Cethereum Anti-Money Laundering Compliance Policy and Programme

1. INTRODUCTION AND PURPOSE

Cethereum Technologies Inc. (**"Cethereum"** or the **"Company"**) believes in being an active participant in maintaining the integrity of the global financial system, including preventing money laundering, terrorist financing, and other financial crimes. The Company is committed to deterring customers and outside parties from using the Company as a conduit for such illegal activity and is committed to its compliance with all applicable laws and regulations designed to combat such illegal activities. Cethereum recognizes that a strong anti-financial crime programme is an essential element in legal compliance and being an active participant in maintaining the integrity of the global financial system. Cethereum designed this Anti-Money Laundering (**"AML"**) Compliance Policy (the **"Policy"**) to do just that.

The Policy will aim to:

1) Establish a framework for protecting the Company from being used to facilitate money laundering or terrorist financing or circumvent economic sanctions;
2) Institute compliance with the legal and regulatory responsibilities applicable directly to the Company and/or its business partners (including the requirements to monitor, detect, prevent, and report possible money laundering, terrorist financing, sanctions breaches, and other financial crimes);
3) Set forth the governing principles and mandatory minimum standards, roles, responsibilities, specific measures, and general expectations of Cethereum personnel [1] as they conduct business; and
4) Communicate the Company's clear commitment to strong compliance culture.

Money laundering is the process by which persons attempt to conceal and disguise the true origin and ownership of illicit funds. Money laundering is generally viewed as a three-stage process: placement, layering, and integration:

- Placement is the introduction of unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement;
- Layering is the moving of funds around the financial system to create confusion and complicate the paper trail; and

[1] Cethereum "personnel" includes all Cethereum employees, officers, temporary staff, contractors, and service providers, including any subsidiary company staff involved in the operations of Cethereum.

- Integration is the further incorporation of unlawful proceeds in the financial system through additional transactions to convert illicit funds into apparently legitimate business earnings.

Policy Statement

It is the policy and intention of Cethereum to comply fully and continuously with all applicable AML laws and related regulations. Cethereum personnel must not conduct any activity in which he or she knowingly violates or circumvents such laws and regulations.

It is the policy and intention of Cethereum to comply fully and continuously with all the laws, regulations, and orders regarding doing business with, maintaining accounts for, or handling transactions or monetary transfers for foreign countries or foreign nationals listed under applicable sanctions programmes. Cethereum personnel must not conduct any business activity in which he or she knowingly violates or circumvents legally applicable sanctions. If Cethereum finds that it has an account for or a customer of Cethereum is included in applicable sanctions programmes, all accounts of such customer shall be blocked. Cethereum recognizes that it requires sanctions controls in order to ensure compliance with sanctions as well as remain aligned to the Company's risk tolerance.

2. POLICY SCOPE

This Policy applies to the Cethereum board of directors (the **"Board"**), all Cethereum personnel, and all Cethereum business activities.

3. POLICY REQUIREMENTS

This Policy requires that the Board adopt, implement and adhere to its components, which includes the following:

- Designation of an AML Officer;
- Governance structure for the Policy;
- Internal controls designed to ensure ongoing compliance with AML requirements applicable to the Company and its financial partners, including:
    - AML compliance risk assessment processes;
    - Risk-based frameworks for a "Know Your Customer" (**"KYC"**) and customer due diligence programme that provides, collects, and verifies, as needed, customer information;
    - Controls to ensure compliance with sanctions laws;

- Risk-based transaction monitoring and suspicious activity reporting, including to financial partners as appropriate;
- Regulatory reporting and record-keeping;
- Information sharing with law enforcement and other financial institutions;
- Mechanisms designed to monitor ongoing compliance (e.g., quality assurance and audit);
- Ongoing training and development for personnel whose routine activities are relevant to AML controls; and
- Periodic independent Policy review by a qualified third party to test and assess the implementation and effectiveness of the Company's Policy and the adequacy of its controls over AML compliance risk.

Cethereum will document its efforts to carry out all activities pursuant to this Policy.

3.1. GOVERNANCE STRUCTURE, ROLES, AND RESPONSIBILITIES

The Board designates the AML Officer,[2] who has responsibility for day-to-day oversight of the Company's AML compliance and execution of this Policy. The AML Officer reports directly to the Cethereum chief executive officer (**"CEO"**) and has direct accountability, and access, to the Board as needed.[3]

The AML Officer and his/her team are independent of the Company's other teams and have the authority to cross departmental lines. They will have unrestricted access to any business records, IT systems, or any other business locations to which they require access in order to fulfil their responsibilities.

The following table summarizes roles and responsibilities for development, implementation, oversight, and review of this Policy.[4] As Cethereum's operations mature, its full-target operating model will be achieved; as such, short-term coverage of certain responsibilities may be provided by identified individuals.

[2] Unless determined otherwise by the Board, the Chief Compliance Officer serves as the AML Officer.

[3] As Cethereum's business and management structure expands, it may implement management-level executive committee(s) responsible for overseeing the Policy, as appropriate.

[4] At this time Cethereum does not have multiple layers of management. As and when Cethereum grows, the AML Officer will amend this Policy to clarify the responsibilities in relation to the Policy.

Responsible Party	Role/Responsibility
Board of Directors (or a delegated committee thereof)	• Designate an AML Officer; • Review and approve this Policy and adopt revisions as necessary, at least annually; • Review, approve, and oversee Company-wide initiatives related to this Policy; • Review escalated issues related to this Policy and resolve them; • Review compliance reports related to this Policy and act on them as needed; • Ensure that the AML Officer has sufficient authority to carry out his or her duties; • Oversee the Policy, assessing its effectiveness via an independent test by a qualified third party at least every two years; • Approve the AML compliance risk assessment required by this Policy; and • As applicable, review feedback from regulatory examinations or correspondence relating to the Policy and receive reports on any remedial action necessary.

