Verum Coin (VERUM)

AML & KYC Policy

February 2025

Website: https://verumcoin.info

Email: support@verumcoin.info

TABLE OF CONTENTS

1. INTRODUCTION

This Manual, has been approved by the Board Members of Verum Messenger LTD[1] for the purpose to provide internal guidance to Verum Coin Project shareholders, management and employees in general regarding the necessary procedures to ensure absolute compliance with the local and international KYC/AML regulations, in accordance with the Money Laundering and Terrorism Financing Prevention Act[2] and other related regulation.

Overseas subsidiaries will be governed by the Anti-Money Laundering and Know Your Client laws, regulations and guidelines dictated by the respective resident countries. Where there are no legal or regulatory guidelines of the resident countries for specific areas considered critical to the AML & KYC program, this Manual document should be adopted for those specified areas of operations.

1.1. Manual Objectives

The Board Members and Management of Verum Coin Project are committed to ensuring the highest ethical and professional standards while conducting our business activities. Verum Coin Project is therefore committed to knowing its clients as well as their banking and investment activities, adopting sound business practices that will detect and identify unusual activities in a timely manner.

One of the objectives is to protect Verum Coin Project's reputation and therefore protect itself from being used as a vehicle for or victim of any illegal activities committed by its clients. In order to achieve this goal, we are focused on developing standards to ensure the highest priority is given to achieving compliance with the relevant regulations and guidelines.

The primary objectives are:

1. To ensure compliance with the AML Act, the EU AML Directives, and other laws impacting Verum Coin Project's compliance obligations and this manual.
2. To protect the reputation and integrity of Verum Coin Project by implementing adequate controls and systems to prevent the possibility of the products and services of Verum Coin Project being used as vehicles for illegal activities.
3. To ensure that all team members are aware of and understand the issues in relation to money laundering and the financing of terrorism and their responsibilities and obligations under the policies of Verum Coin Project and the regulations.
4. To ensure that all team members will be able to recognize suspicious transactions, understand how to report such transactions, and be aware of the penalties and sanctions for non-compliance.
5. To ensure compliance with data protection and privacy regulations, including the General Data Protection Regulation (GDPR), by implementing appropriate data transfer mechanisms when handling personal data outside the European Economic Area (EEA). Verum Coin Project adopts Standard Contractual Clauses (SCCs) as recognized by the European Commission to ensure the lawful transfer of personal data to third countries. These SCCs provide contractual guarantees that protect data subjects' rights and ensure compliance with GDPR principles regarding data security, transparency, and accountability.

1 Hereinafter „Verum Coin Project"

2 Hereinafter „AML Act"

By integrating these measures, Verum Coin Project reinforces its commitment to regulatory compliance, data protection, and the highest ethical business practices.

1.2. Manual Overview

Verum Coin Project operates within the global financial services industry which is highly regulated and a key stakeholder in the fight against money laundering and terrorist financing activities. Verum Coin Project is committed to preserving its reputation through the implementation of programs, policies, and systems to strengthen its AML and Counter Terrorism Financing ("CTF") frameworks. As a regulated group of companies, Verum Coin Project acknowledges the importance of its role in ensuring the safety and soundness of its operations and furthering efforts to combat AML and CTF.

Estonia's regulatory framework continues to be strengthened with the introduction of new guidelines and regulations, expansion of the role and powers of enforcement agencies and revision to existing laws and regulatory guidelines. Failure to comply with these regulations may result in significant penalties or prosecution under the AML Act.

In an effort to protect Verum Coin Project against the possibility of being used for illegal activities, Verum Coin Project has established and implemented these policies and procedures applicable to all subsidiaries to prevent and detect money laundering and terrorist financing.

This Manual may change from time to time in response to new or revised regulations, in order to ensure the effectiveness and efficiency of Verum Coin Project's operations. This Manual is subject to annual review by the Board Members of Verum Coin Project.

The implementation of the AML, CFT and KYC policies and procedures are to ensure that reasonable assurance is given that the risk to Verum Coin Project from money laundering and terrorist financing is minimized.

1.3. Verum Coin Project AML Compliance Policy

Verum Coin Project is required to implement an effective AML compliance policy to ensure compliance with all laws, regulations, and guidelines in relation to AML and CFT. Verum Coin Project's AML compliance policy outlines the following areas, which are detailed further in this and other relevant sections of the policy:

- The documentation, verification and due diligence requirements for new and existing clients.
- The nature and frequency of account and transaction monitoring.
- The internal and external reporting framework for suspicious transactions.
- The frequency, nature and scope of AML compliance testing.
- The nature and scope of AML training.
- Compliance risk assessments for new products and services.

1.4. Verum Coin Project KYC Compliance Policy

Verum Coin Project is required to establish a KYC Policy which is a critical component in the achievement of AML compliance. This policy focuses primarily on client identification requirements, client due diligence, monitoring of accounts and identification of suspicious activity.

2. ROLES AND RESPONSIBILITIES.

The following outlines the roles and responsibilities of the Board Members, Management, the compliance department, and employees, who are critical to the AML and CFT program. The specific responsibilities for each group are as follows:

2.1. The Board Members

The ultimate responsibility for compliance with the AML and CFT policy and procedure lies with the Board Members. In order to fulfil its obligations, the responsibilities of the Board Members include:

- Approving the AML and CFT policy and any amendments thereto.
- Appointing a Compliance Officer.
- Requiring and reviewing compliance and audit reports indicating regulatory compliance as well as compliance with internal control and corrective measures instituted where necessary.
- Reviewing and recommending proposed amendments to this Manual.
- Reviewing internal and external reports of the AML and CFT program.
- Reviewing reports prepared by the compliance officer.
- Reviewing the results of the AML examinations, compliance reviews, audits and independent testing, as well as corrective actions planned or taken in response thereto.
- Monitoring on-going AML activities and issues by receiving and reviewing reports provided by the compliance department on a regular basis.

