confirmation of relevant training completion
2. Understanding of Rules application through appraisal interviews

3. Assessment of duties performance, including KYC processes
4. Regular inspection of Staff documentation and Customer communication

The MLRO provides guidance to Staff on non-routine queries and delivers feedback or disciplinary measures for inadequate performance. Performance reports are prepared biannually and presented to the Management Board, detailing inspection procedures, measures and results analysis.