Executive Management[5]	• Promote a strong culture of compliance at Cethereum; • Ensure that the AML Officer has sufficient authority to carry out all duties related to this Policy; • Ensure that the Company has sufficient resources, including personnel and systems, to implement and meet the objectives of this Policy; • Hold management and all stakeholders accountable for resolution of corrective actions related to this Policy; • Communicate this Policy and its requirements to Cethereum personnel within their area of responsibility; • Implement this Policy and other applicable policies and procedures within their area of responsibility; • Ensure that employees under their supervision receive appropriate compliance training on this Policy; • Review and approve with the AML Officer any Policy exceptions; • Ratify lowering a monitoring threshold or imposing a new threshold; • Review the AML compliance risk assessment required by this Policy; • Review the results of independent testing; • Review the AML Officer's recommended Policy revisions; and • As applicable, review feedback from regulatory examinations or correspondence relating to the Policy and receive reports on any remedial action necessary.
General Counsel[6]	• Interpret laws and regulations; • Provide advice and counsel regarding the requirements of applicable laws, regulations, and Company policies to all stakeholders; • Review and approve all customer-facing documents, and new or significantly revised products, services, geographies, and business practices; and • Initiate and maintain the Financial Transactions and Reports Analysis Centre of Canada (**"FINTRAC"**) registration and relevant licenses.

[5] C-suite level Cethereum personnel
[6] Cethereum may initially consult outside legal counsel while it expands its management structure to include a general counsel.

AML Officer	• Develop and present this Policy for Executive Management review and for Board review and approval, initially and going forward at least annually; • Implement and maintain this Policy and related procedures; • Maintain sufficient staffing, in both numbers and qualifications, to implement the Policy effectively, and request additional resources from Executive Management as needed; • Ensure all Cethereum personnel receive appropriate training on this Policy and that Cethereum documents such training and attendance; • Review and provide guidance, including through engaging outside legal counsel as appropriate, the requirements of applicable laws, regulations, and Company policies, to all stakeholders; • Maintain systems, procedures, reports, and other controls used to support efforts to comply with this Policy, including ensuring that each function conducts on-going monitoring of the effectiveness of its compliance controls, and promptly alerts Executive Management and the Board on any material deficiencies or weaknesses or non-compliance. • Institute and monitor corrective action to remedy any deficiencies found; • Review any changes to AML compliance and sanctions-related laws, regulations, guidance, or regulatory expectations and ensure that the Company implements processes to remain fully in compliance with its AML obligations and regulatory expectations; • Perform the necessary analysis to determine the ongoing effectiveness of the Policy, and review and refresh the Policy, at least annually and more frequently as circumstances require, and ensure that this takes into account applicable law and supervisory or relevant third party input; • Make recommendations for addressing weaknesses or new requirements to the Board, and report them to Executive Management; • Approve exceptions to this Policy and maintain a written record of exceptions, including reasons for granting them; • Conduct an AML compliance risk assessment prior to or within three (3) months of operations commencing, and continue to update it annually; and • Schedule independent third party testing of the effectiveness of the Policy at least every two years.

	• Update the AML compliance risk assessment in light of any issues raised during independent testing; • Set transaction monitoring thresholds and adjust them as needed in response to emerging patterns of activity, documenting the rationale for all threshold changes; • Ensure that the Company fully meets AML reporting and Office of Foreign Assets Control (**"OFAC"**) requirements in a timely fashion applicable to its operations or to its business partners, including designing appropriate controls, conducting testing of their effectiveness, and preparing annual reports to OFAC on the total of blocked funds; • Establish systems and procedures to receive, document, respond to, and evaluate information sharing requests; • Review the AML implications of any new or significantly revised products, services, distribution channels, geographies, initiatives or business practices, and advise Executive Management on necessary steps to mitigate the money laundering and/or sanctions risk; • Provide input into the performance of key Cethereum personnel in meeting their responsibilities under this Policy; • Provide periodic reports to the Board and Executive Management, at least annually, on the state of AML compliance, testing and monitoring reports, and any significant emerging issues; • Report potentially suspicious activity to Cethereum's financial partners on an on-going basis, and alert law enforcement as needed; • Establish a regular quality assurance programme and ensure that the Company's approach to testing AML compliance is consistent with the overarching compliance testing approach; • Ensure adequate staffing of critical programme functions; • Oversee all service providers whose activities impact the Policy; • In conjunction with legal counsel, approve contracts and agreements with affiliated and third party service providers that impact the implementation of this Policy to ensure that every contract clearly identifies the service provider's roles, responsibilities, performance standards, reporting obligations, and liabilities; and • As needed, liaise with regulators on AML compliance issues.

Cethereum Personnel (All Employees and Third party Service Providers)	• Promote a strong culture of compliance at Cethereum; • Know their responsibilities under this Policy and ensure they remain in compliance; • Ensure they complete required AML compliance training; • Ensure they implement the Policy within their sphere of responsibility and deliver compliance outcomes; • Notify and seek the approval of the AML Officer in advance of all proposals for new or modified products, services, geographies, distribution channels, or initiatives that might affect money laundering and sanctions risk; • Identify compliance weaknesses within their areas of responsibility related to this Policy, and promptly alert relevant executive leaders and the AML Officer; • Report unusual or suspicious activity to the AML Officer; • Grant the AML Officer, or designee, unrestricted access to business records, systems, or locations necessary to fulfil the duties described in this Policy; and • For departmental heads: submit plans for any new or substantially modified policies, procedures, or controls for review and approval by the AML Officer.

3.2. RISK TOLERANCE STATEMENT AND BUSINESS DECISIONS

The Company understands that virtual currency transactions pose a potential risk for money laundering and/or terrorist financing and sanctions breaches. The Company's risk tolerance for money laundering risk is low; the Company's has zero tolerance for any breach of this Policy's sanctions compliance requirements. The Company will not accept either natural person or legal entities as customers (both existing and new customers) if they are Specially Designated Nationals, as defined by OFAC. Therefore, the Company requires a robust control environment with low error rates for due diligence after applying internal controls. As a result, the AML Officer will participate in business decisions that affect the Company's AML compliance risk, such as changes to permissible customer types, etc. The Company will adhere to certain standards to limit these risks.

Cethereum's risk assessment will depend on its analysis of the following risk factors:

- the personal and business relationships of the person or entity;
- the products and delivery channels of the person or entity;
- the geographic location of the activities of the person or entity; and
- any other relevant factor.

Cethereum sets appropriate limits on the customer types accepted and the number of permitted accounts and their usage, commensurate with the Company's money laundering and sanctions risk in its activities.