2.2. Management

For the purposes of this Manual, “Management” is comprised of Verum Coin Project’s Executive Team Leader and Senior Team Leaders. They are responsible for ensuring that:

- A strong culture of AML compliance is upheld among Verum Coin Project’s business and support units inclusive of subsidiaries.
- Each business unit takes ownership and is held accountable for implementing the AML Manual by integrating applicable components of the Manual into its business operations, (including KYC Policies), and that business units take corrective actions when breaches are identified.
- The compliance officer has access to required information and personnel.
- Roles and responsibilities relating to the AML policies are communicated by the compliance officer to all team members, that the Manual is observed, that the business

units have adequate team members to support the reasonable performance of the AML functions and responsibilities and that appropriate remedial or disciplinary action is taken if breaches are identified.

2.3. Compliance Department

Through the leadership of the compliance officer, the department provides company-wide AML oversight and support to Verum Coin Project business and support units in establishing and implementing procedures for compliance with the applicable AML laws and regulations and regulatory guidelines. The primary responsibilities of the Compliance Department include:

- Evaluating laws and regulations, with the guidance of external counsel, to determine their applicability to Verum Coin Project, its business units and subsidiaries.
- Performing company-wide risk assessments to identify and evaluate compliance risks and controls for detecting breaches with relevant laws, regulations and significant corporate policies, including with respect to proposed new products or services or significant variations on existing products and services.
- Developing and implementing appropriate compliance training and team member awareness programs.
- Providing guidance to business units on the applicability of laws, rules and regulations to new products.
- Reviewing clients requiring enhanced due diligence, including those classified as High Risk.
- Conducting routine and targeted compliance testing of the business units' related AML procedures and of other key units with AML responsibilities.
- Identifying, monitoring, and investigating any potentially suspicious activity identified by monitoring systems and referred by business units, and making the appropriate reports to the Designated Authority.
- Conducting investigation and verification of information for clients requiring Enhanced Due Diligence.
- Conducting initial client due diligence checks (i.e., OFAC, Politically Exposed Persons ("PEP"), and adverse searches), maintaining evidence of such checks.

2.4. Compliance Officer

The Compliance Officer is responsible for overseeing and managing the AML Program. All references to the Nominated Officer in this document should be interpreted to mean the Group Compliance Officer.

The Compliance Officer may be supported by the Compliance Team which is comprised of a Senior Compliance Manager, Compliance Analysts and a Legal and Regulatory Officer. The

Compliance Officer is responsible for:

- Being fully acquainted with the provisions of the AML and CFT regulations and its amendments in Estonia and EU regulations. He/she must, in particular, be cognizant of the confidentiality requirements with regard to reporting transactions.
- Remaining informed of the local and international developments on money laundering and industry best practices.
- The training of all team members with respect to the AML and CFT program and the applicable regulatory and legal requirements.
- Ensuring that all the companies within Verum Coin Project comply with the appropriate standards and procedures in place for AML and CFT Compliance.
- Ensuring that all team members are kept up to date on current legislative requirements both locally and internationally.
- Establishing a compliance plan which will include independent review and on-going testing of team members' compliance in order to achieve the Know Your Employee (KYE) requirements.
- Implementing programs, policies, procedures and controls to detect money laundering and terrorist financing activities.
- Establishing a reporting system whereby team members can report activities which are not in compliance with Verum Coin Project's policies without fear of reprisal.
- Producing monthly and annual board reports on matters of compliance to the Board Members and Executive Team.
- Ensuring that reports for Threshold and Suspicious Transactions are submitted to the Estonian Financial Supervision Authority[3] in a timely manner.
- Evaluating reports of Suspicious or Unusual Transactions and verify whether they are subject to reporting.
- Providing on-going training to the Compliance Analysts.
- Acting as liaison between Verum Coin Project and regulatory and law enforcement agencies with respect to all compliance matters and investigations.

[3] Estonian Police and Border Guard Board Financial Intelligence Unit (FIU)

- Ensuring that all exceptions are addressed and follow-up to ensure that corrective action is immediately instituted.
- Ensuring that adequate resources are in place to effectively monitor compliance.
- Evaluating new products and services to determine the level of risk and make appropriate recommendations.
- Liaise with Verum Coin Project's legal counsel on AML matters and investigations.

3. LEGAL & REGULATORY FRAMEWORK

3.1. Local legislation

- The Money Laundering and Terrorist Financing Prevention Act
- Requirements for the Rules of Procedure established by credit and financial institutions and for their implementation and verification of compliance.
- International Sanctions Act
- FIU Guidelines.
- EU regulatory framework
- EU IV anti-money laundering directive 2015/849;
- EU III anti-money laundering directive 2005/60;
- Implementing measures (directive 2006/70) for EU III anti-money laundering directive;
- Regulation (EC) No 1781/2006 of the European Parliament and of the Council on information on the payer accompanying transfer of funds;
- Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees;
- European Payment Council Guidance Notes on the implementation of the Regulation (EC) 1781/2006 on the information on the payer;
- 3rd country equivalence, common understanding between Member States, FSA Guidelines 2009.

4. ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM

4.1. Definitions

Money laundering may be defined as:

- The process and transactions conducted to make illegally acquired money look as if it were acquired legally;
- The handling of money in such a fashion in order to conceal its true source of origin;
- The process by which income of illegal origin is transformed into money which appears to have been legitimately earned or obtained.

