

Anti-Money Laundering & Combating the Financing Of Terrorism Policy of Gatepost N.V.

Last updated: 20th May 2025 - Version 1.2

Please read this information carefully for your own benefit.

www.coinhero.io is operated by **Gatepost N.V.** having its office at Landhuis Zuikertuintje, Zuikertuintje z/n, Willemstad, Curacao. Company Registration number 163081.

Section 1. Purpose

This document deals with the measures implemented by GATEPOST N.V., hereinafter referred to as the “company”, to prevent anti-money laundering (AML) within gaming. Together with individual and corporate obligations, it describes the methods that can potentially be used to carry out money laundering in gaming, our identification techniques and the procedures to follow when money laundering is discovered. A reporting process is detailed for all suspicious activity towards the end of the document.

The company takes a zero-tolerance approach to being involved in illegal/illicit activity, and will fully comply with all relevant sections of the AML/CFT/CFP Regulations for the online gaming sector of Curacao, alongside the other legislations, including the:

- National Ordinance on identification when rendering services;
- National Ordinance on the reporting of unusual transactions;
- Sanctions National Ordinance; and
- Kingdom Sanction Act.

All partners and employees of the company are under obligation and duty to comply with the above. This policy & any related procedures aims to help Directors, Managers and staff fulfil these responsibilities, by providing a clear framework, along with setting out the Company’s key principles and obligations.

- Failure to fulfil these responsibilities may result in disciplinary action and may also result in criminal sanctions for the staff involved.
- Breaches may also be reportable to our Compliance Officer or MLRO, which may result in professional disciplinary action.
- Furthermore, a report may also have to be made to the law enforcement agencies, which may result in criminal investigation.

As a company, we are committed to carrying out business in accordance with the highest ethical standards. This includes complying with all applicable laws and regulations aimed at combating money laundering and terrorist financing. This Policy has been developed by the Company to reduce the risk of money laundering and terrorist financing associated with its business and the sale of its products. This Policy explains our individual responsibility in complying with anti-money

laundrying and counterterrorist financing laws ("AML Laws") around the world and ensuring that any third parties that we engage to act on our behalf, do the same.

The Anti-Money Laundering Policy ("AML Policy") applies to the Company, its direct wholly- and majority-owned subsidiaries and their directors, officers, full-time, part-time and seconded employees, and anyone working on the Company's behalf, e.g. consultants and representatives (collectively "Personnel", or the "Employees"). Personnel are expected to act in a manner that will enhance the Company's reputation for honesty, integrity, and reliability. The AML Policy applies in all countries in which the Company operates or conducts business. When the laws of those countries require a higher standard, such standard shall apply. Adherence to this AML Policy is a condition of employment and/or engagement with the Company, and therefore the Employees must acknowledge on an annual basis that they have understood the AML Policy and have disclosed any suspected and actual violations through appropriate channels.

The AML Policy will not give answers for every ethical or legal situation. If Employees have any doubts about the right thing to do, they should seek advice from the relevant member(s) of Compliance or from the General Counsel, as appropriate.

If Employees violate the Company's policies and procedures or any of the laws that govern the Company's business, the Company will take immediate and appropriate action up to and including termination of employment.

The purpose of this AML Policy is to substantially prevent, manage and mitigate the risk that the Company and their Employees become directly or indirectly involved in actual or potential money laundrying activities, or terrorist financing activities.

This AML Policy sets out the key principles and obligations in relation to the AML Framework in order to identify and assess the Money Laundrying ("ML")/Terrorism Financing ("TF") risks to which the Company is exposed to ("ML/TF", respectively the "AML" measures, or more broadly "AML"), as defined below.

For this AML Policy, a counterparty comprises of: the Company's shareholders, companies that the Company has invested in, Employees, financial institutions, service providers and any business relationship. A 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by such law, and which is expected, at the time when the contract is established, to have an element of duration.

If you have any questions about this Policy, you should contact the Ethics and Compliance or the Legal Department.