3.3. INTERNAL CONTROLS AND ESTABLISHMENT OF AML COMPLIANCE PROGRAMME

Cethereum will maintain controls as necessary to mitigate the AML risks presented by its customers, products and services, and operating geographies to an acceptable level. Cethereum may rely on a third party to operate particular compliance controls or systems. Cethereum and the AML Officer ultimately remain responsible for satisfying regulatory obligations and should establish effective oversight processes for any outsourced tasks. The AML Officer oversees the development and implementation of internal controls sufficient to ensure compliance with this Policy, including the following.

3.3.1. KNOW YOUR CUSTOMER PROGRAMME

The Company's risk-based KYC programme has three components: a customer identification programme (**"CIP"**) that allows the Company to identify and verify the identity of its customers with reasonable assurance; a customer due diligence (**"CDD"**) programme; and an enhanced due diligence (**"EDD"**) programme for customers with indicators of heightened risk.

3.3.1.1. CUSTOMER IDENTIFICATION PROGRAMME

Cethereum's CIP is a fundamental control in preventing the Company from becoming involved in money laundering, terrorist financing, or sanctions breaches. The Company's policy is to ensure that it has a reasonable belief that it knows the true identity of its customers at on-boarding. This means that identification information has been obtained for each customer and that independent means have been used to verify some or all of the identification information. This Policy covers all Cethereum customers. Customers include anyone that opens an account, including individuals and corporations and other legal entities.

Cethereum's policy is to collect the following identity information online or on a mobile application for all of its customers at account opening before allowing the customer to deposit funds or conduct transactions:

<u>Individuals</u>

- Full legal name;
- Date of birth;
- Government identification number (i.e. Social Insurance Number);
- Current physical street address;

- E-mail address;
- Mobile telephone number; and
- Valid payment method information, which if is the customer's bank account, should include at least: financial institution, account type, routing number, and account number.

Legal Entities

- Full legal name;
- Government identification number (such as incorporation number, business number or tax number);
- Current physical street address;
- Website;
- E-mail address;
- Telephone number;
- Principal account holder's[7] full legal name. The legal entity's principal account holder is also required to complete CIP, as described above; and
- Valid payment method information, which if is the customer's bank account, should include at least: financial institution, account type, routing number, and account number.

3.3.1.1.1. VERIFICATION

The Company[8] verifies at the time of on-boarding the identity of each customer, including their name, government identification number, and address, through documentary verification methods of customer information listed below.

Individuals

Documents that evidence the existence of an individual are original, unexpired, government-issued, or agencies thereof, documents with a photograph, which contain the name and either an identification number or date of birth. When accounts are applied for, the document must always be sighted through live connection or screenshots/photos. Such documents may include:

- Passport;
- Driver's license;
- Visa;

[7] The principal account holder is the key decision-making party for the product or service with whom Cethereum is engaged.

[8] Cethereum may contract an SLA with a third party to organize and review customer information. The service provider would be subject to the Oversight of Outsourced Service Providers requirements specified in this Policy.

- Photo ID card;
- Armed Forces identification; and
- Permanent Resident card.

The above documents and their similar counterparts must have the following criteria where applicable:

- The document is valid and clearly shows the issue and expiry dates;
- The photograph and all features are clearly visible;
- The side showing the signature is included and the signature is clearly visible;
- The place of issue and number details are included and are clearly legible; and
- Nationality details are included and clearly legible.

Additionally, the customer's address needs to be verified. This may be through documents and resources such as the following:

- Third party databases;
- Government websites;
- Copy of correspondence between the customer and the governmental authority;
- Copy of customer's utility bill (dated within the past three months);
- Copy of current bank statement (dated within past three months);
- Google or other search engine results;
- Copy of Title to Property;
- Copy of executed current mortgage; or
- Copy of executed current lease agreement.

Legal Entities

Documents for entities are original documents issued by governments or agencies thereof bearing the seal of the issuing government body or certified by the government body, all of which must be of the current year, where applicable, and include:

- Certificate of good standing;
- Government-issued business license;
- Certified formation documents;

- Articles of incorporation;
- Articles of organization;
- Articles of association;
- Signed partnership agreement(s);
- Business license; and
- Trust instrument.

3.3.1.1.1.1. RECORD-KEEPING

Cethereum will make and maintain records with regard to the verification of customer identity. Cethereum will retain the original of any application form and all relevant records received, including correspondence with the customer. A record must be made of the description of any documents relied upon to verify the identity of a customer, including the document's type, identification number, place and date of issuance, and expiration date (a copy of the document(s) satisfies the requirement).

Cethereum will electronically retain all CIP information for at least five years after the date of the customer's most recent transaction or transaction attempt.

3.3.1.1.1.2. EXCEPTIONS, EXTENSIONS, AND LACK OF VERIFICATION[9]

In limited circumstances, the AML Officer may grant an exception to the CIP requirements including determining whether account activity must be restricted, or transactions monitored. The AML Officer and at least one member of Executive Management is required to review and confirm/approve any such exceptions. These restrictions remain in place until the verification process is complete or the account or relationship is terminated.

The Company must ensure that proper verification of customer identification for each customer is performed before a new account is opened. However, the AML Officer may grant a temporary extension of thirty (30) calendar days for completing the CIP process. These exceptions must be monitored for aging and completion purposes and reported to Executive Management.

Cethereum will not allow customers awaiting identity verification to deposit funds or conduct transactions of any kind. Cethereum's policy is to not permit individuals or legal entities who fail customer verification to maintain accounts of any kind.

In the event that:

- the customer cannot or will not provide the CIP information requested; or

[9] Pending authentication or failure of the authentication process is grounds for not permitting customer activity or the opening of the customer account.

- the customer's identity cannot be verified with the information provided and the customer cannot subsequently provide sufficient proof of identity; or

- there are anonymous accounts or accounts under fictitious names; or

- the customer has provided information that is false or contains significant inconsistencies that cannot be resolved after further investigation,

then the Company will suspend the due diligence and onboarding process, notify the AML Officer, and the Company will not enter a relationship with the customer or open the account, or the Company will exit the existing relationship within thirty (30) calendar days. If appropriate, the AML Officer may escalate such customers for potential investigation of suspicious activity if Cethereum identifies reportable suspicious activity identified in the due diligence processes.