The three basic stages by which criminals attempt to launder money are:

- Placement: Placing unlawful money into a financial and/or non-financial institution;
- Layering: Separation of unlawful money from the original source, through the use of layers of financial transactions. Layering would include such actions as transferring the principal sum into multiple smaller amounts, which are then converted into traveller's cheques, money orders or other valuable assets (jewellery, art and paintings etc.);
- Integration: Using apparently legitimate transactions to disguise unlawful cash. Financial

Institutions as providers of a wide range of services, are vulnerable to being used at all stages but are primarily used in the layering and integration stages.

Terrorist Financing

Financing of terrorism is a term used to describe the accommodating or facilitating of financial transactions that may be directly or indirectly related to terrorists, terrorist activities and/or terrorist organizations. In some cases, proceeds from criminal activities are used in funding terrorist organizations or activities. It should also be noted that terrorist funding may be generated from legal sources.

Business relationship

A business relationship, which is expected, at the time when the contract is established, to have an element of duration.

EEA

European Economic Area

Beneficial owner

A natural person that some other person acts for or, if the customer is a legal person, the party that exercises a decisive influence over the customer.

Risk-based approach

The current applicable regulatory framework emphasize the concept of a risk-based approach to combating money laundering and terrorist activities. Therefore, Verum Coin Project has implemented a risk-based customer due diligence process, and the scope of such measures are adapted according to each specific case with regards to risks of terrorist financing or money laundering.

The following definitions will be extremely helpful in understanding the risk-based approach:

- Undertaking means: the following activities engaged in by those natural and legal persons that operate:
- Banking or financial business under the relevant legislation.
- Life insurance businesses.
- Activities described in the Securities Market Act.
- Activities that require notification or application of the Estonian Financial Supervision Authority
- Insurance mediation.
- Activities relating to the issue of electronic money.
- Mutual fund activities.

Internal rules means: policy and governance documents, guidelines, instructions or other written documents through which the issuer governs the operation.

Internal control means: a process by which the undertaking's Board Members, managing

director, management or other personnel create reasonable certainty that the undertaking's goals are fulfilled in the following areas that:

- The undertaking has an appropriate and efficient organization and management of the operations.
- Information provided to the regulator is reliable.
- The undertaking complies with applicable laws, ordinances and other regulations.

4.2. Fulfilling the risk-based approach requirements

In order to fulfill the requirements of the applicable regulations, the Verum Coin Project shall undertake:

Conduct a risk assessment.

Maintain procedures, etc. in accordance with the law.

Monitor and update the risk assessment on an ongoing basis and, when needed, revise the procedures, etc.

4.3. Risk-based assessment

A risk-based assessment requires an analysis of an undertaking's products, services and customers, as well as other relevant factors as related to the undertaking's operations such as geographical regions and distribution channels of the undertaking's operations. The implementation of a risk-based approach requires that Verum Coin Project and its employees have a comprehensive understanding of relevant risks as well as the ability to exercise sound judgment. In order for this to occur, a creation of risk expertise must be formed through training, recruitment and on the job learning. Such risk based assessment processes will benefit greatly form information sharing amongst the Estonian authorities and Verum Coin Project.

An adequate risk-based mechanism will be designed so as to allow designated competent authorities to effectively assess and review the procedures adopted by Verum Coin Project so that such bodies can determine how Verum Coin Project manages risk and the degree of risks facing Verum Coin Project and there specific clients and transactions. Furthermore, relevant organizations must be capable of reviewing the determinations made by Verum Coin Project as a result of their risk-based assessment. A proper risk-assessment must also contain components addressing country-wide risks in an undertaking's operations as well as both Verum Coin Project's customer due diligence and internal control systems.

4.4. Record keeping

Record keeping is very important to the Anti-Money Laundering, Counter Financing of Terrorism & FACTA program as it provides valuable information for not only commercial considerations of each entity within Verum Coin Project, but also to assist the investigating authorities in accounts suspected of money laundering and financing of terrorism. Records should be maintained to facilitate easy

retrieval of relevant information without undue delay. Records should also be maintained for a minimum period of seven (7) years after the relationship has been terminated. Records should be maintained for a minimum period of six (6) years after a report has been made on a client and or account with respect to FATCA. Verum Coin Project may be required to extend the six year period if the IRS requests such an extension prior to the expiration of the six year period.

A static data file should be maintained for all clients. Such files will include the following minimum information:

- Completed account opening documents signed by the client
- Certified copies of incorporation documentation and records of client identification (KYC documents)
- Any other information including client instructions and client correspondence for each client

Records of all transactions undertaken during the course of a client relationship will be retained in the form of original documents, copies of original documents, and electronic data. Each document retained should provide information of the date and nature of the transaction, the amount and type of currency used (where applicable) and the client account(s) affected by the transactions. Each record should provide sufficient information to ensure that a satisfactory audit trail exists.

Transaction and client identification records will be maintained for a period of at least seven (7) years after the date the relationship has been terminated.

4.5. Enforcement and investigations

Verum Coin Project may be required to provide information, monitor accounts or perform certain activities based on Court Orders. These Orders may include Forfeiture, Pecuniary, Penalty, Restraint, Disclosure and Account Monitoring, Search and Seizure and Client Information Warrants. These enforcement and investigatory Orders may be served on Verum Coin Project and the required action in relation to client relationships that are maintained or were maintained with any entity within Verum Coin Project.

