



FRAUD, AML & CFT POLICIES

Of
Zerone B.V.

Content

1. Introduction	2
2. Important Definitions	2
3. Objective of this Police	3
4. Financing Terrorism	3
5. Politically Exposed Person (PEP)	3
6. Forbidden Countries	5
7. Operational Principles	6
8. Red Flags for Money Laundering and Terrorist Financing	7
9. Obligations	9
10. Procedures	10
11. Final Provisions	25

1. Introduction

Zerone B.V. is licensed and regulated by the Government of Curaçao, to offer remote (online) games over the internet, under the Remote Gaming Regulations.

Under the license conditions issued by Curacao Authorities, Zerone B.V. is required to have in place adequate measures to prevent its systems from being used for the purposes of money laundering, terrorist financing or any other criminal activity.

Zerone B.V. is committed to conducting its business with the highest ethical and legal standards and expects all employees and other individuals acting on its behalf to uphold this commitment. As such, the Zerone B.V. has adopted this Anti-Money Laundering Policy ("Policy"), which is applicable to all directors, officers, employees, agents, representatives, consultants, advisors, distributors, supplier contractors, or other third parties acting on behalf of Zerone B.V., even on a provisional and temporary basis ("Zerone B.V. Personnel").

Zerone B.V. will not conduct business with individuals or corporations whose conduct may give risk to suspicions of involvement with illegal activities. Zerone B.V. will report any suspicions of money laundering or terrorist financing activity to the relevant authorities.

This Policy and the internal controls herein have been designed to avoid money laundering, including the laundering of illicit proceeds by the same person (self-laundering), and the use of money, goods, or gains of illicit provenance and, consequently, prevent potential criminal liability of the Zerone B.V. that could result from such violations/crimes.

Zerone B.V. Personnel who violate this Policy may be subject to disciplinary action, including dismissal from the Zerone B.V., termination of agreements, and or any other associated legal and out-of-court actions, in accordance with the applicable law. The consequences for violating anti-money laundering laws can be severe for the Zerone B.V., including significant fines, loss of operating licenses, limitations on engaging in certain business activities, imprisonment and reputational damage.

The Zerone B.V. Personnel must comply with the anti-money laundering laws of all countries where the Zerone B.V. carries out its activities.

2. Important Definitions

Money laundering is defined as engaging in acts to conceal or disguise the origins of illegally or criminally derived proceeds and assets so that they appear to have legitimate origins and are introduced into the legal financial and business as if they were lawful. If any Zerone B.V. Employee or Zerone B.V. Personnel suspects that there has been money laundering, that person must immediately report the suspected violation to Zerone B.V.'s Compliance Team.

For the purposes of this policy, the following conducts shall be regarded as money laundering:

- The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, 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 an activity to evade the legal consequences of that person's action.

- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such activity.
- The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity.
- Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of the above-mentioned actions.

Examples of illicit provenance are forgery of money, extortion, robbery, and drug crime, as well as fraud, corruption, organized crime, or terrorism, etc.

The money laundering process consists of three "stages":

- 1) **Placement:** This involves the introduction of illegally obtained monies or other valuables into financial or non-financial institutions.
- 2) **Layering:** Layering occurs by conducting multiple, complex financial transactions that make it difficult to link the money to an illegal activity. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.
- 3) **Integration:** Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds.

3. Objective of this Policy

Zerone B.V. is fully committed to be constantly vigilant to prevent money laundering and combat the financing of terrorism to minimize and manage risks such as the risks to its reputational risk, legal risk and regulatory risk. It is also committed to its social duty to prevent serious crime and not to allow its systems to be abused in furtherance of these crimes.

Zerone B.V. will endeavor to keep itself updated with developments both at national and international level on any initiatives to prevent money laundering and the financing of terrorism. It commits itself to protect, at all times, the organization and its operations and safeguards its reputation and all from the threat of money laundering, the funding of terrorist and other criminal activities.

4. Financing Terrorism

Zerone B.V. Personnel must immediately report any suspected or known terrorist financing to Zerone B.V.'s Compliance Team. For the purposes of this Policy, "terrorist financing" means the provision or collection of funds, by any means, directly or indirectly, with the intention to be used or in the knowledge that they are to be used, in full or in part, in order to use indiscriminate violence as a means to create terror, fear, or to achieve a political, religious, or ideological aim.

5. Politically Exposed Person (PEP)

European guidelines regarding "The Prevention of Laundering the Proceeds from Criminal Activity (Money Laundering) and Terrorism Financing" entered into effect, changing the definition of politically exposed person. To minimize corruption and money laundering risks, BetNacional is obliged by law to collect data and identify which of the clients / clients' beneficiaries should be considered as politically exposed persons, their family members or close associates.

Transactions involving Politically Exposed Persons ("PEPs") require enhanced due diligence. A PEP is an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering offenses and related predicate offenses, including corruption and bribery, as well as conducting activity related to terrorist financing.

The potential risks associated with PEPs justify the application of additional anti-money laundering/counter-terrorist financing preventive measures.

For the purposes of this Policy, Politically Exposed Persons ("PEP") includes, but are not limited to:

- Heads of State, heads of government, ministers and deputy or assistant ministers.
- Members of parliament or of similar legislative bodies.
- Members of the governing bodies of political parties.
- Members of supreme courts, of courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances.
- Members of courts of auditors or of the boards of central banks.
- Mayors and members of local administration, city and district assemblies.
- Ambassadors, chargés d'affaires and high-ranking officers in the armed forces.
- Members of the administrative, management or supervisory bodies of State-owned enterprises.
- Directors, deputy directors and members of the board or equivalent function of an international organization.