3.3.1.2. CUSTOMER DUE DILIGENCE

3.3.1.2.1. CUSTOMER DUE DILIGENCE REQUIREMENTS

Cethereum performs CDD and collects additional customer information for all customers, as follows:

Individuals

- Source of funds;
- Occupation;
- Annual income;
- Expected product usage (e.g. buying, selling or mining); and
- Account activity (expected monthly dollar amounts for buy/sell transactions, number of monthly buy/sell transactions, and mining revnue).[10]

Partnerships

- Registration documentation;
- Partnership agreement(s);
- Full CDD on all individual partners (as described above in the individual section); and
- Full CDD on all corporate partners (as described below in the legal entities section).

[10] After on-boarding the customer, Cethereum will continue to keep this information updated on a periodic and risk-based basis.

Legal Entities

- Source of funds;
- Most recent audited financial statements, if they exist;
- Central security register;
- Director and officer registers;
- Full CDD documentation on each director and officer (as described above in the individual section);
- Full CDD documentation any company/corporate body with an interest in the applicant;
- Resolution of the board of directors to open an account and identification of those who have authority to open the account;
- Expected product usage and account activity;
- Description of industry; and
- Legal entity ownership structure.
    - The Company requires, for all legal entity customers, collection of information on the customer's ownership structure and the identification of beneficial owners and the ultimate parent. A **"beneficial owner"** is a legal entity or individual that directly or indirectly owns or controls 25% or more of a customer. A customer can have any number of beneficial owners or the customer may have none. An "ultimate beneficial owner" (**"UBO"**) is an individual or legal entity that directly or indirectly owns or controls 25% or more of a customer and does not itself have any individual or legal entity with a controlling interest of 25% or more. The UBO is at the top of the ownership structure. A customer might have up to four UBOs or the customer may have none. For Politically Exposed Persons [11] (**"PEPs"**), the threshold for determining a UBO is 10% or more.
    - An **"ultimate parent"** is a legal entity that directly or indirectly owns or controls more than 50% of a customer and does not itself have a legal entity with a controlling interest of more than 50%. A customer usually has one ultimate parent but in rare circumstances will have none. This situation would occur when Cethereum has a customer that is the "top of the house" entity.
    - As part of documenting the ownership structure of a customer, all beneficial owners must be identified including the full legal name and the percentage ownership.

[11] People who hold, or have held, important public functions, including heads of state, senior politicians, senior government and judicial officials at all levels of government, senior military leaders, senior executives of state-owned corporations, and important political party officials

In addition, since account applications occur online or through a mobile application, Cethereum may at account opening or during the CDD process collect information for other purposes that will deepen its understanding of customer identity and help further assess risk, including telephone usage, IP address and location information, and social networking and public record information.

Prior to the completion of CDD, Cethereum will not allow customers to deposit funds or conduct transactions of any kind. Cethereum's policy is to not permit individuals or legal entities who fail required CDD to maintain accounts of any kind.

In the event that:

- CDD measures cannot be applied; or
- the customer cannot or will not provide the CDD information requested; and/or
- the customer has provided information that is false or contains significant inconsistencies that cannot be resolved after further investigation,

then the Company will suspend the due diligence and on-boarding process, notify the AML Officer, and the Company will not enter a relationship with the customer or open the account, or the Company will exit the existing relationship within thirty (30) calendar days. If appropriate, the AML Officer may escalate such customers for potential investigation of suspicious activity if Cethereum identifies reportable suspicious activity identified in the due diligence processes.

3.3.1.3. ENHANCED DUE DILIGENCE

Cethereum conducts EDD to assess the risks associated with its users and expected transaction activity on a risk-based basis. Customers subject to additional due diligence include:

- Any customer identified as a Higher-Risk Customer type (in the section below); and
- Any customer with gross transactions of $50,000 or more over the previous twelve (12) months.

3.3.1.3.1. HIGHER-RISK CUSTOMER TYPES

The Company has identified certain customer types as presenting a greater likelihood of money laundering and sanctions risks. The following list is non-exhaustive:

- Customers identified as PEPs, and individuals or entities closely socially, familially or professionally associated with PEPs;
- Embassy, foreign consulate, and foreign consulate employee customers;
- For-profit religious or spiritual organizations;

- Dealers in precious metals and stones;
- Charities, not-for-profit organizations, and non-governmental organizations that are either unregistered, or located or operating in high risk jurisdictions;
- Customers organized, domiciled, or doing business in high risk jurisdictions;
- Legal entity customers for whom UBO information or information regarding the legal entity's directors, managing partners, trustees, settlors, and beneficiaries, cannot be obtained or its accuracy reasonably confirmed;
- Customers subject to significant negative news, as identified through screening and due diligence activities;
- Customers with suspicious background or links with known criminals;
- Customers with false ID documents or ID documents that cannot be verified within a reasonable period of time;
- Doubt over the real beneficiary of the account;
- Accounts opened with names very close to other established business entities;
- Several accounts having a common account holder or authorized signatory or associated account holders and authorized signatories with no explanation;
- Unusual activity compared to past activity (spike in transaction volume/amount, dormancy to activity spike, etc.);
- Activity inconsistent with what would be expected from declared business;
- Doubtful source of funds;
- Transaction values just under the reporting threshold; and
- Use of a mixer, tumbler or fogger.

A Higher-Risk Customer Types list is maintained by the AML Officer and is reviewed at least annually.

3.3.1.3.2. EDD REQUIREMENTS

EDD will include some or all of the following, conducted upon the customer being identified as higher risk:

- Negative news and internet searches of the customer, and for legal entities also the controlling principal, beneficial owners, and ultimate parent;
- Collection of additional CIP documents;
- Collection of information on the customer's banking relationship with other institutions;

- Collection of information on the purpose of transactions;
- Meeting with Cethereum personnel;
- Assessment of expected transactional activity;
- Review of actual transactional activity against expected activity; and
- Collection of information for legal entity customers, including:
    - Legal formation number assigned by the formation entity and formation documents for corporate entities;
    - AML programme information, if applicable;
    - Beneficial owners, controllers, and signatories of legal entity customers.