The Compliance Department must ensure that the appropriate responses are provided to these requests noting the stipulated deadline. Consultations should be made with External Legal Counsel where necessary, in responding to these Orders.

Any request of this nature received by any other Department within Verum Coin Project should be forwarded to the Compliance Department and the person forwarding the information should maintain the confidentiality standards based on current regulation.

4.6. Accountability

Verum Coin Project is aware of the risks attached to having inadequate systems to deal with for e.g. dishonest team members because the success of the AML and CFT program depends to a large extent on the integrity of team members. Verum Coin Project has established and implemented appropriate

policies and procedures to ensure that team members are “fit and proper” persons.

To this end, potential team members are subjected to a comprehensive screening process, which involves a thorough investigation of the potential team member’s background, honesty, competence and integrity.

Verum Coin Project has also instituted processes geared towards ensuring the continued maintenance of a high level of integrity and competence among team members. This includes but is not limited to:

- Establishment of a Code of Ethics & Conduct;
- Regular review of team member’s performance and adherence to internal policies and procedures including codes of conduct and AML and CFT requirements;
- Imposition of appropriate disciplinary actions for breaches of the institution’s AML and CFT policies;
- Close scrutiny and investigation of team members whose lifestyles cannot be supported by his or her known income;
- Review of team members’ account.

The reputation and operations of any institution rests heavily on the integrity, quality and efficiency of its team members.

At Verum Coin Project, all team members must be guided by the Code of Ethics/Conduct, which all team members must read and sign at the beginning of their employment with Verum Coin Project. Team members accounts should be operated according to the guidelines set out in the “Operation of Team members Accounts” procedure. Activity on all team members’ accounts will be monitored by the Compliance Officer.

The foregoing KYC reviews would also be necessary under the following circumstances:

- Upon the execution of a significant transaction;
- Upon material changes to client documentation standards;
- When there is material change in the manner in which the account is operated;
- When, during the course of the business relationship, doubt arises regarding the true identity of the client or the beneficial owner of the account;
- When there is any change in the ownership or control of a corporate client;
- Where the financial institution becomes aware at any time that it lacks sufficient information about an existing client or existing business relationship with another person;
- Where transactions carried out in a single operation or in several operations appear to be linked;
- Where a transaction is carried out by means of wire transfers;
- Where there is any doubt about the veracity or adequacy of previously obtained evidence of identity;

- Ascertain team member's citizenship status.

If during the course of the updating exercise or any time after the business relationship has commenced and Verum Coin Project discovers that the information on file is not accurate, or is no longer applicable and the correct or updated information is not available or cannot be obtained for any reason, then Verum Coin Project may take steps to terminate the relationship and should consider referring the matter to the Designated Authority.

The Compliance Department will conduct the necessary analysis and review of the account to inform its consideration of whether the matter should be referred to the designated authority.

All team members of Verum Coin Project are required to be trained at least annually on this policy and procedure.

Training initiatives can either be done via:

- Scheduled sessions;
- Randomly selected areas of operation both in-house(i.e. via Department or via frontline operations, or via sensitive operations);
- Randomly selected branches and subsidiaries;
- Video taping;
- Intranet learning systems.

Each team member will be tested on the material and a pass rate of 80% must be achieved before certification is received. Where a team member does not achieve the required 80% pass rate, a special training session will be held for such team members.

Willful blindness occurs when a team member ignores facts which a reasonable person would consider suspicious. A team member does not have to be actively involved in assisting money laundering in order to be held legally liable for the crime of money laundering. To the contrary, a team member who had the knowledge or should have known that funds were tainted or who fails to investigate red flags for suspicious activity, but still completes a transaction involving such funds, may be liable for money laundering. Even where there is no direct evidence of an individual's knowledge concerning tainted funds, individuals may be found to have been willfully blind or acted with reckless disregard for the facts, and therefore liable.

Team members should not:

- Knowingly, or with willful blindness, provide advice or other assistance to clients or anyone doing business with Verum Coin Project, who wish to violate/avoid money laundering laws or provisions of the AML Program;
- Knowingly, or with willful blindness, permit clients or anyone doing business with Verum Coin Project to execute transactions in such a manner, so as to break or obscure the audit trail;

- Conceal a suspicious client transaction;
- Advising client on FATCA.

Sanctions in relation to non-compliance:

- Sanctions for non-compliance with all policies, procedures and practices range from verbal warnings to termination of employment. Additionally, non-compliance with the relevant laws and regulations may result in a criminal liability for which a team member may be held accountable.
- Each team member is responsible for protecting Verum Coin Project from being used by money launderers. Involvement with money laundering activity, even if unintentional or indirect, e.g., through an association with a client or other persons that are involved in such activities, could also cause significant and long-term harm to the reputation of Verum Coin Project.
- Verum Coin Project will take all necessary steps to prevent its products, services and facilities from being used to launder funds derived from illegal activities.
- Team members must therefore comply with the applicable AML laws and regulations as well as regulatory expectations, the provisions of this AML Manual, and the policies and procedures and internal controls that apply to his or her position and duties.
- Failure to comply with applicable legal requirements or the AML Manual and Verum Coin Project related policies and procedures will result in disciplinary action including termination of employment. Individual team members may also be subject to criminal and civil penalties, including, but not limited to incarceration and monetary penalties, for failure to comply with AML laws and regulations.

Documents to be Signed by Team members Annually:

- The Verum Coin Project Code of Conduct;
- Anti-Money Laundering & Counter Financing of Terrorism Policy Statement.