Not only the person that officiates a public function must be considered as PEP, also close family members must be included in the assessment. For the purpose of this Policy, family members mean:

- The spouse, or a person considered to be equivalent to a spouse, of a politically exposed person.
- The children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person.
- The parents of a politically exposed person.

Also, persons known to be close associates to a PEP must be assessed with the same risk approach that includes:

- Natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a Politically Exposed Person.
- Natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a Politically Exposed Person.
- President, State Governors, mayors, and any kind of ancillary such as ministers, counselors and secretaries.
- Officers or employees of national, federal, regional, local, or other, government bodies, departments, or agencies.
- Officer or employees of state-owned or state-controlled entities, national or international.
- Heads of state or anyone who exercises governmental authority.
- Politicians, political party officials and candidates for political office.
- Employees of regulatory agencies, public entities and mixed capital societies.
- Officers and employees of public international organizations, as the United Nations, the World Bank and the International Monetary Fund.

6. Forbidden Countries

Currently the license of Curaçao is unique and allows operation with any type of gambling, both from website operators and technology and gaming providers internationally, except in Aruba, Bonaire, Curacao, France, Netherlands, Australia, United Kingdom, Spain, Saba, Statia, St Martin, USA, or any other jurisdiction that the Central Government of Curaçao (Netherlands Antilles) considers online gambling illegal or is blacklisted.

7. Operational Principles

The careful examination of those operations where risk factors exist is important. For example, this could mean those in which third parties propose the use of cash or bearers' checks, international transactions (in particular those with persons or entities residents in tax havens or high-risk territories, or different locations from those where the Zerone B.V. operates), operations with persons holding positions of public responsibility or PEPs or transactions conducted through or related to intermediary companies.

The Zerone B.V. Personnel should not initiate, maintain or accept a new business relationship (customer, supplier, financier, etc.), provide services or take action with anyone know or suspect to be involved in money laundering or terrorist financing, even if in different businesses from the relationship being established with Zerone B.V..

Likewise, the Zerone B.V. Personnel should not deal with money, goods or valuables that know or suspect to be of illicit origin or that are unaware of.

Zerone B.V. is committed to fight against money laundering and the financing of terrorism. Therefore, the following due diligence principles should be followed, not only in situations where particular risk factors exist, but as to all customers and third parties:

a. Identifying the Third Party

Zerone B.V. Personnel must conduct due diligence on customers and other third parties and document the findings. As part of the due diligence process, the following information (as applicable) should be collected: name, date of birth, address, National Identification Document, passport number, Foreigner's Identity Number or residence card if it is a physical person or Zerone B.V. name, registered office, corporate purpose, Employer Identification Number, Tax Identity Code (CIF), and/or incorporation details.

As part of due diligence, the Zerone B.V. must verify that the customer or third party does not appear on any of the US Department of the Treasury Office of Foreign Assets Control's sanctions list, including the Specially Designated Nationals and Blocked Persons lists.

b. Identifying the Ultimate Beneficial Owner (UBO)

Before the commencement of a commercial relationship, whether of a habitual nature, and prior to its execution, the Ultimate Beneficial Owner of any Third Parties who are formally involved must be identified. Zerone B.V. Personnel must document this analysis. Ultimate Beneficial Owner (UBO) means the person who directly or indirectly controls 25% or more of the equity or voting rights in the corresponding Zerone B.V. or owns the Zerone B.V.. In the event of the existence of a beneficial owner in the third party, that person must be identified through their name, nationality, National Identity Number, passport, Foreigner's Identity Number (RNE) or residence card. Listed companies are excluded from the obligation to identify the UBO.

If the UBO is a PEP, then the Zerone B.V. must conduct enhanced due diligence before entering into any contractual or commercial relationship with the entity.

c. Obligation to formally record commercial relationships in writing

Before the commencement of commercial relationships and prior to carrying out transactions with third parties (attention being paid to those of an international nature) the relationship must be formally recorded in a written agreement in accordance with Zerone B.V.'s standards. The provisions in a written agreement should include a commitment to comply with the Anti-Money Laundering laws, and Zerone B.V.'s right to immediately terminate the contract in case of violation, subject to applicable law.

8. Red Flags for Money Laundering and Terrorist Financing

Red Flags for Money Laundering and Terrorist Financing include:

- Unexplained spikes in account activity.
- Large number of transactions, which could indicate layering.
- The third party tries to conceal its identity or the source of its funds.

- The third party is an entity without a clear registered office and does not appear online.
- The third party's structure makes it difficult to recognize it.
- The third party funds for the transaction come from abroad when there is no apparent link between this country where the funds are sourced and the third party.
- The third party uses multiple bank accounts or ones held abroad without any justification.
- The third party intends to make payments in cash or using bearer checks.
- The third party intends to pay a higher price for the services for no good reason.
- The third party is based in a tax haven or a high-risk country.

9. Obligations

Appoint one of its senior officers as the designated Money Laundering Reporting Officer (MLRO) whose responsibilities will include the duties required by the laws, regulations and guidance notes.

All instances of suspected Money Laundering attempts must be reported to the MLRO, but that suspicion must not be conveyed to the customer and further actions must await consents. The MLRO is then responsible for liaising with, submitting Suspicious Activity Reports and seeking consents from the responsible legal authority in the jurisdiction where the transaction was done, when appropriate. He will also ensure that appropriate registers are kept for all related reporting. Take reasonable steps to establish the identity of any person for whom it is proposed to provide its service. For that Zerone B.V. will implement a FULL 'Know Your Customer' policy. Customers will be advised at registration and generally on the supporting non-transactional website that Zerone B.V. will utilize online verification tools and that in instances where we are not able to satisfy criteria, ID and address verification documents will be requested.