Cethereum will not allow customers awaiting completion of EDD to deposit funds or conduct transactions of any kind. Cethereum's policy is to not permit individuals or legal entities who fail required EDD to maintain accounts of any kind.

In the event that:

- EDD measures cannot be applied; or
- the customer cannot or will not provide the EDD information requested; and/or
- the customer has provided information that is false or contains significant inconsistencies that cannot be resolved after further investigation,

then the Company will suspend the due diligence and on-boarding process, notify the AML Officer, and the Company will not enter a relationship with the customer or open the account, or the Company will exit the existing relationship within thirty (30) calendar days. If appropriate, the AML Officer may escalate such customers for potential investigation of suspicious activity if Cethereum identifies reportable suspicious activity identified in the due diligence processes.

Any transaction of $100,000 or more shall not be processed before determining if the requesting party is a PEP.

Certain transactions will require confirmation as to proof of funds before they can be made. These are:

- Any transaction from a PEP customer;
- Any transaction from a non-PEP customer with a fiat value in excess of $10,000; and
- Any transaction from a non-PEP customer which would result in that customer having completed transactions with a fiat value of more than $10,000 in the previous 12 months.

Customers requested to provide confirmation of source of funds should provide:

- An explanation of where the funds for the trade in question have originated (from income, savings, liquidation of another asset, etc.).
- Depending on the explanation of the source of funds, documentary evidence of the explanation, such as copy bank statements, investment account records or a solicitors' or accountants' letter confirming source of funds (such professional being in good standing).
- In the case of cryptocurrency-to-fiat transactions, evidence of the original fiat-to-cryptocurrency transaction and the source of the fiat funds for that original acquisition. This will include details of the original transaction or transactions, including time, date and transferor/transferee wallet details. The Company reserves the right to carry out due diligence via analysis of the blockchain to verify past transactions, including cross checking against any "blacklisted" wallets associated with historical illegal behaviour (such as the Mt. Gox theft or wallets linked to cyber-extortion). With some cryptocurrencies (such as XRP and some altcoins), blockchain analysis may not be possible, in which case the customer will be expected to provide independent verification of historical transactions.

For high value transactions, Cethereum staff also reserve the right to verify that the cryptocurrency wallet from which a client is sending cryptocurrency or to which Cethereum is asked to send cryptocurrency belongs to that client. This will typically consist of a small pilot transfer of cryptocurrency to the client wallet which the client will transfer back to evidence of client wallet control.

The AML Officer should be consulted in each source of funds request and, following receipt of relevant documentation, his/her consent obtained before any transaction may take place.

3.3.1.4.PROHIBITED CUSTOMER TYPES

The process of the customer identification programme and due diligence enables the business to determine whether a potential customer is a "prohibited customer" who is prohibited from using the Company's products and services (**"Prohibited Customers"**). Prohibited Customers are individual or legal entity customers that appear to be involved in activity that may be illegal or poses potential legal, regulatory, reputational, or sanctions risk or penalties that exceed the Company's risk appetite. Specifically, it is the Company's policy to prohibit the following types of individuals and legal entities from using the Company's products and services:

- Individuals and legal entities whose wealth or funding appears to be accumulated through corruption or activities that are illegal in the Canada, the United States of America or in the country of origin;
- Entities that issue shares in bearer form;
- Payable-through-accounts and nested accounts;

- Non-traditional financial services companies (unless expressly approved by the AML Officer) including casas de cambio, exchange houses, check cashers, and currency dealers or exchangers);
- Individuals and legal entities who are designated under OFAC;
- Individuals and legal entities whose identities are not known or cannot be verified as per the CIP and due diligence sections above;
- Individuals and legal entities included in (or closely associated with those included in) Cethereum's internal watch list;
- Individuals and legal entities whose accounts were previously closed, and the relationship terminated by the Company for AML, sanctions, or other anti-financial crime compliance reasons;
- Individuals and legal entities whose accounts on other platforms, or in other financial institutions, were previously closed and the relationship terminated by the service provider for AML, sanctions, or other anti-financial crime compliance reasons; and
- Individuals or legal entities who the AML Officer or designee deems to pose unacceptable money laundering or sanctions risk.

The specific types listed above are representative, but not exhaustive. The Company shall review and update this designation at least annually.

In the event that it is unclear whether a party is a Prohibited Customer, the decision must be escalated to a higher, qualified authority (e.g. the AML Officer) who shall take into consideration the elements of the Company's reputational risk policies and practices. If the Company finds that an individual or legal entity should be classified as a Prohibited Customer, the Company will suspend the due diligence and on-boarding process, notify the AML Officer, and the Company will not enter a relationship with the customer or open the account, or the Company will exit the existing relationship within thirty (30) calendar days. Prohibited Customers may also be escalated for potential investigation of suspicious activity, as appropriate.

3.3.1.5. PERIODIC REVIEWS

Throughout the course of a customer relationship, certain occurrences or changes in a customer's profile or activity may impact or raise concerns regarding the money laundering and sanctions risk of that customer. Cethereum will ensure, on a risk-based approach, that customer information is maintained, updated, and refreshed after account opening, and that transactional activity is incorporated into the Company's understanding of the customer's risk, on an on-going basis. All customers identified as higher risk and subject to EDD, including a customer who has a change in profile, or who requested activity or modified terms of service (such as increasing transaction limits), will be reviewed after account opening as appropriate and at least every six (6) months, and all other customers are reviewed at least every twelve (12) months. The scope of the review includes:

- Confirming that CIP was performed and all CDD and EDD information in a customer's file is current;
- Incorporating any new or additional information on the customer since the last review;
- Including information regarding the transactional activities of the customer; and
- Considering the results of transaction monitoring and case investigations, as relevant.

The Company will record the steps taken and the results of the review.

At a minimum, all CIP/CDD/EDD documentation for every customer (and associated parties) will need to be refreshed with current documentation upon the expiry of previously relied upon documentation, based on either an explicit expiry date or the lapse of the document's referred year.

Additionally, a fresh PEP and sanctions check must be conducted on each customer and associated parties every three months from initial onboarding, or, if a customer has not traded in the previous three months, before any subsequent trade can be executed.