Section 2. Definitions of money laundering and terrorism financing

Money Laundering is the process by which it attempts to hide and disguise the true origin and ownership of the proceeds from criminal activities, thereby avoiding prosecution, conviction and confiscation of criminal funds.

Money laundering means exchanging money or assets that were obtained criminally for money or other assets that are 'clean'. The clean money or assets don't have an obvious link with any criminal activity. Money laundering also includes money that's used to fund terrorism however it's obtained.

The following types of activities are considered to be "money laundering" and are prohibited under this Policy:

- a) the conversion or transfer of property (including money), knowing or suspecting that such property is derived from criminal or certain specified unlawful activity ("criminal property"), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;
- b) conducting a financial transaction which involves criminal property;
- c) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, ownership or control of criminal property;
- d) the acquisition, possession or use of criminal property;
- e) promoting the carrying on of unlawful activity; and
- f) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

The broad definition of money laundering means that anybody (including any the Company employee) could be in violation of the law if he/she becomes aware of, or suspects, the existence of criminal property within the business and becomes involved in or continues to be involved in a matter which relates to that property being linked to the business without reporting his/her concerns.

Property can be criminal property where it derives from any criminal conduct, whether the underlying criminal conduct has taken place in the country where you are situated or overseas.

Terrorism Financing means: the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any terrorist act.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Responsibilities

The teams / person responsible for the implementation and effectiveness of this policy are:

- **Payment Officer:** Processes customer payments, performs basic CDD, flags anomalies, and ensures accurate transaction recordkeeping.
- **Chief Financial Controller:** Monitors financial risks, reviews sources of funds, supports MLRO with suspicious activity detection, and integrates AML into financial oversight.
- **Compliance Officer:** Implements AML procedures, ensures CDD and CAP compliance, coordinates risk assessments, manages policy updates, and conducts staff training.
- **Money Laundering Reporting Officer (MLRO):** Oversees AML compliance, manages internal and external STRs, liaises with authorities, reviews high-risk cases, and assesses control effectiveness.

Section 3. Enforcement

Any employee found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment. Companies contracted to the Company found to be violating this policy will be deemed to be in breach of contract.

Section 4. Revision and Changes

All the Company procedures are subject to an annual revision which has to be completed before the annual financial audit of the company. Significant changes to any policy or procedures are to be approved by the Key Official and communicated to the relevant Authorities.

Section 5. Anti-Money Laundering Policy

Gaming operations are exposed to financial and reputational risk posed by fraud and money laundering. Good controls should be in place in order to establish a complete set of monitoring techniques to detect and continuously combat money laundering. Having controls and processes in place that can detect and prevent Money Laundering constitutes an essential part of sound risk management; it helps to protect the integrity of the company and its operations by reducing the likelihood of it becoming a vehicle for or a victim of financial crime. It forms part of a general responsibility to uphold the soundness of the financial system which we form a part of.

Section 5.1 Business Risk Assessment

In compliance with the Curaçao Gaming Authority's AML/CFT regulations, Gateopost N.V. conducts a comprehensive Business Risk Assessment (BRA) to identify and evaluate the money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks associated with our operations. This assessment considers factors such as the nature of our products and services, delivery methods, customer demographics, and geographic locations. The BRA is reviewed and approved by senior management and updated regularly to reflect changes in the business environment or emerging risks. The findings inform the development and implementation of appropriate policies, controls, and procedures to mitigate identified risks.

Section 5.2 Customer Risk Assessment

Prior to establishing a business relationship, Gatepost N.V. performs a Customer Risk Assessment (CRA) to evaluate the potential ML/TF/PF risks posed by individual customers. This assessment involves collecting detailed information about the customer, including identity verification, source of funds, and transaction patterns, to develop a risk profile. Customers are categorized into risk levels, low, medium, or high, based on the assessment. The CRA is conducted at the outset of the relationship and updated periodically or when there are significant changes in the customer's circumstances. The results guide the application of appropriate Customer Due Diligence (CDD) measures.