4.7. Integrity and awareness

Obtaining and maintaining the requisite personal and financial history of team members. The information required is in accordance with best practices for the financial industry and ensures that team members meet the fit and proper standards required for their employment. This information is also used in establishing the Know Your Employee (KYE) Program.

Subjecting potential team members to a comprehensive screening process, which will involve from time to time:

- A thorough investigation of the potential team member’s background, honesty, competence and integrity;
- Reference checks;
- Checking the authenticity of academic qualifications;

- Reviewing the financial history of the potential team member.
- Establishing a Code of Ethics & Conduct for all existing team members to guide team member's conduct.
- Ensuring that the KYE program is effective and in compliance with the regulatory guidelines and internal policies in collaboration with Verum Coin Project Compliance Officer and the Compliance Department.
- Imposing the appropriate disciplinary action (including dismissal were appropriate) for breaches of Verum Coin Project's AML and CFT and Know Your Client Policies and Procedures.

Managers and Department Heads are responsible for:

- Ensuring that their team members comply with the policies of Verum Coin Project. Where there is non-compliance resulting in disciplinary action, information must be communicated to the Compliance Department and Human Resources Department to ensure the applicable disciplinary action is applied.
- Notifying the Compliance Department and Human Resources Department where there are indications of unusual changes in the team member's lifestyle and behavior that may be difficult to substantiate.

The effectiveness of the policies contained herein to a large extent will depend upon each team member's understanding of the impact of money laundering and terrorist financing on our day to day business activities. As a result:

- All team members must be aware of their personal obligation under the Regulations and the policies and procedures as detailed in this policy document.
- All team members should understand their obligation and responsibilities under the Code of Conduct, the Anti-Money Laundering Policy Manual and the reporting channels for suspicious or unusual activities.
- All new team members of the Verum Coin Project, irrespective of their level or seniority, must receive training in Anti Money Laundering and the Counter financing of Terrorism during their Orientation Period. Training will address the following areas:
- The policies and procedures in place to detect and prevent money laundering and terrorist financing.
- The basic elements of the current applicable regulations.
- The sanctions for non-compliance under these Acts & Guidelines.
- The background to money laundering and the international initiatives driving the changes including the Basel Committee, the Financial Action Task Force (FATF), Caribbean Financial Action Task Force (CFATF) and the applicable EU directives.
- The Verum Coin Project Code of Ethics and Conduct to be signed and distributed to all team

members annually.

- The obligations of the team members and Verum Coin Project under the relevant laws with an emphasis on the legal obligation of each team member.
- The recognition and handling of suspicious or unusual transactions
- An explanation of the legal obligations of both the team member and the employer under the current Anti-Money Laundering and Counter Terrorist Financing Laws and Guidelines
- Current and emerging money laundering and terrorist financing methods, trends and best practices
- Verum Coin Project's "Know Your Client" Policies and Procedures.

All team members should receive refresher training annually. Evidence of this training will be documented and filed. All team members must be aware of their own personal obligations, as they can be held liable for failure to report suspicious transactions to the Compliance Department.

Team members must also be aware that they may be subject to taking a test on Verum Coin Project's Anti-Money Laundering and Terrorist Financing Policies and Procedures.

Refresher courses will be conducted annually or at other intervals considered necessary. This is to ensure that all team members are aware and understand the policies of Verum Coin Project and the importance of compliance with the Anti-Money Laundering and Counter Terrorist Financing Regulation and their responsibilities and obligations under the relevant laws.

Training will take the form of formal presentation by external or in house experts or external courses conducted by reputable and competent institutions. Team members will also be provided with relevant materials through the intranet to enhance awareness of compliance issues and to communicate updates in the regulations or guidance notes issued by the regulators.

Training records should be maintained which detail the following information:

- The details of the course material and the targeted level of team members
- The names and signature of all team members in attendance and the date the training course was delivered
- The name of the presenter and completed evaluation form.
- The results of any test taken by team members to assess their understanding of the money laundering requirements in relation to the training course.

4.8. Tipping Off

It is an offense for anyone who knows, suspects or has reasonable grounds to suspect that a report has been made, or the compliance officer is acting or proposing to act in connection with an investigation into money laundering, to prejudice the investigation by so informing the person who is the subject of a suspicion, or any third party of the report, action or proposed action.

Where it is known or suspected that a suspicious transaction report has already been disclosed

to the compliance officer and it becomes necessary to make further enquiries, great care should be taken to ensure that clients do not become aware that their names have been brought to the attention of the authorities.

4.9. Confidentiality of reports

Reports submitted to the Financial Intelligence Unit and any other regulatory body whether locally or internationally must remain confidential. Reports filed for suspicious transactions with the Financial Intelligence Unit should not be disclosed to any person or entity unless required based on the current laws or regulations.

Team members should not disclose to any other team member, colleagues or clients (except the person to whom the transaction should be reported, or to the Compliance Officer): that a Suspicious Transaction Report has been filed; that the transaction is or appears to be suspicious; or that the transaction or the client is being investigated.

Team members will not be held liable in relation to any criminal, civil or administrative liability as the case may be for breach of any restriction on disclosure imposed by contract or any legislative, regulatory or administrative provision if transactions are reported in accordance with this policy and confidentiality of the report is maintained.

A team member who makes unauthorized disclosures of any confidential reports in relation to suspicious, threshold transactions or any other such regulatory report is subject to disciplinary action including dismissal and may also be fined under the current legislation.

4.10 Suspicious activity reporting (SAR) and cross-border compliance

SAR Filing for U.S. Transactions

Verum Coin identifies and reports suspicious activities involving transactions with a U.S. nexus. All transactions that meet reporting criteria are promptly filed with the Financial Crimes Enforcement Network (FinCEN) in compliance with U.S. anti-money laundering (AML) regulations. Compliance staff are trained regularly to ensure timely detection and accurate filing of SARs.