Always keep a secure online list of all registered Players.

Retain identification and transactional documentation as defined in the laws, regulations and guidance notes.

Systems will be operating to record all transactions for an account. These account histories will be subject to a program of regular and continual checks against fraud and social responsibility indicators. Where unusual bet patterns and winning patterns are detected, these will also be cross-referenced to call history to ensure that staff are not colluding with customers or acting illicitly.

Zerone B.V. will also keep a register of those customers that it identifies as high risk or politically exposed. Those accounts will be subject to greater scrutiny and frequency of checks.

In general, where illegal or inappropriate behavior by staff is identified, investigatory and disciplinary procedures will follow those outlined in staff contracts as required by employment law directives and the need to use in greater propensity, measures such as suspension when for example transactional fraud is suspected and those activities form a standard part of an employee's job description.

All transactions carried out on our site may be controlled to avoid money laundering or terrorist financing activities. Suspicious transactions will be reported to the relevant authority, depending on the jurisdiction governing the transaction.

If our risk and fraud department suspects fraud, it may require the player to provide appropriate documentation. If there is enough evidence of fraudulent behavior (eg bank repudiation, account operated by third parties, use of forged documents, fraud of means of payment, etc.), the account will be suspended until the situation is cleared. The suspension shall be communicated to the relevant authority together with the respective grounds (evidence or evidence collected) within 24 hours and to the authorities responsible for criminal proceedings. Parallel to the suspension, Zerone B.V. may proceed to the immobilization, as a precautionary measure, of the balance of the player account, until the decision of the competent authorities.

Provide initial and ongoing training to all relevant staff, including, but not limited to: procedures in respect of identifying players; monitoring player activity; record- keeping; reporting any unusual/suspicious transactions; unusual betting patterns; suspicious deposit and withdrawal patterns (size and frequency); reliability of Card Data; customer verification issues and identity theft; account linkage/multiple accounting; high risk jurisdictions;

Ensure that this policy is developed and maintained in line with evolving statutory and regulatory obligation and advice from the relevant authorities.

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.

Zerone B.V. may terminate Accounts with immediate effect and retain all account funds in the event of a credible suspicion of fraudulent activity including, but not limited to, the supply of fraudulent, forged, altered, or stolen personal data and, still, in the case of multiple account registration.

Report any suspicion or knowledge of money laundering or terrorist financing to the Financial Intelligence Analysis Unit (FIAU) set up by law as the 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.

An employee must not, under any circumstances, disclose or discuss any AML concern with the person or persons subject to an investigation, or any other person for that matter. Disclosure (also known as "tipping off") is strictly prohibited and carries with it very serious legal penalties.

Furthermore, and in order to keep ourselves protected as much as possible, no remark should ever be left on an account that would give any indication that ML is suspected, a player being entitled, at any point in time, to request the full notes/remarks on their account.

Cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity.

Moreover, Zerone B.V. shall:

1. Not accept to open anonymous Accounts or Accounts in fictitious names such that the true beneficial owner is not known.
2. Not accept cash from Players.
3. Funds may be received from Players only by any of the following methods: credit cards, debit cards, electronic transfer, wire transfer, cheques and any other method approved by the Regulator.
4. Not register a Player who is under eighteen (18) years of age.
5. Only register a single account in the name of a particular person: multi-account practices are strictly prohibited.

6. Transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.

7. Not accept a wager unless a User Account has been established in the name of the Player and there are adequate funds in the Account to cover the amount of the wager.

8. Not accept a wager unless the funds necessary to cover the amount of the wager are provided in an approved way.

9. Not accept Players residing or playing from non-reputable jurisdictions.

10. Not make a payment in excess of two thousand three hundred EUR (€ 2,300) or cumulative out of a User Account to a Player until the Player's identity, age, and place of residence have been verified.

11. If no transaction has been recorded on a User Account for thirty months, close the User Account and remit the balance in that account to the Player, or if the Player cannot be satisfactorily located, to the regulator.

12. Where it deems necessary, verify creditworthiness of the Player with third parties who previously provided any information on the Player.

13. If it becomes aware that a person has provided false information when providing due diligence documents, not register such person. Where that person has already been registered, Zerone B.V. shall immediately cancel that person's registration as a Player with the Zerone B.V..

Zerone B.V. applies internal regulations and special programs of measures to help national and international organizations combat money laundering and the financing of terrorism around the world.

By registering an account on our website, the User assumes the following obligations:

- You grantee that you will comply with all applicable anti-money laundering and terrorist financing laws and regulations, including but not limited to the AML Policy;
- You confirm that you have no knowledge or suspicion that the funds used to fund your account were obtained from an illegal source or are in any way related to money laundering or other illegal activities prohibited by applicable law or the instructions of any international organization;
- You also agree to promptly provide us with any information we deem necessary for us to comply with applicable anti-money laundering laws and regulations.

The users cannot use loans to participate in Zerone B.V. website. Zerone B.V. will not grant the user any kind of loan or mechanism that allows them to take out loans or transfer funds between players, at any time. Zerone B.V. reserves the right to supervise any transfer of funds that are deposited or withdrawn by any user and to report any user information to the regulatory or criminal authorities and/or payment service providers.

We monitor any suspicious activity on the User's account, as well as operations carried out under special conditions.

We have the right to ban the user at any time, if we have reason to believe that any transaction has anything to do with money laundering and criminal activities. In accordance with international law, we are not obliged to inform you about your suspicious activity and to inform you that such activity has been transmitted to the competent authorities.