Section 5.3 Customer Acceptance Policy

Based on the outcomes of the CRA, Gatepost N.V. establishes a Customer Acceptance Policy (CAP) to determine the appropriate level of CDD to apply. The CAP outlines criteria for accepting or rejecting customers, considering factors such as risk level, source of funds, and compliance with regulatory requirements. Special attention is given to Politically Exposed Persons (PEPs), individuals from high-risk jurisdictions, and those subject to international sanctions. PEP status is assessed using reliable and independent sources, and enhanced due diligence measures are applied accordingly. The CAP is reviewed and approved by senior management and is aligned with the company's overall AML/CFT strategy.

Section 5.4 Customer Due Diligence

The Company implements a risk-based approach to Customer Due Diligence (CDD) in accordance with Curaçao's AML/CFT regulations. CDD measures are applied when:

- Establishing a business relationship.
- Carrying out occasional transactions equal to or exceeding NAf. 4,000 (approximately €2,000).
- There is suspicion of money laundering or terrorist financing.
- Doubts exist about the veracity or adequacy of previously obtained customer identification data.

CDD procedures include:

- Identifying and verifying the customer's identity using reliable, independent source documents.
- Understanding the nature and purpose of the business relationship.
- Conducting ongoing monitoring of the customer's transactions to detect and report suspicious activities.

Enhanced Due Diligence (EDD) is applied to higher-risk customers, such as PEPs or individuals from high-risk jurisdictions. EDD measures may include obtaining additional information on the customer's source of funds and the purpose of transactions. All CDD and EDD measures are documented, proportionate to the assessed risks, and reviewed periodically.

Section 6. General Policy

To initiate AML Procedures the Company will adhere to the requirements of the Prevention of Money Laundering Act, the regulations and any guidance notes the Company and shall as a minimum:

- Appoint one of its senior officers as the designated Compliance Officer whose responsibilities will include the duties required by the laws, regulations and guidance notes.
- Retain identification and transactional documentation as defined in the laws, regulations and guidance notes.
- Keep at all times a secure online list of all registered players.
- Take reasonable steps to establish the identity of any person for whom it is proposed to provide this service. For this purpose, the process for the registration of players provided for under the General Terms and Conditions provides for the due diligence process that must be carried out before the opening of a User Account.
- Ensure that this policy is developed and maintained in line with evolving statutory and regulatory obligation and advice from the relevant authorities.
- Provide initial and on-going training to all relevant staff so that they are aware of their personal responsibilities and the procedures in respect of identifying players, monitoring player activity, record-keeping and reporting any unusual/suspicious transactions.
- Report any suspicion or knowledge of money laundering or terrorism financing to the Financial Intelligence Unit (FIU) set up by law as a Government Agency responsible for the collection, collation, processing, analysis and dissemination of information with a view to prevent money laundering and combat the funding of terrorism.
- Examine with special attention, and to the extent possible, the background and purpose of any complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.
- Co-operate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity.

Section 7. Continuous Monitoring and Control

In gaming, rousing of suspicions of money laundering should occur when certain client behaviors are observed, these can manifest as but are not limited to one or many of the below:

- Observing money being placed into the site and then withdrawn in a different way either before or after gaming, especially if the depositing and withdrawing methods are located in different countries. Note with an e-wallet it's generally not possible to know the country where funds are going; unsurprisingly e-wallets are commonly used for money laundering.
- Suspecting an account is being controlled under a false identity either with fake documentation being supplied or with genuine documentation but the account being controlled not by the person who is stated / verified on file.
- Observing a customer holding large volumes of money in the site unnecessarily/not to game (to conceal it from authorities).

- Observing manipulated game play is designed to deliberately move money from account to account or to manipulate the odds of the game.

Section 8. Specific Policy

The following are some specific cases where monitoring and control should be exercised. Monitoring and control should not be limited only to the following list of cases.