Internal SAR Filing Threshold and Timeline

Verum Coin enforces an internal threshold of $5,000 for SAR submissions involving U.S. jurisdictions, ensuring compliance with industry best practices. Once suspicious activity is detected, a SAR is filed within 30 days, following FinCEN guidelines. In cases where additional information is required for an ongoing investigation, the submission timeline is extended up to 60 days, as permitted by regulatory provisions.

Cross-Border Transactions and U.S. Compliance

Verum Coin implements enhanced screening mechanisms for transactions involving cross-border activities with a U.S. nexus. All transactions are reviewed for indicators such as U.S.-based IP addresses, U.S. bank accounts, or U.S.-registered entities. If a transaction is deemed suspicious, SAR requirements are applied, and reports are filed with the appropriate authorities.

Monitoring and Internal Controls

FinCEN SAR Portal: https://bsaefiling.fincen.treas.gov

To ensure ongoing compliance, Verum Coin:

- Maintains detailed records of all SAR filings and supporting documentation for a minimum of five years.
- Conducts regular audits of SAR processes to assess effectiveness and adherence to legal requirements.
- Provides annual compliance training for employees responsible for SAR filing, ensuring up-to-date knowledge of evolving AML threats and regulatory obligations.
- Updates SAR policies periodically, aligning them with FinCEN requirements and global AML standards.

These measures reinforce Verum Coin's active commitment to global AML compliance, risk mitigation, and regulatory adherence in transactions involving U.S. jurisdictions.

4.11 Travel Rule Compliance and Third-Party Intermediary Transactions

Compliance with the Travel Rule

Verum Coin has implemented robust procedures to ensure full compliance with the Travel Rule, as mandated by the Financial Action Task Force (FATF) and FinCEN. For all transactions exceeding $3,000, Verum Coin collects, verifies, and securely transmits the required sender and recipient information to the receiving institution. This includes:

- Full name of the sender and recipient
- Account numbers and unique identifiers
- Physical address, date of birth, and national identification number (where applicable)

All transmitted data is encrypted and securely stored to maintain compliance with regulatory requirements and ensure confidentiality. Transactions missing required information are flagged for further review before processing.

Handling of Third-Party Intermediary Transactions

Verum Coin actively monitors transactions involving nested exchanges, money transmitters, or other third-party intermediaries to prevent illicit financial activity. For transactions routed through third parties:

- Due diligence checks are conducted on all counterparties, ensuring they comply with AML regulations.
- Transaction monitoring systems detect patterns indicative of layering or structuring.
- Heightened scrutiny is applied to transactions involving high-risk jurisdictions or institutions with inadequate compliance programs.
- Ongoing audits and reporting ensure continued compliance with international AML standards.

These measures reinforce Verum Coin's commitment to preventing financial crimes, ensuring regulatory compliance, and enhancing the security of cross-border digital asset transactions.

5. KNOW YOUR CLIENT

"Know Your Client" Policies and Procedures are critical to the effective management of risks and the safety and soundness of the integrity of the system as a whole. Know Your Client ("KYC") is closely associated with the fight

against money laundering and financing of terrorism, and is also an essential part of controlling and mitigating against reputational, operational, regulatory and legal risks to Verum Coin Project.

5.1. Scope and purpose

The KYC policies of Verum Coin Project will address four key elements of sound KYC standards:

- Client Identification and Verification;
- Client Acceptance Policy;
- Monitoring of Accounts;
- Risk assessment of client relationships.

Verum Coin Project has adopted a risk based approach to the classification of its clients to ensure that the due diligence standards on clients are heightened in instances where client information indicates a higher susceptibility to money laundering risk.

These Know Your Client Policies and Procedures are designed to foster a strong relationship with our clients, while taking all possible steps to protect Verum Coin Project's reputation.

With the introduction of FATCA Verum Coin Project will be required to ascertain whether any of our clients are US persons as defined by the FATCA regulations. Where a US person is identified additional scrutiny and in some cases reporting requirements will apply. Refer to full KYC Procedures for specific procedure guidelines.

5.2. Client identification and verification

Verum Coin Project must at all times establish to its satisfaction that it is dealing with a real person (natural, corporate or legal). The identity of all persons conducting business with Verum Coin Project must be verified.

Proper identification of each client (including parties who may have a beneficial interest in the transaction or the account) and those that may be acting on their behalf (agents) must be ascertained before the commencement of any relationship.

Before establishing an account, verification must be performed for all persons authorized to operate the account. This includes:

- Any persons or entities, corporate or unincorporated who seek to establish a relationship.
- Any person who is the beneficial owner of the account.
- Any person having a beneficial interest in the account or has direct or indirect control of the account.

5.3. Prohibited accounts, relationships and transactions

Verum Coin Project prohibits wire transfers to the following countries via Accounts (ie US, CDN$, Sterling & Euro): Burma (Myanmar), Cuba, Iran and Sudan, Western Balkans, Cote d'Ivoire, Democratic Republic of the Congo, Iraq, Liberia (Former Regime of Charles Taylor), Lebanon, North Korea, Sierra Leone, Syria and Zimbabwe. As some of our bankers might have US payable through

account this means we must never process wire transfers to these countries unless further advised. All funds wired will be blocked by the US authorities and most often never returned.

Verum Coin (VERUM) is subject to specific liquidity restrictions. Buyers of Verum Coin are prohibited from selling or cashing out their holdings until the token is officially listed on Tier 1 cryptocurrency exchanges, such as Binance, ByBit, or equivalent Tier 1 exchanges.