3.3.2. TRANSACTION MONITORING AND SUSPICIOUS ACTIVITY/TRANSACTION REPORTING

Cethereum monitors customer activity to detect unusual or suspicious transactions. Cethereum's policy is to take a conservative approach to monitoring by setting low dollar monitoring thresholds commensurate with the Company's high money laundering and sanctions risk in its activities. The Company will deny accounts that exceed set limits or display unusual activity. At a minimum, the Company will monitor all transactions, including fiat currency and virtual currency transactions, at the customer and account levels, for:

- Customers who appear to be structuring to avoid certain financial reporting (i.e. smurfing, etc.);
- Unusually large transactions;
- Customers who change linked bank accounts frequently;
- Multiple accounts or transactions assigned to one business number, address, or telephone number;
- Transactions with high-risk geographies;
- Customers for whom increased monitoring would be appropriate, including those considered to be higher risk and those on an internal Cethereum watch list;
- Use of a mixer, tumbler or fogger; and
- Previously dormant accounts.

The AML Officer will ensure that his or her staff review alerts in a timely fashion. In addition, the Company requires all personnel to report any unusual customer or transactional activity they observe to the AML Officer. The AML Officer will ensure that all employees receive training on how to report unusual activity as part of the AML compliance training programme. The AML Officer will set transaction monitoring thresholds. The AML Officer reviews the sufficiency and calibration of the thresholds no less than annually and will have authority to make changes including as needed in response to emerging patterns of activity. The AML Officer will document and retain the rationale for raising or eliminating a monitoring threshold and report that to Executive Management for approval. Executive Management must also ratify lowering a monitoring threshold or imposing a new threshold. However, in the event that new patterns of suspicious activity emerge prior to Executive Management approving such a change, the AML Officer is authorized to impose new thresholds pending Executive Management's approval. The AML Officer will ensure that the rationale for all changes in thresholds is documented and retained.

Cethereum must report suspicious transactions to FINTRAC as soon as practicable after first detection. The AML Officer will complete the Suspicious Transaction Report and retain a copy of these reports for audit purposes.

3.3.3. SUSPENSION, TERMINATION, AND CANCELLATION OF CUSTOMER ACCOUNTS

The AML Officer is permitted to suspend, restrict, or terminate a customer's access to any or all of Cethereum's services, or deactivate or cancel accounts that have been identified as posing unacceptable money laundering or sanctions risk to the Company. This includes accounts for which:

- Cethereum is so required by a personally served valid subpoena, court order, or binding order of a government authority;
- Cethereum reasonably suspects the customer of using its Cethereum Account in connection with a prohibited business or practice that violates this Policy;
- Use of a Cethereum Account is subject to any pending litigation, investigation, or government proceeding and/or the Company perceives a heightened risk of legal or regulatory noncompliance associated with account activity;
- The Company's service partners are unable to support the account use;
- The customer takes any action that Cethereum deems as circumventing Cethereum's controls, including, but not limited to, opening multiple Cethereum Accounts or abusing promotions which Cethereum may offer from time to time;
- The account:

- involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity;

- is designed to evade the requirements of AML laws and regulations to which Cethereum is subject, whether through structuring or other means;

- Serves no business or apparent lawful purpose, and Cethereum knows of no reasonable explanation for the transaction after examining all available facts; and/or

- Involves the use of the Company to facilitate criminal activity.

If Cethereum suspends or closes an account, or terminates use of Cethereum services for any reason, it will provide the customer with notice of the Company's actions unless a court order or other legal process prohibits Cethereum from providing such notice.

3.3.4. OTHER REGULATORY REPORTING AND RECORDKEEPING

3.3.4.1. FUNDS TRANSFER RECORDKEEPING

The Company collects and maintains records of all funds transmittals valued at $1,000 or more in aggregate on the same day per customer. The following information is included for each such transaction record:

- Name of the transmitter and, if the payment is ordered from an account, the account number;
- Address of the transmitter;
- Amount of the transmittal order;
- Date of the transmittal order;
- The exchange rates used and their source;
- Identity of the recipient's financial institution; and
- As many of the following items as possible:
    - Name and address of recipient;
    - Account number of the recipient;
    - Every transaction identifier, including the sending and receiving addresses;
    - Any other specific identifier of the recipient;
    - Either the name and address or the numerical identifier of the transmitter's

financial institution.

The Company makes record and reports to FINTRAC, within five working days, transactions of $10,000 or more in a single transaction (or in aggregate within a 24-hour period by, for, or to the benefit of the same party) and that contains the following information:

- the date of the receipt;
- if the amount is received for deposit into an account, the name of each account holder;
- the name and address of every other person or entity that is involved in the transaction, the nature of their principal business or their occupation and, in the case of a person, their date of birth;
- the type and amount of each virtual currency involved in the transaction;
- the exchange rates used and their source;
- the number of every other account that is affected by the transaction, the type of account and the name of each account holder;
- every reference number that is connected to the transaction and has a function equivalent to that of an account number;
- every transaction identifier, including the sending and receiving addresses;
- If the amount is received from someone acting on behalf of a third party:
    - if the third party is a person, their name, address and date of birth and the nature of their principal business or their occupation;
    - if the third party is an entity, its name and address, the nature of its principal business, its registration or incorporation number and the jurisdiction and country of issue of that number; and
    - the relationship between the third party and the person from whom the fiat or virtual currency is received; and
- If third party involvement cannot be verified, but is suspected, the Company shall keep a record stating:
    - whether, according to the person from whom the fiat or virtual currency is received, they are acting on their own behalf only; and
    - the reasonable grounds to suspect that they are acting on behalf of a third party.

Cethereum shall maintain required records for a period of at least five years in a form that facilitates reconstruction of individual transactions and allows prompt retrieval in response to regulatory or law enforcement requests.

3.3.5. INFORMATION SHARING

The Company will cooperate fully with federal government authorities, law enforcement authorities, and financial institution partners on AML compliance investigations to the extent allowable under applicable privacy and other laws.

The AML Officer will establish systems and procedures to ensure that the Company:

- Establishes a central process for receiving, documenting, and responding to requests for information sharing and subpoenas, and ensuring that these procedures include notification of the AML Officer to allow for the review of customer activity; and
- Promptly evaluates all information sharing requests received, including those from its financial partners, and provides timely responses with all information that Cethereum is legally allowed to share.