In accordance with internal AML procedures, we carry out initial and ongoing procedures to verify personal identity according to the risk level of each user, such as:

- We ask the User to provide the minimum information to confirm the identity;

- We record and preserve all data and documents, as well as the confirmation methods used and the results of verification procedures.
- We check Users' personal data to check against the list of suspected terrorists, which is formed by the authorized state and independent authorities. A minimal set of identifying data includes: the User's full name; date of birth (for individuals); User's residential address or registered address;
- We request that the User provides information regarding the sources of funds that he/she plans to deposit into the account.

To verify and confirm the authenticity of the data, we may require the following documents:

- Passport or identification card, or other equivalent document that meets the following requirements: containing the name, date of birth and a photograph of the holder of the document;
- Issued by national public authorities, a recently obtained receipt for payment of utility bills (dated no later than 3 months) or other documents confirming the User's address.

We may also require additional information to confirm the corresponding documents. In certain cases, we may also require certified copies of User's documents.

Proof of ID

- a.** Signature Is preferable
- b.** Country is not a Restricted Country: United States of America and its territories, France and its territories, Netherlands and its territories and countries that form the Kingdom of Netherlands including Bonaire, Sint Eustatius, Saba, Aruba, Curacao and Sint Maarten, United Kingdom of Great Britain and Northern Ireland, Sweden, North Korea, Singapore, Kazakhstan, Iran, Afghanistan, Cyprus, and Macedonia.
- c.** Full Name matches client's name
- d.** Document does not expire in the next 3 months
- e.** Owner is over 18 years of age

Proof of Residence

- a.** Bank Statement or Utility Bill
- b.** Country is not a Restricted Country: United States of America and its territories, France and its territories, Netherlands and its territories and countries that form the Kingdom of Netherlands including Bonaire, Sint Eustatius, Saba, Aruba, Curacao and Sint Maarten, United Kingdom of Great Britain and Northern Ireland, Sweden, North Korea, Singapore, Kazakhstan, Iran, Afghanistan, Cyprus, and Macedonia.
- c.** Full Name matches client's name and is same as in proof of ID
- d.** Date of Issue: In the last 3 months

Selfie with ID

- a. Holder is the same as in the ID document above
- b. The ID document is the same as in "1". Make sure photo/ID number is the same

Notes on "KYC Process"

When the KYC process is unsuccessful then the reason is documented and a support ticket is created in the system. The ticket number along with an explanation is communicated back to the user.

Once all proper documents are in our possession then the account gets approved.

"Other AML Measures"

If a user has not passed full KYC then they cannot make additional deposits or withdrawals of any amount.

In cases when the Zerone B.V. receives proof of identity and address proof documents from Customers and information/details in the provided identity and address proof documents are different than details in provided filled online application form in the sign-up process – Customer account opened with the Zerone B.V. is closed and business relationship with the Customer is terminated. Also, in cases when the Zerone B.V. receives filled online application and personal proof of identity documents of the Customer and determines that the Customer is underaged (under age that gambling or gaming activities are legal under the law or jurisdiction that applies to Customer) and/or is prohibited to participate in gambling activities (listed on register of persons restricted from participation in gambling) the Zerone B.V. immediately notice Customer regarding decision not to establish business relationship. Respective record is made in the register of terminated business relationships.

Zerone B.V. requests to be provided with suitable documents once again and until provided cannot verify the Customer's identity in cases as follows:

- a. The Customer did not provide any of required documents confirming his identity;
- b. The Customer did not provide all required documents or provided documentation was incorrect/unrelated with the data indicated in online application;
- c. The documents were not provided in conformity to points 3.4. and 3.6. of this Policy.
- d. All data and documents of the Customer collected during the stage of the Customer's identification indicated in section 3 of this Policy shall be recorded and stored in accordance to this Policy.

If a user has passed the KYC process successfully then.

Complementary and automatic processes carried out by Zerone B.V.

Zerone B.V. will use, in addition to the identity proof process carried out by the user, external sources and automatic processes to consult and validate the data presented by the player.

In cases when results of risk-based evaluation indicates that no more than one the risk factor applies to the Customer – meaning Customer was classified as Medium Risk Customer – Zerone B.V. shall perform **Enhanced Due Diligence (EDD)** of the Customer.

Zerone B.V. is entitled to adopt decision not to perform **Enhanced Due Diligence (EDD)** of the Customer as indicated in point 2.5. of this Policy. In cases when at least two of the factors listed.

Respective record shall be made in the register of terminated business relationship.

By performing Enhanced Due Diligence (EDD) of the Customer, Zerone B.V. implements measures to eliminate risk of money laundering and/or terrorist financing as follows:

- obtaining additional information/explanation and/or documents from the Customer;
- obtaining the approval of senior manager of the Zerone B.V. for establishing the business relationship;
- obtaining information and/or documents on the source of funds and source of wealth of the customer;
- any other data/information that employees of the Zerone B.V. considers relevant to eliminate or mitigate the risk.
- If the Customer avoids to provide above mentioned explanations/information and/or documents or provided explanations/information and/or documents do not allow to mitigate the risk of money laundering and/or terrorist financing, the Zerone B.V. notice Customer regarding decision not to establish business relationship.
- In cases when Customer provides requested information/explanation and/or documents and provided information/explanation and/or documents allows to eliminate or mitigate the risk of money laundering and/or terrorist financing, the Zerone B.V. decides whether to establish or not business relationship with the Customer.
- Zerone B.V. decisions to or not to establish business relationship after performance of **Enhanced Due Diligence (EDD)** shall be expressed by making a record in the Zerone B.V.'s register of establishment of a business relationship with Customers or register of terminated business relationship. Following the decision to establish a relationship with the Customer, Zerone B.V. while providing services continues to perform ongoing due diligence of the Customer, periodic reviews of the relevance of the data and notices the Supervisory authority about unusual/suspicious activity.
- All data of the Customer collected during stage of **Enhanced Due Diligence (EDD)** of the Customer indicated in section 5 of this Policy shall be recorded and stored in accordance to point 9.3. of this Policy.