Verum Coin reserves the right to monitor transactions and enforce compliance with this restriction. Any violation may result in the suspension or freezing of assets, reporting to relevant regulatory authorities, and other corrective measures deemed necessary.

Verum Coin Project will not conduct businesses with clients or execute any transaction where the following apply:

- Illegal Activities are suspected: Clients whose information indicates possible involvement in illegal activities.
- Verification Not Possible: Clients with businesses that make it impossible to verify the legitimacy of their activities or the source of funds.
- Refusal by the client to Provide Required Information: Clients who refuse to provide the required information or documentation.
- Entity is a Shell Bank: Banks having no physical presence in the jurisdiction in which it is licensed to operate.
- Ownership Structure is via Bearer Shares: Bearer Shares are shares which are owned by the persons holding these shares. This allows ownership of shares to change easily and it may be difficult to determine the true beneficial owner.
- Nominee Shareholders are used: Foreign entities having nominee shareholders and it is difficult to determine the ultimate beneficial owners.
- Anonymous or Fictitious Names are used: Where clients wish to open anonymous accounts or accounts using fictitious names.
- Entity is a Shell Company: Legal entities that act as a “front” for illegal activities. It may be difficult to determine the true activity of such companies and therefore enhanced due diligence procedures must be adopted where there are indications that entities have no business substance.
- Listed Persons or Entities: Individuals and Entities names appearing on the US treasury OFAC list or UN Sanctioned List.
- Suspicious Transactions: Where information obtained before processing a transaction is deemed suspicious.

5.4. Client due diligence

Client Due Diligence (“CDD”) refers to basic information that should be collected from all potential clients before they are approved for acceptance. The objective of CDD is to understand the client’s

business and the types of transactions it will likely engage in and assist in the identification of unusual or suspicious activity. CDD also assists in risk rating the client and identifying clients that may pose increased risks (i.e., risk rated as high) for money laundering who may require enhanced due diligence and increased monitoring. In addition to the documents and information required for each client type, Verum Coin Project will adopt the following principles and guidelines for client due diligence:

A. Acquiring Knowledge and Understanding of the Client:

a) Verum Coin Project should gain sufficient knowledge about our clients to ensure that we are doing business with reputable clients and suppliers whose association with Verum Coin Project will not expose the company to negative publicity.

b) Additional enquiries should be made to verify information if there appears to be doubt or inconsistencies in the information provided.

c) Any update or change in existing information on the client that is in accordance with the KYC policy should be documented and included on the clients' file.

d) Verum Coin Project, at its discretion, may request additional information from clients in order to corroborate any information previously supplied by the client.

e) In accepting business from clients who resides overseas, Verum Coin Project will ensure that:

- Documents presented are certified/notarized
- Documentation presented is verified by contacting a third party
- Original certificate of good standing for corporations registered overseas

f) Verum Coin Project will not facilitate any wire transfers or other electronic fund transfer activities unless this is being done for a client of the institution.

g) Where funds are wired on behalf of professional intermediaries, all the relevant information must be obtained before such transaction is executed.

B. Verification and review of client information by team members.

The team member opening the account is required to examine the identification carefully to ensure that it is not forged or altered and that the description on the ID is consistent with the appearance of the person who presents it.

Each team member is required to check that all information in relation to the client is valid and is corroborated based on references and documents provided to support information included on the client database form. All accounts designated as "high risk" must be referred to the compliance department.

C. Review and update of existing client information.

Each team member must initiate on-going updates of client's KYC information.

At any time after the client relationship is established, the compliance department may request

team members to contact clients to obtain certain KYC information or documentation. Team members should contact the client to request the information and conduct any required follow-up considered necessary. Once the information and/or documentation are received, the team member should communicate with the compliance department where necessary and update the client record.

D. Enhanced Due Diligence Requirements.

In addition to obtaining the required information and documentation to satisfy the requirements of Client Due Diligence process, team members and the Compliance Department may also be required to conduct Enhanced Due Diligence (EDD) on potential or existing clients that have been determined to be high risk or otherwise have been identified as requiring EDD.

EDD requirements may include the following:

- Searches of databases and websites for additional information that may be available. This includes general searches on Google, local or international newspapers, regulatory organizations websites in other countries.
- OFAC list
- Compliance software
- Independent confirmation with overseas or local entities and individuals
- A report on the physical site visit that was conducted by the relationship managers to the applicant's principal office or operating location. The report should contain the following information: the address visited; date of visit; name of the person(s) visited and their positions within the organization or relationship to the company; a general description of the visit.
- Information regarding the AML supervisory and law enforcement regime of the jurisdiction that issued the license to the company and of the parent entity if the institution is regulated whether locally or overseas.
- Information regarding whether the client has been subject to any criminal, civil or regulatory enforcement actions;.
- Other information that may be required based on the circumstances of each case.
- Enhanced due diligence.