Other than these processes, the Company does not disclose information relating to its transaction monitoring activities to third parties except with the written consent of the AML Officer. The Company prohibits employees from disclosing information about its AML compliance activities or Policy without receiving written permission from the AML Officer.

3.3.6. OVERSIGHT OF OUTSOURCED SERVICE PROVIDERS

Cethereum may outsource specified systems and controls to service providers, which the Company defines to include affiliates as well as third parties. However, in all cases the Company retains full responsibility for complying with AML laws and regulations, as well as ensuring the full implementation of the Policy. The AML Officer, in conjunction with Executive Management and legal counsel, is responsible for approving contracts and agreements with affiliated and third party service providers that impact the implementation of the Policy to ensure that every contract clearly identifies the service provider's roles, responsibilities, performance standards, reporting obligations, and liabilities. These agreements include the service provider's obligations to provide documentation on customer information and investigations, and clearly detail the Company's requirements for internal controls, audit reviews, and the conditions for the termination of the affiliate or supplier relationship.

The AML Officer oversees all service providers that perform risk management and control processes whose activities significantly impact Cethereum's Policy. This oversight includes:

- Conducting due diligence on capabilities ahead of approving the decision to outsource;
- Establishing SLAs[12] setting standards the service provider must meet;
- Requiring the service provider to provide training to applicable employees that is broadly equivalent to the training that a Company employee would receive to fulfill the same role;
- Requiring reporting on performance against SLAs; and
- Performing periodic testing of service providers' performance as per SLA requirements.

[12] "Service Level Agreements"

3.3.7. SANCTIONS COMPLIANCE

The AML Officer will establish and maintain controls to ensure that Cethereum complies with sanctions regulations to enforce economic and trade sanctions, including OFAC. These controls will apply to all parties with which the Company does business, including, but not limited to, customers, other transaction parties, and Cethereum personnel. The AML Officer will establish and oversee systems and procedures to ensure that the Company:

- Fully incorporates sanctions risk within its AML risk assessment;
- Screens each customer and other transaction party[13] subject to CIP against OFAC sanctions programmes at account opening and prior to processing any transaction;
- Screens Cethereum personnel prior to doing business with them;
- Updates internal OFAC and other applicable lists in a timely fashion when OFAC announces changes to sanctions programmes;
- Prevents all customers under review for a potential OFAC hit from conducting transactions;
- Reviews all transactions identified through screening as potential OFAC violations;
- Documents rationale for clearing all false-positive OFAC hits;
- Blocks or rejects transactions as appropriate under Canadian sanctions law;
- Reports blocked and rejected items to OFAC and prepares annual reports to OFAC on the total of blocked funds; and
- Establishes similar controls in relation to U.N. sanctions lists and other applicable sanctions programmes.

At this time the Company has identified the following as sanctioned nations, in accordance with OFAC guidance:

1) Democratic People's Republic of Korea (North Korea);
2) Belarus;
3) Burundi;
4) Central African Republic;
5) Cuba;
6) Democratic Republic of the Congo;
7) Iran;
8) Iraq;
9) Lebanon;
10) Mali;

[13] Includes known beneficiaries of payments (including as permitted in virtual currency transactions) and associated parties such as beneficial owners and controllers of accounts identified by CIP and CDD.

11) Nicaragua;
12) Somalia;
13) Sudan;
14) South Sudan;
15) Syria;
16) Ukraine;
17) Russia;
18) Venezuela;
19) Yemen; and
20) Zimbabwe.

3.3.8. MECHANISMS DESIGNED TO MONITOR ONGOING COMPLIANCE

3.3.8.1. STAFFING

The AML Officer will ensure that he or she has adequate staffing, both in numbers and qualifications, to implement the Policy effectively, or request additional resources from Executive Management as needed. At least annually, the AML Officer will present his or her approach to staffing to Executive Management for approval and will ensure that all activities performed on behalf of the Company comply with Company policies and procedures and all applicable regulatory requirements regardless of the personnel performing the tasks.

3.3.8.2. REPORTING

To ensure effective Executive Management and Board oversight of the Policy, the AML Officer reports at least quarterly on the status of the programme to Executive Management and the Board. The reporting is compiled by the AML Officer, and may include:

- Overall AML compliance risk levels against the targeted risk level;
- Progress in implementation of the Policy, such as:
  - KYC metrics;
  - Suspicious activity/transaction monitoring (transactions processed, cases generated, etc.);
  - Training sessions scheduled and completed; and
  - Q and A reviews and results.
- AML compliance trends;
- Material Policy compliance issues and/or escalated issues;

- Emerging AML compliance issues, which the Company will need to address;
- Status of Policy corrective actions; and
- Independent testing findings, financial partner concerns, and/or regulatory concerns.

No less than annually, the AML Officer will provide a report on the state of Policy compliance and any significant emerging issues that will assist Executive Management and the Board in evaluating any Policy changes that may be appropriate.

3.3.8.3. QUALITY ASSURANCE AND TESTING

A quality assurance testing programme helps to ensure that the Company maintains a high-quality AML programme by implementing monitoring processes to promptly identify systematic errors and control deficiencies. Quality assurance testing may review the Company's:

- KYC programme;
- Transaction monitoring;
- Regulatory reporting, to the extent applicable in the previous year;
- Referrals to financial partners;
- Information sharing;
- Sanctions screening;
- Record-keeping; and
- Training.

The AML Officer is responsible for overseeing quality assurance testing, taking necessary corrective action to remediate findings, and reporting such information to Executive Management and the Board.

3.3.8.4. NEW PRODUCTS OR BUSINESS PRACTICES

All new or modified products or services, distribution channels, geographies, and business initiatives or practices require, among other things, sign-off by the AML Officer. The AML Officer evaluates from a compliance perspective the risks to ensure that any such risks are appropriately identified and mitigated. The AML Officer updates the AML risk assessment when such practices are introduced and ensures the Company implements any needed additional controls before adopting the new or modified product or practice.