Ongoing Due Diligence

- While providing services, Zerone B.V. shall continue to perform ongoing monitoring of the Customer, periodic reviews of the relevance of the data and informs the Supervisory authority about possible suspicious activity.
- Zerone B.V. must ensure continuous monitoring of Customers transactions and behavior to identify unusual operations or activities. Unusual indications may be related to the deposits made into Customer's account opened with Zerone B.V., abuse of bonuses or other promotions, using unfair external factors or influences, taking unfair advantage, opening any duplicate accounts with Zerone B.V., undertaking fraudulent practice or criminal activity, etc.
- Zerone B.V. shall ensure that the data, documents and information about the Customer are constantly updated (at least once every 24 months). In cases **Enhanced Due Diligence (EDD)** applied to the Customer during onboarding stage, data, documents and information shall be updated at least once every 12 months.

- If the Customer avoids to submit updated documents, information and other data required by Zerone B.V. within the reasonable time, the Zerone B.V. might terminate business relationship with the Customer. Even if the Customer provides requested information, decision to terminate or continue business relationships with the Customer is at the discretion of Zerone B.V. and shall be made in accordance with any potential risk factors indicated in this Policy. Respective decision of Zerone B.V. shall be expressed by making a record in the Zerone B.V.'s register of termination of a business relationship with Customers or register of continued business relationship with Customers.
- All data of the Customer collected during stage of Ongoing Due Diligence of the Customer indicated in section 6 of this Policy shall be recorded and stored in accordance to point 9.3. of this Policy.

Recognition, documentation and reporting of unusual/suspicious transactions

- An unusual transaction shall be considered a transaction which is inconsistent with the Customer's business behavior or personal activities.
- Zerone B.V. shall pay special attention to all complex, unusually large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purposes.
- To guard against money laundering and/or terrorist financing the Zerone B.V. shall record any suspicious/unusual transaction in writing by making a record in the Zerone B.V.'s register of unusual/suspicious transactions of the Customer. Such findings shall be kept of at least five years and shall be available for respective Curacao supervisory authorities.
- In case unusual/suspicious transaction was detected and recorded, the senior manager shall be internally reported regarding this matter within undue delay, in the manner approved by the Zerone B.V..
- Together with internal unusual/suspicious report senior manager shall be provided with all collected data related with the Customer being reported.
- In cases when senior manager had evaluated nature, risks and other relevant circumstances of the transaction and authorized received report, external report shall be prepared and submitted to Supervisory authority without undue delay.
- If the unusual transaction is not authorized by senior manager to be incorporated and reported to Supervisory authority, all documents relevant to the transaction including reasons for nonauthorization shall be documented, undersigned by senior manager and kept for internal records in accordance to this Policy.
- The Zerone B.V. shall appoint a Money Laundering Reporting Officer (the "MLRO") who as the Non-Executive Director shall be responsible for the filing of a Quarterly preformatted Report, pertaining a risk analysis on Money Laundering (the "MLR") with the designated authorities.
- The Executive Director shall be responsible for the drafting of the MLR and shall timely present a properly filled out MLR to the MLRO for approval and filing with the authorities in accordance to point.
- Both the Executive Director and Non-Executive Director are required to sign the MLR prior to its filing.
- Notwithstanding anything to the contrary as referenced in point.
- The MLRO shall also be responsible for ensuring that, when appropriate, the information of any other matter leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of Money Laundering is properly disclosed to relevant the authority.

- The Report in accordance shall at minimum include the following information:
 - (i) a general description of the policies on AML that have been implemented, including any updates or material changes; (ii) any suspicions on Money Laundering; (iii) any Incidents.
 - Whenever events transpire in accordance to the point.
 - (ii) and (iii) the MLR.

Registration of Customer's Account

The Zerone B.V. shall have the right to appoint or engage either third parties or its affiliate(s) as a payment processor or payment solution provider to act, receive and/or pay funds on behalf of the Zerone B.V..

- The Zerone B.V. shall have the right to appoint or engage either third parties or its affiliate(s) as an operator to operate the Account.
- The Customer is only allowed to open one Account with the Zerone B.V.. In case the Customer attempts to open more than one Account, the Zerone B.V. shall have the right to block or close all accounts the Customer tries to open. In case the Customer notices having more than one Account under different names, the Customer must notify the Zerone B.V. immediately.
- Account is created when the Customer logs-in using through the Zerone B.V.'s website.
- Upon the opening of the Account the Customer must provide the following personal information:
 - full name and date of birth;
 - an address, telephone number and e-mail address ("**Contact Details**").
- The Contact Details may be updated from time to time by contacting Customer Services; or through the Account management page on the Zerone B.V.'s website.
- The Zerone B.V. reserves the right to refuse to open an Account in case of violation of the Zerone B.V.'s Terms and Conditions or policies, or terms and conditions or policies of third parties or affiliate(s) engaged by the Zerone B.V., or other laws, regulations and policies applicable to the Zerone B.V. or by request of the relevant third parties (including governmental bodies and regulators).
- To open the Account, the Customer must be 18 (eighteen) years of age or older, or such higher minimum legal age as stipulated in the laws of jurisdiction applicable to the Customer and, under the laws applicable to the Customer, the Customer is allowed to participate in the games offered on the Zerone B.V. website.
- In opening the Account, the Customer warrants that is aware that the right to access and use the Zerone B.V.'s website and any products there offered, games, Zerone B.V.'s services and the Account may be considered illegal in certain countries or jurisdictions. The Zerone B.V. is not able to verify the legality of service in each and every jurisdiction, consequently, the Customer is responsible in determining whether the Customer's accessing and using the Zerone B.V.'s website is compliant with the applicable laws in the Customer's country and the Customer warrants to the Zerone B.V. that gambling is not illegal in the territory where the Customer resides.
- For various legal or commercial reasons, the Zerone B.V. does not permit Accounts to be opened or used by resident of certain jurisdictions (the "**Restricted Jurisdictions**").
- If on completion of Zerone B.V.'s KYC and verification checks, the Customer is shown to be underage or be resident of any Restricted Jurisdiction (the "**Ineligible Person**"), or use

the Zerone B.V.'s website and any products there offered, games, Zerone B.V.'s services and an Account from a Restricted Jurisdiction:

(a) Zerone B.V. will block the Customer's Account;

(b) All transactions made whilst the Customer was Ineligible Person will be made void, and all related funds deposited by the Customer will be frozen and transferred back to the Customer's account or wallet address.

- The Zerone B.V. will consider and review carefully each case of opening an Account by an Ineligible Person and take the appropriate decision as regards to such Account and the deposited funds to such Account.
- The Zerone B.V. shall have the right to engage local consultants and governmental agencies residing in the jurisdiction where an Ineligible Person resides for the purpose of full compliance with laws and regulations applicable to such Ineligible Person. In the event that such engagement results in any expenses for The Zerone B.V. the latter shall have the right to debit an amount of such expenses from the Account opened (registered) by an Ineligible Person unless otherwise expressly established by the applicable laws and regulations.
- The Zerone B.V. shall have the right to eventually decide at its sole discretion either to (i) freeze the funds and such Account until an Ineligible Person becomes compliant with Terms and Conditions or (ii) close an Account and return an amount of deposited funds excluding fees and charges applicable to the respective return transaction(s), withdrawal fee and other expenses.
- The Customer is not allowed to transfer funds Account to other users or to receive funds from other users into Account, or to sell, transfer and/or acquire accounts to/from other users.
- The Zerone B.V. may refuse to open an Account or close an existing Account in case of violation of our Terms and Conditions or policies, or terms and conditions or policies of third parties or affiliate(s) engaged by The Zerone B.V., or other laws, regulations and policies applicable to The Zerone B.V. or by request of the relevant third parties (including governmental bodies and regulators). However, all contractual obligations already made will be honored.
- Account shall be deemed inactive if it has not been accessed for one hundred eighty (180) days and the positive balance shall be reset. If the Customer wishes to reinstate this balance, the Customer should contact Customer Support Service.
- All transactions will be checked by the Zerone B.V.'s Anti-Fraud department in accordance with the prevention of money laundering laws and regulations as applicable.
- Any suspicious activity on the Customer's Account could lead the Customer to being reported to the relevant authorities and freezing of the balance of the Account in full. It could also lead to the closure of the Account and forcible withdrawal or confiscation of the Customer funds.

- The Zerone B.V. will consider and review carefully each case of opening an Account by an Ineligible Person and take the appropriate decision as regards to such Account and the deposited funds to such Account.
- The Zerone B.V. shall have the right to engage local consultants and governmental agencies residing in the jurisdiction where an Ineligible Person resides for the purpose of full compliance with laws and regulations applicable to such Ineligible Person. In the event that such engagement results in any expenses for The Zerone B.V. the latter shall have the right to debit an amount of such expenses from the Account opened (registered) by an Ineligible Person unless otherwise expressly established by the applicable laws and regulations.
- The Zerone B.V. shall have the right to eventually decide at its sole discretion either to (i) freeze the funds and such Account until an Ineligible Person becomes compliant with Terms and Conditions or (ii) close an Account and return an amount of deposited funds excluding fees and charges applicable to the respective return transaction(s), withdrawal fee and other expenses.
- The Customer is not allowed to transfer funds Account to other users or to receive funds from other users into Account, or to sell, transfer and/or acquire accounts to/from other users.
- The Zerone B.V. may refuse to open an Account or close an existing Account in case of violation of our Terms and Conditions or policies, or terms and conditions or policies of third parties or affiliate(s) engaged by The Zerone B.V., or other laws, regulations and policies applicable to The Zerone B.V. or by request of the relevant third parties (including governmental bodies and regulators). However, all contractual obligations already made will be honored.
- Account shall be deemed inactive if it has not been accessed for one hundred eighty (180) days and the positive balance shall be reset. If the Customer wishes to reinstate this balance, the Customer should contact Customer Support Service.
- All transactions will be checked by the Zerone B.V.'s Anti-Fraud department in accordance with the prevention of money laundering laws and regulations as applicable.
- Any suspicious activity on the Customer's Account could lead the Customer to being reported to the relevant authorities and freezing of the balance of the Account in full. It could also lead to the closure of the Account and forcible withdrawal or confiscation of the Customer funds.

Deposits into Account

- Unless otherwise established by Terms and Conditions, the Customer may participate in a game only if the Customer has sufficient funds on the Account for such participation.
- All information required to deposit funds into the Customer's Account (including available currencies and payment methods), can be found under the Account. The Customer can use any of the payment methods available to the Customer as specified on the Zerone B.V.'s policies as may be amended from time to time.
- Deposits in the Account can be made in virtual currencies (USDT, CHP, BTC and ETH) or FIAT currencies (EUR or other fiat currency if available). The Customer may only deposit funds to the Account using virtual or fiat currencies, that are indicated in this point of this policy. Deposits made in BTC, ETH, EUR or other fiat currency if available will be automatically exchanged to USDT.