Section 8.1 Know Your Client Procedure

Each client must register and follow the KYC procedure. This procedure is the root of identifying and verifying the players that have access to the system, effect financial and gaming transactions and participate in the games offered.

Minimum-level CDD measures are to be applied at account opening by collecting personal details and conducting PEP and sanctions screening. The following personal details are to be collected for identification purposes:

- Name and surname
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number
- Email Address
- Contact Number

When unable to comply with these requirements, players will be unable to open an account with the Company.

In such scenario identify verification will be carried out on the basis of risk using reliable, independent, source documents such as:

- Driver's license;
- ID card; and
- Passport.

Furthermore, the company reserves the right to verify the residential address by obtaining any of the following documents **not older than 6 months**:

- Bank statement
- Utility Bill
- Rental or lease agreement
- Official correspondence from a central or local government authority, department or agency

If inconsistencies are identified, the Company will apply more in-depth verification measures, by using methods such as go-location information, IP address data and other technological measures.

Following identity verification, the Company will carry out a CRA in order to have sufficient information available to detect unusual transactions during the course of the business relationship. The CRA will be conducted to classify players as posing a low, medium or high risk to the Company in accordance with the Customer Acceptance Policy (CAP).

Section 8.2 Unusual Transactions

In case of unusual or unreasonable transactions, employees should report the transaction to the relevant individuals. The Compliance Officer should always be informed and have the case investigated. Each suspicious transaction should be reported to the relevant authority accordingly.

Section 8.3 Cash Transactions

Cash transactions for player deposits or withdrawal are not allowed. Player deposits and withdrawals must be made through the available payment options.

Section 8.4 Withdrawal Processing

All withdrawals should be checked before being processed. The Fraud Team should check each withdrawal for unusual activity. Any unusual transaction should not be processed before investigated and verified as being legitimate.

Section 8.5 Abnormal Transactions

Abnormal transactions refer to substantial deposits and withdrawals or substantial wins or losses as compared to average player activity. In case of abnormal transactions, employees should investigate the abnormality of the transaction and if the outcome is still not clear report the transaction to the Money Laundering Reporting Officer in order to investigate the case further. The checks should include but not limited to verify player, check game play and verify account activity. Each suspicious transaction should be reported to the relevant authority accordingly.

High rollers and VIP players should be earmarked to avoid confusion; nonetheless, their transactions should still be monitored accordingly.

Section 8.6 Payment Options

Withdrawals should only be processed to the same payment option used for depositing. If this is not possible use a method that can be verified, using any means stipulated above to ensure that is in the name of the same person making the deposit.

Section 8.7 Suspicious Transactions

Investigate and report all suspicious transactions.

Section 8.8 Transaction Recording

All player financial and gaming transactions should be recorded and accounted for.

Internal Financial Transactions

Internal financial transactions should also be recorded and accounted for. The CFO should follow the Accounting Standards accordingly.

Section 8.9 Transaction Monitoring

Both player and corporate transactions should be monitored continuously and where possible implement verification requirements for substantial transactions. As part of the ongoing monitoring process, transaction monitoring is to be carried out to determine whether the player's activity is in line with the expected activity. When this is not the case the Company is obliged to:

- Establish the source of funds;
- Revise the risk profile of the player and where necessary collect the source of wealth; and
- Decide whether transaction is an unusual transaction reportable to the FIU.

Section 8.10 Ongoing Monitoring

In carrying out ongoing monitoring the Company should ensure that documentation and information collected from the player is kept updated and relevant. In case of expired verification documents, fresh, valid documents are to be collected.

Section 8.11 Multiple Account Monitoring

The Company shall implement mechanisms to detect the opening of accounts by the same customer, but using third-party identities (e.g. same financial information, geo-location monitoring, etc.)

Section 9. Company Obligations

The Company aims to satisfy all responsibilities and requirements identified by the National Ordinance Reporting Unusual Transactions (NORUT) and the National Ordinance Identification when Rendering Services (NOIS).