3.3.8.5. TRAINING AND DEVELOPMENT

The Company requires that the Board and all Cethereum personnel whose jobs impact the Company's AML compliance receive AML compliance training appropriate to their roles and responsibilities at least on an annual basis. In addition, orientation for all new personnel should contain an overview of the requirements of AML compliance and this Policy. The goals of Cethereum's AML compliance training programme are to:

- Ensure that the Board and Executive Management are knowledgeable regarding Cethereum's obligations and responsibilities under AML law;
- Ensure Cethereum personnel are familiar with relevant AML compliance requirements pertaining to their specific job functions and that they receive the most current information available;
- Encourage an understanding of the significance of Cethereum's AML efforts and help develop a strong culture of AML compliance across the Company; and
- Develop a cadre of personnel and managers throughout Cethereum to detect, escalate, and manage AML compliance-related risks as and when they arise.

Consistent with this Policy, the AML Officer is responsible for ensuring that a risk-based AML compliance training programme is developed, that it is presented to Executive Management for approval and that employees in need of advanced training receive such training and that records of training attendance are maintained.

3.3.8.6. INDEPENDENT TESTING

The Board oversees the completion, at least every two years, of an independent review and test of Cethereum's AML compliance by a qualified third party, for the purpose of assessing the implementation and effectiveness of the Policy and the adequacy of its controls over AML compliance risk. The AML Officer is responsible for updating Cethereum's AML compliance risk assessment in light of any issues raised during the independent testing and taking necessary corrective action to remediate findings.

4. POLICY ADMINISTRATION

4.1. DEVELOPMENT, REVIEW, AND APPROVAL

This Policy is presented to the Board, or a designated Board committee, for review and approval at least annually or upon any request for significant modifications to this Policy.

The AML Officer is responsible for the custody and issuance of this Policy. Under the direction of the AML Officer, this Policy and related procedures are required to be reviewed and reaffirmed, or appropriate updates to it will be recommended to the Board, at least annually or more frequently as appropriate. The review includes consideration of current, and changes in, applicable laws, regulations, or regulatory guidance, current and changes in the Company's products and services or operating geographic locations; feedback on the effectiveness of the Policy, and any supervisory and/or audit input. The AML Officer, if necessary, may consult legal counsel.

The AML Officer may make minor modifications or supplement this Policy without Board approval, so long as these changes are within the principles and limits of this Policy and do not have the effect of reducing them. The AML Officer ensures that development and any revision of this Policy includes circulating a draft to all relevant stakeholders (including Executive Management) for review and feedback and reflecting the consideration of any applicable law and supervisory or relevant third party input.

4.2. COMPLIANCE

4.2.1.VARIANCES

No part of this Policy or its supporting procedures should be interpreted as contravening or superseding other legal and regulatory requirements imposed upon Cethereum, including financial partner requirements.

Any conflicts between this Policy and other legal obligations must be submitted immediately to the AML Officer for further evaluation. The AML Officer, if necessary, will consult outside legal counsel, and if appropriate will report the conflict and its resolution to Executive Management and the Board. All variances to this Policy must be approved by the AML Officer and at least one member of Executive Management.

4.2.2. EXCEPTIONS

All exceptions to this Policy require the approval of the AML Officer and the Board. The Company must apply for an exception to this Policy by contacting the AML Officer in writing and the AML Officer must inform Executive Management, report the exception request and recommendation to the Board, and take additional measures to effectively handle money laundering and/or sanctions risk. Additionally, the AML Officer will review the conditions that led to the exception, evaluate corrective actions, and identify an appropriate action plan to either return to compliance with this Policy or seek modification to the Policy. Action plans to cure exceptions to this Policy will be presented to the Board for review and approval or review and rejection, as appropriate. Questions or suggestions about this Policy should be directed to the AML Officer.

4.2.3. BREACHES

The Policy prohibits Company personnel from participating in any activity that facilitates money laundering or terrorist financing, or knowingly violates legally applicable sanctions. The Company does not tolerate: any conscious avoidance of facts; a failure to resolve indicators of potentially suspicious activity or possible violations of law, or other significant inconsistencies that arise in review of a customer's due diligence or transaction activity; or negligence on the part of its personnel. This Policy prohibits advising or providing any other assistance to individuals for the purposes of circumventing financial crime laws or regulations or Company internal procedures.

Company personnel are required to promptly report any breach of or non-compliance with this Policy to the AML Officer. The AML Officer ensures Cethereum personnel can report violations of this Policy anonymously by phone and/or e-mail. The AML Officer further ensures that this mechanism is well-publicized to all employees and takes all possible steps to ensure reports of potential violations remain anonymous and confidential. Cethereum never tolerates retaliation of any kind against an employee who reports a potential violation of the Policy. Any employee who commits such retaliation, or otherwise violates this Policy, will be subject to the Consequences of Non-Compliance section of this Policy. The AML Officer, or designee, must track the remediation and disposition of an identified Policy breach. The AML Officer, if necessary, will consult outside legal counsel. Where appropriate, the AML Officer is responsible for informing the relevant authorities.

4.2.4. CONSEQUENCES OF NON-COMPLIANCE

Cethereum recognizes that if it fails to comply with this Policy and applicable AML laws and related regulations, it could result in significant adverse legal, reputation, and financial impact on the Company.

All Cethereum personnel are responsible for assisting in Cethereum's compliance with applicable AML laws and related regulations. All Cethereum personnel are responsible for understanding this Policy and undertaking any specified responsibility assigned to them. Compliance with the requirements of this Policy and applicable AML laws and related regulations must be included as applicable in the job descriptions and performance evaluations of Cethereum personnel. The AML Officer, at his or her discretion, may provide input into any employee's performance evaluation. Personnel who fail to comply with this Policy will be held accountable for their performance and may be subject to disciplinary action up to, and including, termination of employment in appropriate cases. Individuals who fail to comply with the applicable AML laws and related regulations can also be subject to personal liability such as civil and/or criminal penalties and imprisonment, and as such may be referred to law enforcement or regulatory authorities in accordance with the requirements of the relevant government authority.

4.3. COMMUNICATION PLAN AND CONTACT

Upon the Policy's approval, the AML Officer is responsible for communicating this Policy through the following channels:

- Sending an e-mail to stakeholders detailing material updates; and
- Publishing the Policy and related documentation to the location as agreed by the stakeholders.

The AML Officer is available for consultation on the interpretation and administration of this Policy.