- The Customer himself cannot change the deposited virtual currency from one virtual currency (e.g. BTC) to another virtual currency (ETH) in the Account as the Zerone B.V.'s do not offer virtual currency exchange services.
- If the Customer makes a stake while the game session and lose it, the balance of the Customer's game session as well as the balance of the Account will decrease on the respective amount of funds in the Account. In the event of the winning, the balance of the Customer's game session and the balance of the Account will increase respectively.

Account balance is the amount of virtual currency/FIAT currency paid into Account and automatically exchanged to USDT, plus any winnings (including bonuses if any) and/or minus any losses accrued from using the Zerone B.V. Services, less any rakes or entry or other fees, if applicable, and less any amounts previously withdrawn, loss by the Customer or amounts forfeited or reclaimed by the Zerone B.V. due to any known or suspected fraud

- Only the Customer may deposit to the Account and no other person shall make transfers or payments to deposit funds to the Customer's Account. Should the Zerone B.V. find that the Account has been deposited by a third party (the "Prohibited Deposit"): (a.) the Zerone B.V. will immediately return the amount of the respective Prohibited Deposit by the same payment method used for transfer of the Prohibited Deposit, wherever practicable, excluding all applicable fees and charges to the Zerone B.V. for such return and no winnings will be paid; and (b.) all transactions made whilst the Customer was using any amount of the Prohibited Deposit will be made void.
- Should the Account be deposited by the Prohibited Deposit more than one time, the Zerone B.V. shall have the right to close the Account and return the balance of the Account to the Customer excluding all fees and charges applicable to the Zerone B.V. for such return.
- The Zerone B.V. reserves the right to use additional procedures and means to verify the Customer's identity when effecting deposits into the Account.
- The Zerone B.V. is not a financial institution and thus should not be treated as such. The Account will not bear any interests and no conversion or exchange services (including fiat-crypto exchange) will be offered at any time. Balances in the Account will not bear interest. The Zerone B.V. does not grant any credit for the use of its website or services.
- The Zerone B.V. offers basic protection and ensures that the Zerone B.V. at any time has enough funds to pay the withdrawals to the Customer.
- The Zerone B.V. shall not be responsible for any fluctuations, both down and up, of currency exchange including cryptocurrency over short periods of time on a regular basis. Such fluctuations are due to market forces and represent changes in the balance of supply and demand. The Zerone B.V. shall not be liable for any losses or any special, incidental, or consequential damages arising from, or in any way connected to such fluctuations.
- Deposited funds are available on the Account within a reasonable amount of time after the confirmation of the deposit. Before a withdrawal can be made, all previous deposits need to be confirmed.
- The Zerone B.V. reserves the right to use additional procedures and means to verify Customer's identity (Know Your Customer) when effecting deposits into the Account. This could include (but is not limited to) a selfie with a document or form of identification.

- When depositing available virtual or FIAT currency, the Customer must ensure that the Customer is depositing an amount which is not less than the minimum deposit amount for that particular virtual currency, as displayed on the deposit page of the Account. Deposits below this limit will not be processed and will not reach the Account and nor can it be returned back to the Customer.

Account Administration

- The Zerone B.V. operates the Account, calculating the amounts the Customer has staked or offered to stake, which represents Customer's potential exposure at any time and calculating your available to play balance, from time to time.
- The amount of Principal Currency in the Account which has not yet been used for a stake (game) is available to play balance and will determine the limit.
- Any deposit made by the Customer into the Account will be held for the use until the Customer places a stake or plays a game on the Zerone B.V.'s website. The Zerone B.V. will then hold such an amount awaiting the outcome of the stake or a game.

Payouts

- When the outcome of a game the Customer participates in is determined or, where applicable, the Zerone B.V. has confirmed the relevant result of an event and settled the markets, all winnings will be paid and available for use in the Account.
- Payments are processed in a time not exceeding 48 hours from the moment of the submission of the request. Before the first payment is made to the Customer, the Customer is obliged to attach an electronic copy of a passport to confirm the identity. In cases of suspicion of placing a counterfeit or an edited copy of the documents by electronic methods, the Zerone B.V. shall have the right to send such documents to the appropriate regulatory authorities.
- Before making the payment, the Zerone B.V. will verify the correspondence of the name, surname, birth dates of the Customer and also other data. If differences are found between the actual data and the data provided by the Customer, the Zerone B.V. shall have the right to make a refund for all stakes by the Customer and refuse to pay out winnings to the Customer unless the Customer proves the identity and accuracy of entered data.
- If the Zerone B.V. by mistake credits the Account with winnings that do not belong to the Customer, whether due to a technical or human error or otherwise, the amount will remain the property of the Zerone B.V. and the amount will be transferred from the Account. If prior to the Zerone B.V. becoming aware of the mistake the Customer has withdrawn the funds, without prejudice to other remedies and actions that may be available by law or otherwise, the amount paid by mistake will constitute a debt owed by the Customer to the Zerone B.V.. In the event of an incorrect crediting, the Customer is obliged to notify the Zerone B.V. immediately by e-mail support@SportLocker.com.
- The Zerone B.V. will carry out additional verification procedures for any payout exceeding particular equivalent in that is set by the Zerone B.V. and reserves the right to carry such verification procedures in case of lower payouts.

- The Zerone B.V. reserves the right to check and verify any of the Customer's winning with the relevant provider of the games and gaming content. The Zerone B.V. shall have the right to define at its sole discretion whether the amount of the winning is substantial or not. The Zerone B.V. shall have the right to payout amounts of substantial winnings in monthly installments.
- The Zerone B.V. is not responsible for changes in the amount of payments related to fluctuations of currency (rate of exchange).
- Before ordering the first payment, the Customer must gamble 100% of the deposit. This requirement is introduced to combat fraud and "money laundering" by players.