- Customer due diligence (CDD);
- Internal record keeping;
- Reporting (both internal and external); and
- Employee instruction and training.

The Company has suitable controls in place that allow the identification of customers via a 'know your client's (KYC) procedure as indicated above. Further CDD will be performed based on the following defined thresholds of activity by the fraud department:

- Players engage in financial transactions either in one transaction or a series of two or more related transactions >= NAF 4,000 (approx. EUR 2,046).
- There is a suspicion of ML/FT or the operator has doubts about the veracity of customer identification data.

The company reserves the right to enhance its CDD exercise in cases where risk of ML/FT is higher, including cases of PEPs, high-risk jurisdictions.

The CDD measures to be undertaken are as follows:

- Collect additional information on the player;
- Conduct more frequent reviews of the player's identification data;
- Obtain details regarding the player's Source of Funds (SoF) and Source of Wealth (SoW);
- Acquire information on the player's expected level of activity;
- Secure senior management approval to initiate or continue the business relationship; and
- Increase monitoring of transactions by enhancing the frequency and timing of controls, and perform more detailed analysis of transactions; and

Require payments to be processed through an account held in the player's name at a reputable bank. During this process players may be allowed to use their gaming account, however, deposit or withdrawal functionalities must be restricted. If documentation is not received within 30 days from when the threshold is reached, the Company must terminate the business relationship and report the transaction to the FIU.

In addition, the company shall maintain the above documentation and information according to the retention periods below:

- All necessary records of transactions (both domestic and international) to enable compliance with any information requests from the competent authorities for at least five years;
- Any CDD documentation obtained should be kept for at least five years after the business relationship is ended, or after the date of the occasional transaction.

The Company also have suitable internal controls in place that prevent money laundering such as having a tight card policy, examples of this include only allowing one card on an account at a time and always processing withdrawals by default back in the same direction as deposits (closed loop). Appropriate transaction records are kept within the Company game servers or on the accounting and auditing tool.

Enhanced Due Diligence (EDD) is applied to higher-risk customers, such as PEPs or individuals from high-risk jurisdictions. EDD measures may include obtaining additional information on the customer's source of funds and the purpose of transactions. All CDD and EDD measures are documented, proportionate to the assessed risks, and reviewed periodically.

Section 9.1 Simplified Due Diligence

The company acknowledges that simplified CDD measures may be permitted when the risk of money laundering (ML) or terrorist financing (FT) is lower. These measures could include:

- Verifying the customer's identity after establishing the business relationship;
- Reducing the frequency of updates to customer identification;
- Decreasing the level of ongoing and transaction monitoring; and
- Inferring the purpose and intended nature of the relationship from the types of transactions conducted.

Section 9.2 AML Compliance Program

The key elements that the company must ensure are addressed in its AML Compliance Program include:

- **Internal Policies, Procedures, and Controls:** The company shall establish, maintain, and regularly update a comprehensive framework of internal AML/CFT policies, procedures, and controls, approved by senior management or the Board of Directors. These controls shall be effectively communicated to all relevant staff and integrated into daily operations to ensure compliance with applicable AML/CFT legal and regulatory obligations in Curaçao.
- **Designation of a Compliance Officer (MLRO):** A suitably qualified Compliance Officer, who may also serve as the Money Laundering Reporting Officer (MLRO), shall be appointed and vested with sufficient authority, independence, and access to resources. This officer shall be responsible for the implementation, management, and continuous improvement of the AML/CFT compliance framework, including the filing of Unusual Transaction Reports (UTRs) with the FIU Curaçao, oversight of internal controls, training initiatives, and regular reporting to the Board or Senior Management.
- **Employee Screening and Training:** The company must conduct pre-employment screening of all prospective employees, including criminal background checks, to assess their suitability for roles with AML-related responsibilities. An ongoing AML training program must be developed and implemented to ensure that all employees, particularly those in sensitive or risk-related functions, receive adequate, role-specific training. This includes periodic refresher courses to maintain awareness of evolving AML risks, reporting obligations, and regulatory updates.
- **Independent Testing and Internal Audit Function:** The AML/CFT program shall be subject to regular, independent audit or compliance testing, either internally or by external experts, to assess its effectiveness and adherence to LOK and other applicable requirements. Such audits must be conducted at least annually. A report on the findings, including any deficiencies and corresponding corrective action plans, shall be submitted to the Board of Directors or governing body, with documented follow-up on remediation.