E. Clients requiring Enhanced Due Diligence (EDD) and identification of high risk accounts.

High Risk clients are clients whose transactions are considered large or the nature and structure of business or profession makes them more susceptible to being used for illicit activities. A detailed assessment of the following should be conducted:

- Clients background
- Country of origin

- Profession
- Public or high profile position
- Source of funds
- Accounts that are determined as high risk must not be opened without the approval of Verum Coin Project's compliance officer. These accounts will be subjected to enhanced due diligence including:
- Obtaining all relevant identification information that is required as per procedure prior to establishing the business relationship.
- Verifying identification information.
- Accessing publicly available information to assist in the determination as to whether or not the person is acceptable to Verum Coin Project.
- Investigating and determining the source of funds to commence and maintain business relationship.
- Conducting a face to face meeting with the prospective client to discuss/confirm the information given, purpose of account and source of assets by Compliance Officer or authorized company's affiliates who comply with Verum Coin Project's client identification and verification rules.
- Seeking approval from executive team leader and compliance officer to open account or establish the business relationship.
- Making a request for submission of personal data and verification of income sources.
- Investigation to ascertain if the account holder has been refused banking facilities at another financial institution.
- Regular review of client records.
- On-going monitoring of accounts.

The following categories of clients should be classified as high risk due to the size of the transaction or the nature and complexity of the business or profession. Accordingly, all business that are classified as one of the following will receive increased scrutiny from the compliance officer.

Verum Coin Project will not establish business relationships with:

- Foreign entities with bearer shares.
- Investment clubs (partner plans, pyramid schemes).
- Cheque cashing businesses.
- Adult entertainment clubs.
- Gaming and casino dealers.
- Individuals who reside in jurisdictions or countries with inadequate AML and CFT

framework.

The following individuals and entities are deemed high risk and therefore enhanced due diligence will need to be done. The compliance department will review and determine whether or not we will enter into a business relationship.

- Politically exposed persons and immediate family members
- Remittance companies
- Non-residents
- A person acting as a trustee for another relation to the business relationship or one-off transaction concerned.
- A company having nominee shareholders, or shares held in bearer form.
- A member of such other class or category of person as the supervisory authority may specify by notice published in an official Gazette.

If the ultimate beneficiary or beneficiaries or beneficial shareholders cannot be reliably established or there are no reliable measures in place to monitor any changes in the ownership structure, the relationship should not be commenced, or where a business relationship has already been established, this relationship should be legally terminated.

F. Politically exposed persons (PEP).

Enhanced due diligence is required for transactions involving high risk activities, businesses, foreign countries and politically exposed persons (PEPs).

PEPs are individuals who are or have been entrusted with prominent public functions including:

- Heads of state or government
- Senior politicians
- Members of parliament
- Ministers of government
- Senior government officer
- Member of judiciary
- Military official above rank of captain
- Member of the police or above rank of assistant commissioner
- Permanent secretary, chief technical director or chief officer in charge of the operations of a ministry, department of government, executive agency or statutory body.
- A director or chief executive of any company in which the government owns a controlling interest.
- Senior executives of publicly owned corporations.
- Official of political party.
- Individual who holds or has held a senior management position in an international

organization.

- Immediate family., i.e. parent, sibling, spouse, children, in-laws as well as close associates (persons known to maintain unusually close relationships).

The identity of the account holder must be ascertained and enhanced due diligence must be applied. This includes:

- Stricter KYC procedures, more detailed information on the background, reputation, etc.
- Tagging of all such accounts on auto ID.
- Approval from business operations manager and compliance officer to open these accounts.

G. Accounts opened by professional intermediaries.

This group includes pension funds, unit trusts, and other fund managers, as well as lawyers, security dealers and stock brokers managing single or pooled accounts held on deposit or in escrow.

If Verum Coin Project determines that the account is being held on behalf of a single client, then the identity of the relevant KYC information for the client must be ascertained.

Where pooled accounts are maintained, Verum Coin Project may rely on the professional intermediary's due diligence process and not look through to the ultimate beneficiary, but only if the following conditions are met:

- The intermediary engages in sound due diligence practices; and
- The institution is able to verify the reliability and effectiveness of the intermediary's client due diligence.

H. Accounts identified for the purposes of FATCA.

Where a client account has been identified for the purposes of FATCA enhanced due diligence and reporting will be required.

5.5. Non-cooperative countries and countries with inadequate AML/CFT frameworks.

Verum Coin Project will periodically provide information on the list of non-cooperative countries and countries with inadequate AML and CFT frameworks and categorized as a significant threat to the Counter-financing of Terrorism. The countries included in this list are subject to change and will be communicated by the Compliance Department from time to time. The current list of countries includes:

- Countries subject to United Nations Sanctions.
- Counties subject to prohibitions in the U.S. Office of Foreign Asset Control (OFAC).
- Countries with poor records of combating money laundering and terrorist financing or which are the subject of considerable unrest and lack of political stability.
- Countries which are considered 'high risk "under FATF recommendations.[4]

[4] http://www.fatf-gafi.org/countries/#high-risk

Clients with origins or links to countries, or clients under international personal sanctions[5] or PEP[6] on this list may not be accepted as clients of Verum Coin Project without the prior approval of Verum Coin Project Compliance Officer.

Countries on the OFAC and UN sanction list include:

- Afghanistan;
- Burundi;
- Balkan (Former Yugoslav Republic of Macedonia, Southern Serbia, Federal Republic of Yugoslavia, Bosnia, Kosovo);
- Burma (Myanmar);
- Cote d'Ivoire;
- Cuba;
- Democratic Republic of Congo;
- Democratic Peoples' Republic of Korea;
- Iran;
- Iraq;
- Liberia;
- Lebanon;
- Libya;
- North Korea;
- Rwanda;
- Sierra Leone;
- Somalia;
- Sudan;
- Syria;
- Tanzania;
- Uganda and Zaire;
- Zimbabwe.

Particular care should be taken when establishing relationships with clients from jurisdictions known to have weak anti-money laundering and financing of terrorism regulations or with entities where there is no regulatory oversight by an independent body.

[5] https://www2.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/

[6] https://namescan.io/FreePEPCheck.aspx