Bonuses and contributions

- All bonuses of the Customer are limited individually to one person and depends on its personal information, behavior, technical tools Customer is using and other criterions, know to the Zerone B.V.. If bonus is provided is provided to the Customer, terms for granting/using/expiring bonus are provided to the Customer separately.
- Customers using Zerone B.V. platform shall pay commission charges to the Zerone B.V. (the "Community Contributions") for each poker game. Detail guidelines on Community Contributions are outlined in Zerone B.V.'s Terms and Conditions.

Withdrawals from the Account

- A withdrawal is subject to the Customer having made and sufficiently wagered a virtual currency/FIAT currency deposits or non-restricted bonus in Account, accrued winnings, any deposit method restrictions and/or bonus restrictions. Withdrawals will be completed to the same e-wallet address which was confirmed by the User of the Zerone B.V. Account.

The Customer may withdraw particular amount up to the available to withdraw balance in the Account by issuing the Zerone B.V. with a valid notice of withdrawal on the Zerone B.V.'s website. Withdrawals can be made in USDT and CHP (unless any other withdrawal options are introduced by the Zerone B.V.). The Zerone B.V. may request from the Customer KYC, identification documents, and/or Customer's behavior on Zerone B.V. platform will be reviewed for any irregular playing patterns. Should Zerone B.V. deem that irregular playing patterns have occurred or Customer avoid paid and available for use in the Account, providing requested personal information, Zerone B.V. reserves the right to withhold any withdrawals, and/or confiscate all prizes and bonuses.

- Customer can withdraw any amount up to the "Available to Withdraw" balance in Zerone B.V. Account by issuing Zerone B.V. with a valid notice of withdrawal within the application. Notices for withdrawals must be made via the application. The Zerone B.V. will not accept requests for withdrawal made by (i.) telephone, (ii.) analog mail (including letters), (iii.) fax or (iv.) electronic mail (including email, telegram, or social media messages).
- Considering that the Customer has submitted identification documents (if applicable), the Zerone B.V. will process the withdrawal request. The withdrawal request processing may

take from ten (10) minutes or more, if the Zerone B.V. or relevant third parties have to perform additional checks.

- After the funds have been withdrawn from the Account, the Customer is solely responsible for any freeze or confiscation that may arise due to the exchange terms of use that restrict transactions from gambling websites. The Customer must always read and understand exchange's or other wallet provider terms of use and use at own risk.
- Before any withdrawals are processed, the Customer's behavior on the Zerone B.V.'s website/usage of the games may be reviewed for any irregular use of any vulnerabilities. Should the Zerone B.V. deem that irregular have occurred or a vulnerability was used, the Zerone B.V. reserves the right to withhold any withdrawals and/or confiscate all winnings and bonuses and to block your account.
- In the case of withdrawal requests pertaining balance that was not used for wagering, the Zerone B.V. will only remit withdrawal when the extended due diligence procedure has been successfully carried out. The Zerone B.V. might apply a charge on withdrawal in amount defined at the Zerone B.V.'s sole discretion.
- The Customer acknowledges that the funds in virtual currency are consumed instantly and the Zerone B.V. do not provide for refunds or cancellation.
- Maximum limit for withdrawals of a non-deposit amount bonus or free spins winnings are not exceed the amount of a bonus applied.

Employees training

- The Zerone B.V. provides anti-money laundering/terrorism financing risk awareness training for employees. The Zerone B.V. intends to conduct trainings so frequently so Zerone B.V.'s employees would be well familiarized with latest AML/KYC practices;
- Regardless of who conduct the employees training (senior manager or external providers) employees shall be instructed about the following matters:
- Obligations under Curacao anti-money laundering/terrorism financing laws and FATF, CFATF recommendations;
- The consequences of not complying with anti-money laundering/terrorism financing requirements; 8.2.3. the types and patterns of money laundering and/or terrorism financing that the Zerone B.V.'s business or organization might face and the consequences of these risks;
- The Zerone B.V.'s compliance to anti money-laundering/terrorism financing laws, including the Zerone B.V.'s processes and procedures to identify, manage and mitigate risks related to money laundering/terrorism financing.
- Anti-money laundering/terrorism financing risk awareness training programs to all employees, director(s) of the Zerone B.V. shall be conducted by senior manager. Aforementioned programs to senior manager shall be conducted by external providers.
- Types of training, detailed training programs and its frequency shall be specified in the internal policies of the Zerone B.V..
- The Zerone B.V. ensures that Customers identifications of their identity or monitoring of their operations will be conducted by professional, well trained Zerone B.V.'s employees.

Storage of registers and Customer's data

- Zerone B.V. shall maintain, and store registers as follows:
- Register of establishment of business transactions;
- Register of continued business transactions;
- Register of terminated business transactions;
- Register of unusual/suspicious transactions.
- The registers referred to in point.
- Of the Policy shall be stored in electronic format for 5 years from the date of termination of business relations with the Customer.
- All information/explanation, data and documents related with the Customer shall be stored in electronic format for 5 years from the date of termination of business relations with the Customer.
- Zerone B.V. shall keep secure all data given by the Customer shall not sold or give to anyone else. The data may only be shared with the AML authority of the affected state if forced by law, or to prevent money laundering.

Final provisions

This Policy is approved by the Zerone B.V.'s Director. The Policy shall enter into force on the date of its approval, unless otherwise specified. The Zerone B.V.'s Policy is reviewed regularly, but at least once a year and in case any adjustments are required, the new version of the Zerone B.V.'s Policy takes effect from the date of its approval.

MLRO - Alexandre Ramalho - alexandre.ramalho@sportlocker.com

A handwritten signature in black ink, appearing to be 'Alexandre Ramalho', written in a cursive style.