Section 9.3 Record Keeping

The Company will retain the following documentation and information according to the specified retention periods:

- All necessary transaction records (both domestic and international) for at least five years to ensure compliance with any information requests from competent authorities.
- All Customer Due Diligence (CDD) documentation for a minimum of five years after the business relationship has ended or after the date of the occasional transaction.

Adequate record keeping will allow for the reconstruction of individual transactions, along with supporting evidence if needed, to facilitate the prosecution of criminal activity.

Section 10. Course of Action in Case of Suspicion of Fraud

It is a duty as an operational member of staff to be alert for the signs of money laundering as detailed in this document, through further training and via usage of reasonable levels of skepticism and common sense.

Confidential money laundering issues should be reported to the Compliance Officer or MLRO using a Suspicious Transaction Report (STR), accompanied by all relevant supporting documentation. The Compliance Officer or MLRO is responsible for the investigation cases of suspected money laundering and if deemed necessary escalation of them to the Financial Intelligence Unit (FIU).

Employees should email Suspicious Transaction Report directly to the Compliance Officer or the MLRO who will then handle the document appropriately in the event of any of the scenarios listed below, as defined by the Ministerial Decree of 1st December 2015, as mentioned in Article 10 of the NORUT which are deemed unusual:

- Transactions reported to the Police or to the Department of Justice in connection with ML/FT;
- Transactions by or on behalf of a natural or legal person, named on the Sanctions National Ordinance list;
- Transactions equal to or exceeding the amount of NAF 5,000, whether as a bank transaction, the sale of chips or credits or the payment of prizes. (A transaction
- Transactions where there is cause to presume that they can be related to ML/FT.

IMPORTANT NOTE

A customer should never be informed that a suspicious activity report has been raised against them or imply in any way to a customer that their account may be under investigation. Doing this would constitute ‘tipping off’ the customer. Tipping off a customer can unnecessarily alarm them if they are not committing an offence but most importantly, if they are involved in criminal activity, it could aid them by indicating they are being investigated. It would ‘tip off’ a criminal to quickly destroy incriminating evidence against them and change their mode of operation. This would jeopardize any investigation into them. In some countries ‘tipping off’ if proven can constitute a criminal offence and can in the absence of further evidence inadvertently implicate you in the operation of the crime. Do not inform or unnecessary staff either, as this may inadvertently lead to tipping off via a 3rd party route. Do not do anything to a client’s account that could tip them off which includes closing it, the AML team can handle this if needed.

An employee who has failed to act or acted negligently in the light of proven ‘reasonable grounds to suspect’ money laundering is also liable to prosecution.

Report suspicious activities and transactions, using an STR to the Compliance Officer.

Do not inform a customer that a STR has been raised involving them. Do not inform unnecessary personnel about your report or suspicions.

Fraud/Money Laundering involving Internal Staff

Although it is very rare and certainly not part of the Company agenda, money laundering and/or fraud unfortunately can also occur internally within a business.

Extreme candor should be exercised in handling any of the scenarios below, ideally one would have at least some basic evidence or indications of where evidence would lie to back up any reported suspicions. Poorly handled or judged situations of this nature can result in significant unnecessary harm either to any of the individuals involved and/or the business.

1. Pressure or instructions by privileged members of staff to perform transactions or make changes that would deliberately ignore or avoid due diligence, should be reported to the Compliance Officer. It is advised that the person is not confronted by member(s) of staff, nor should anyone else be enquired about the activity by any member of staff. The investigation should be carried out by the appointed and responsible parties. Unnecessary people should not be informed about the report/suspicion.
2. If any employee sees a colleague, no matter how senior, engages in suspicious activity such as performing unauthorized transactions, frequently working late/alone without apparent reason, taking sensitive documents from the office or being untruthful about their activity report it to the Compliance Officer. It is advised that the person is not confronted by member(s) of staff, nor should anyone else be enquired about the activity by any member of staff. The investigation should be carried out by the appointed and responsible parties. Unnecessary people should not be informed about the report/suspicion.

ANNEX 1

1. LIST OF DEFINITIONS

1.1 In this AML Policy, the following terms have the following meanings:

AML means anti-money laundering.

AML Policy means the Anti-Money Laundering Policy of the Company

Board of Directors means the board of directors of the Company

Company means the Company, its direct and indirect parent companies, its direct wholly- and majority-owned subsidiaries.

Compliance Program means the compliance program of the Company as adapted by the Supervisory Board.

Employee means any director, officer, full-time, part-time and second employee including any third-party contractor, who receives or is entitled to receive remuneration for goods or services from the Company

General Counsel means the general counsel of the Company

ML means Money Laundering.

MLRO – Money Laundering Reporting Officer

Money Laundering means Money Laundering as defined in this AML Policy in Clause 4.

Personnel mean the directors, officers, full-time, part-time and seconded employees of the Company, and anyone working on the Company's behalf, e.g. consultants and representatives.

Supervisory Board means the supervisory board of the Company

Terrorist Financing means Terrorist Financing as defined in this AML Policy in Clause 4.

TF means Terrorist Financing.

1.2 Save where the context dictates otherwise, in this AML Policy:

- a) unless a different intention clearly appears, a reference to a Clause or Annex is a reference to a clause or annex of this AML Policy;
- b) words and expressions expressed in the singular form also include the plural form, and vice versa;
- c) words and expressions expressed in the masculine form also include the feminine form; and
- d) a reference to a statutory provision counts as a reference to this statutory provision including all amendments, additions and replacing legislation that may apply from time to time.

1.3 Headings of clauses and other headings in this AML Policy are inserted for ease of reference and do not form part of this AML Policy for the purpose of interpretation.

ANNEX 2

1. FACTORS OF HIGHER RISK SITUATIONS

1.1 Counterparty risk factors

- a) the business relationship is conducted in unusual circumstances;
- b) counterparties that are resident in geographical areas of higher risk;
- c) legal people or arrangements that are personal asset-holding vehicles;
- d) companies that have nominee shareholders or share in bearer form;
- e) businesses that are cash-intensive; and
- f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

1.2 Product, service, transaction or delivery channel risk factors

- a) products or transactions that might favor anonymity;
- b) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
- c) payment received from unknown or unassociated third parties; and
- d) new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products;

1.3 Geographical risk factors

- a) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective anti-money laundering and counter terrorist financing systems;
- b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
- c) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations; and
- d) countries providing funding or support for terrorist activities, or that have designated terrorist organizations operating within their country.

ANNEX 3

1. FACTORS OF LOWER RISK SITUATIONS

1.1. Counterparty risk factors

- a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership.
- b) public administrations or enterprises from countries or territories having a low level of corruption; and
- c) counterparties that are resident in geographical areas of lower risk.

1.2 Product, service, transaction or delivery channel risk factors

- a) products, service, transactions or delivery channel where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (particularly, certain types of electronic money).

1.3 Geographical risk factors

- a) the counterparty is in one of the Member States of the European Union;
- b) the counterparty is in a third country having effective anti-money laundering and counter terrorist financing systems;
- c) the counterparty is located in third countries identified by credible sources as having a low level of corruption or other criminal activity; and
- d) the counterparty is located in third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent.