

ANTI MONEY LAUNDERING POLICY AND KNOW-YOUR-CLIENT POLICY (AML&KYC)

1. INTRODUCTION

In response to the international community's growing concern with regard to Money Laundering and possible financing of terrorism, many countries worldwide enacted or strengthened their laws and regulations regarding this subject.

The international regulating bodies have issued a number of recommendations outlining the obligations of companies with regard to Money Laundering and the fight against Terrorist Financing. These recommendations encompass provisions applicable to Svideloco N.V. (hereinafter – the "Company").

The aim of the policy of the Company is to prohibit and actively prevent Money Laundering and any activity that facilitates Money Laundering or the funding of terrorist or criminal activities by complying with all applicable requirements.

To align with the National Ordinance on Games of Chance (LOK) 2024 and the Curaçao Gaming Authority (CGA) AML requirements, the Company has implemented a comprehensive AML/CFT Compliance Program that incorporates a risk-based approach to identifying, mitigating, and managing financial crime risks. This program ensures that all departments and employees of the Company comply with:

- Regulatory requirements set forth by the Central Bank of Curacao and St. Maarten, Curaçao's Financial Intelligence Unit (FIU) and CGA.
- Know Your Customer (KYC) and Customer Due Diligence (CDD) obligations, including enhanced measures for high-risk Transactions and Customers.
- Mandatory reporting of unusual Transactions, threshold-based reporting, and immediate escalation of suspicious activities.
- Strict internal and regulatory policies for Transaction monitoring, record-keeping, and staff training.

The AML/CFT Compliance Program is approved, continuously updated, and reinforced through stringent internal controls, governance structures, and independent audits.

2. OBJECTIVES

This policy establishes the general framework for the fight against Money Laundering and Terrorist Financing throughout the Company and Company's affiliates.

The Policy is designed particularly to:

- Provide guidance to the Company and its officers and employees on the risks faced by the Company;
- Ensure appropriate management of the risks identified;
- Detect and prevent possible attempts to abuse the Company's services for conduct of Criminal Activity, Money Laundering purposes, for Terrorist Financing purposes and from attempts at contraventions of sanctions;
- Ensure compliance with legal and regulatory requirements;
- Ensure full cooperation with regulatory authorities;
- Preserve the regulatory status and reputation of the Company towards national and international authorities, thereby also protecting Company's Partners and Customers.

The objectives of this Policy are to ensure compliance with the national and international regulatory framework towards AML/CFT and for this purpose; to lay down the principles applicable to the Company's framework of internal regulation that governs the Company's operations designed in accordance with legal and regulatory requirements.

The Company is committed to high standards of anti-Money Laundering / counter Terrorist Financing (AML/CFT) compliance and requires management and employees to adhere to these standards in preventing the use of its products and services for Money Laundering or Terrorist Financing purposes.

3. DEFINITIONS



For the purposes of this Policy, the following terms, definitions, and abbreviations shall be used

AML/CFT	Anti-Money Laundering/Combating the Funding of Terrorism
5AMLD	Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of Money Laundering or Terrorist Financing, and amending Directives 2009/138/EC and 2013/36/EU
Business Relationship	Business relationship established with Customers and Partners for the provision of the Company's services with duration
Compliance Officer	The officer responsible for overall Money Laundering and Terrorist Financing deterrence and detection procedures;
Criminal Activity	Any kind of criminal involvement in the commission of punishable criminal offenses as defined in AML Law and the 5AMLD, including non-exhaustively illicit drug trafficking, activities of criminal organizations, corruption
Customer	Natural person who has applied for or with whom a Business Relationship has been established for the provision of the Company's services
SDD	Simplified Due Diligence, measures to Customers only when the risk is low
CDD	Customer Due Diligence, procedures to be able to take reasonable steps in order to determine and verify the true identity of Customers, their economic profile, the source of funds and wealth
EDD	Enhanced Due Diligence, risk assessment procedures for identification of Customers posing high risk of Money Laundering
FATF	Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against Money Laundering, Terrorist Financing and the financing of proliferation of weapons of mass destruction
FIU	The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT
Money ("ML")	Laundering means - 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 an 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 an activity; - 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.

Money Laundering consists of three stages:

- Placement. During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without paying or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- Layering. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve Transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- Integration. The re-entry of funds into the economy in what appears to be normal business or personal Transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

NOIS National Ordinance on Identification when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2010, no. 40 as last amended by N.G. 2015, no. 69).

NORUT National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2010, no. 41 as last amended by N.G. 2015, no. 68).

OFAC Office of Foreign Assets Control of the US Department of Treasury which administers and enforces economic and trade sanctions based on policies of the United States of America

Partner A legal entity that has submitted an application or with whom a Business Relationship has been established by the Company

Politically exposed person ("PEP") means a natural person who is or who has been entrusted with prominent public functions and includes the following:

- a) head of State, heads of government, ministers and deputy or assistant ministers;
- b) members of parliament or of similar legislative bodies;
- c) members of the governing bodies of political parties;
- d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
- e) members of courts of auditors or of the boards of central banks;
- f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- g) members of the administrative, management or supervisory bodies of State-owned enterprises;
- h) directors, deputy directors and members of the board or equivalent function of an institution of the European Union or any other international body.

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials

Shell Bank Credit institution or an institution engaged in equivalent activities incorporated in a jurisdiction which it has no physical presence, involving



		meaningful mind and management, and which is unaffiliated with a regulated financial company
Terrorist ("TF")	Financing	Means the provision or collection of funds and other assets, by any means, directly or indirectly, with a view to, or in the knowledge that those means will be used in full or in part by a terrorist organization or by a terrorist acting alone, even without any connection to a particular act of terrorism. The most basic difference between financing of terrorism and Money Laundering involves the origin of the funds. Terrorist Financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money Laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, TF is mostly concerned with obscuring the end recipient of the funds.
Transaction		An action or combination of actions by or on behalf of the Natural or legal person as referred to in art. 1, par. 1, sub o, of the NOIS or art. 1, par. 1, sub c, of the NORUT
United Nations ("UN")		United Nations, an intergovernmental organization tasked to promote international cooperation and to create and maintain international order

4. POLICY STATEMENT

This policy statement expresses the commitment to combat the abuse of its facilities, products and services for the purpose of Money Laundering and Terrorist Financing.

The policy states about the intention to comply with current anti-Money Laundering and Terrorist Financing legislation as well as provisions and guidelines, in particular the laws and guidelines regarding Customer Due Diligence and the reporting of unusual Transactions, i.e. the NOIS and the NORUT and abide by all applicable laws and regulations on AML/CFT applicable to its operations in all jurisdictions they are conducted, and has for this purpose:

- Established a risk-based AML/CFT approach which includes all necessary measures to mitigate against financial crime.
- Developed and implemented a comprehensive internal framework of policies, procedures, measures and controls to identify, manage and control risks that arise in the context of its business and at all stages of Business Relationship with Customers and Partners.

To ensure compliance and prevent abuse of its services, the Company conducts its business in compliance with the following main general principles:

- take reasonable steps to determine the true identity of all Customers/Partners and ensure that none of its Customers/Partners are subject to financial sanctions as listed by the EU, UN, OFAC, or other applicable body established by which applies to the Company;
- do not knowingly accept funds from, or engage in any business relations with Customers/Partners whose money, the Company reasonably believes, is derived from Criminal Activity;
- do not open anonymous accounts;
- do not cooperate with Shell Banks in any way possible;
- monitor transactional activity of its Customers to prevent the abuse of products and services for illicit purposes;



- take seriously any indications that a Customers/Partners' money might potentially originate from criminal or other Money Laundering activities. If the Company becomes aware of facts which lead to a reasonable presumption that funds held by it are from criminal or other Money Laundering activity or that Transactions entered into are themselves criminal in purpose, appropriate measures, consistent with the law, will be taken, including denial of provision of services to the Customer, severing relations with the Customer/Partner, closing or freezing Transactions and filing of a suspicious activity report wherever required and appropriate;
- do not support or assist Customers seeking to deceive law enforcement agencies through the provision of false, altered, incomplete or missing information;
- cooperate fully with law enforcement and regulatory agencies to the extent that it can under all applicable international and domestic laws; and,
- report all identified instances of suspicious activity to the extent that it can do so under all applicable foreign and domestic laws.

To ensure compliance with above principles, the Company:

- Has appointed designated personnel responsible for compliance with anti-Money Laundering and Terrorist Financing provisions.
- Established Customer Due Diligence ("CDD") and know your Customer ("KYC")/know your business ("KYB") procedures to be able to take reasonable steps in order to determine and verify the true identity of its Customers and Partners, their economic profile, the source of funds and wealth.
- Established procedures for ongoing monitoring of its Customers and Partners.
- Developed and implemented appropriate methods of control to detect suspicious activity of its Customers/Partners and take appropriate actions.
- Established risk assessment procedures for identification of Customers/Partners posing high risk of Money Laundering where application of Enhanced Due Diligence ("EDD") measures is required.
- Has identification and monitoring procedures in place to ensure that none of its Customers/Partners are subject to local and international sanctions.
- Has procedures for identification and monitoring of Customers falling in the category of PEP.
- Has procedures for identification and monitoring of Partners associated with PEPs.
- Reports all identified instances of suspicious activity to government authorities in accordance with applicable requirements.
- Informs and trains all employees, including management, on the matters covered in this Policy.
- Complies with applicable requirements established by law for the obtaining of documents and record-keeping.
- Cooperates fully with the government authorities to the extent that it can do so under all applicable foreign and domestic legislation.

5. GOVERNANCE

To monitor compliance with legal requirements, the Company established Compliance department developing AML/CFT and KYC/KYB procedures, obligatory for all employees of the Company and determining the policy of engagement with Customers and Partners.

6. RISK ASSESSMENT

The Company is required to assess on a yearly basis the risks of Money Laundering and Terrorist Financing, taking into account risk factors:

- Governance;
- Customers/Partners;
- Countries or geographic areas of operation;
- Employees;
- Products or services; and
- Payments.

The purpose of AML risk assessment is to identify, analyze, assess and mitigate any potential ML/FT risks and any other associated risks that the Company may be exposed to in relation to laundering of proceeds of crime and financing of terrorism.



Applying Risk-based Approach means that the Company has to:

- Assess the risks that Money Laundering or Terrorist Financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Record the risk assessments, including everything that has been done and the reason for this being done.

The steps of the risk assessment methodology are as follows:

- Identification
- Analysis and Assessment
- Taking appropriate actions to ensure effective minimization or mitigation of identified risks.

This approach also allows Company to prioritize its actions and focus on risks presenting greater severity and likelihood of materialization.

The Company will collect certain Customer's identification information from each Customer; utilize risk-based measures to verify the identity of each Customer; record Customer identification information and the verification methods and results; and compare Customer identification information with government-provided and other public resources.

The Company will collect certain Partner identification information from each Partner:

- For the Partner and corporate shareholder of the Partner:
 - a) Certificate of Incorporation/Registration;
 - b) Certificate/Corporate Register of Directors;
 - c) Certificate/Corporate Register of Shareholders;
 - d) Memorandum and Articles of Association;
 - e) Certificate of Good Standing (not older than 6 months);
 - f) Operating License Certificate;
 - g) Corporate Structure.
- For each Individual Director the copies of the following:
 - a) Passport of ID card (Certified copy);
 - b) Copy of the utility bill (not older than 3 month).
- For each Corporate Director:
 - a) Certificate of Incorporation/Registration;
 - b) Certificate/Corporate Register of Directors;
 - c) Certificate/Corporate Register of Shareholders.
- For each Beneficial Owner:
 - a) Passport of ID card (Certified copy);
 - b) Copy of the utility bill (not older than 3 month).

The Company complies with local and international regulatory requirements, sanctions lists of competent authorities (FATF, UN, EU, OFAC) against countries, legal entities, financial institutions and natural persons.

The screening procedure, taking place at first deposit and throughout the course of the Business Relationship, includes screening against Sanctions Lists, PEP Lists.

Wherever a match with a sanctioned individual is determined to be a true match, the following steps will take place:

- Relationship with the Customer is terminated or not established;
- Compliance Officer informs Management;
- Compliance Officer shall file a report to relevant FIU, if apart from Customer/Partner being sanctioned, there is also knowledge or suspicion on AML/CFT; and,



- Compliance Officer shall report to the respective governmental agencies for further guidance in relation to blocking and freezing of funds.

Wherever a PEP is identified, the following steps will take place:

- Senior management approval to service the PEP should be obtained;
- Source of wealth and, where applicable, their source of funds should be established;
- Enhanced on-going monitoring of the Customer's activity should be conducted.

7. KNOW YOUR CLIENT

Customer Identification and Verification:

The Company has established standards regarding KYC. These standards require due diligence on each prospective Customer before entering into a Business Relationship:

- via identification and verification of his identity and, as the case may be, his representatives on the basis of documents, data or information obtained from a reliable and independent source compliant with the domestic and European anti-Money Laundering legislation and regulations;
- via obtaining information on the purpose and intended nature of the Business Relationship.

Prior to opening an account for the Customer, the Company will collect the following information for all accounts for any person that is opening a new account and whose name is on the account (Preliminary identification):

- a) the Customer's full name;
- b) the Customer's permanent residential address;
- c) the Customer's IP address;
- d) date of birth;
- e) place of birth;
- f) nationality;
- g) identity number.

The Company does not allow its Customers to open anonymous accounts. In low risk scenarios the Company may limit identification to the personal details set out in (a) to (g) above.

The Company does not allow its Customers to make any Transactions or money withdrawal from the accounts till Complete identification (hereinafter – the "Complete identification").

Prior to allowing any Transactions or money withdrawal from the account for the Customer the Company will conduct Simplified Due Diligence and collect the following information about the Customer:

- the name (name confirmation);
- date of birth (confirmation);
- an address, which will be a residential or business street address (for an individual), or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and
- an identification number or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard; and
- phone number.

The Company has developed a list of documents, the provision of which is necessary for a Customer for the purpose of Complete identification, namely:

- color passport copy (first and second pages with photo, as well as a page with data of registration);
- color copy of a document, which is proper for Customer's identity verification under the law of the country of residence;
- a copy of driver's license (upon the Company's request);
- a receipt of payment of utility bills to confirm the place of residence of the Customer (upon the Company's request);

Also, the verification process involves mandatory confirmation of Customer's phone number.



Based on the risk, and to the extent reasonable and practicable, the Company will ensure that it has a reasonable belief that it knows the true identity of the Customer by using risk-based procedures to verify and document the accuracy of the information it gets about Customers. The Company will analyze the information it obtains to determine whether the information is sufficient to form a reasonable belief that the Company knows the true identity of the Customer (e.g., whether the information is logical or contains inconsistencies).

The Company will verify Customer identity through documentary means, non-documentary means or both. The Company will use documents to verify Customer identity when appropriate documents are available. In light of the increased instances of identity fraud, the Company will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. The Company may also use non-documentary means, if it is still uncertain about whether the Company knows the true identity of the Customer. In verifying the information, the Company will consider whether the identifying information that it receives, such as the Customer's name, street address, zip code, telephone number, date of birth and ID number, allow us to determine that the Company has a reasonable belief that it knows the true identity of the Customer (e.g., whether the information is logical or contains inconsistencies).

The Company understands that it is not required to take steps to determine whether the document that the Customer has provided to the Company for identity verification has been validly issued and that the Company may rely on a government-issued identification as verification of a Customer's identity. If, however, the Company notes that the document shows some obvious form of fraud, the Company must consider that factor in determining whether it can form a reasonable belief that the Company knows the Customer's true identity. The Company may request any additional documents deemed necessary and appropriate for AML policy.

The Company will use the following non-documentary methods of verifying identity:

- Independently verifying the Customer's identity through the comparison of information provided by the Customer with information obtained from a consumer reporting agency, public database or other source [identify reporting agency, database, etc.];
- Checking references with other financial institutions; or
- Obtaining a financial statement;
- Phone calls to the Customer.

If a potential or existing Customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not open a new account and, after considering the risks involved, consider closing any existing account.

8. KNOW YOUR BUSINESS

Partner Identification and Verification:

The Company has established standards regarding KYB. These standards require due diligence on each prospective Partner before entering into a Business Relationship if:

- an occasional Transaction with the Partner amounts to €15,000 or more when the Transaction is carried out in a single operation or in several operations that appear to be linked.

The Company will collect certain Partner identification information from each Partner:

- For the Partner and corporate shareholder of the Partner:
 - a) Certificate of Incorporation/Registration;
 - b) Certificate/Corporate Register of Directors;
 - c) Certificate/Corporate Register of Shareholders;
 - d) Memorandum and Articles of Association;
 - e) Certificate of Good Standing (not older than 6 months);
 - f) Operating License Certificate;
 - g) Corporate Structure.
- For each Individual Director the copies of the following:
 - a) Passport or ID card (Certified copy);



- b) Copy of the utility bill (not older than 3 month).
 - For each Corporate Director:
 - a) Certificate of Incorporation/Registration;
 - b) Certificate/Corporate Register of Directors;
 - c) Certificate/Corporate Register of Shareholders.
 - For each Beneficial Owner:
 - a) Passport of ID card (Certified copy);
 - b) Copy of the utility bill (not older than 3 month).

A "Beneficial Owner" is defined for the purposes of this Policy as any individual who: (i) exercises ultimate control over the management of the body corporate; (ii) who ultimately owns or controls (in each case whether directly or indirectly), more than 10% of the shares or voting rights in the body corporate; (iii) who holds the right, directly or indirectly to appoint or remove a majority of the Board of directors; or (iv) has the right to exercise, or actually exercises, significant influence or control over the body corporate.

Where it is not possible to identify the Beneficial Owner of a body corporate after taking all necessary reasonable measures, the Company will verify the identity of the senior managing official.

The 10% threshold stated here applies without prejudice to the right of the Company to decide that a lower percentage may be indicative of ownership and control in relation to any particular Partner.

9. INDIVIDUAL RISK ASSESSMENT

The factors taken into account for the individual risk assessment and classification of Company Customers/Partners on a risk-sensitive category to Low-Medium-High:

- Customer/Partner risk;
- Geographical risk;
- Products/services and Transactions; and,
- Distribution channels risk.

The different risk variables within each of the risk categories and their subcategories are each awarded a score on a scale from 1 to 20, with extra high-risk triggers of 50 scores, where a score of 1 is the variable that poses the lowest risk and a score of 50 is the variable that poses the highest risk.

Once the scoring for each key risk category is calculated (i.e. by summing up scoring of each sub-category), the Customer is then assigned with the overall Risk Score.

In cases where the Company has determined that the Customer/Partner is risk rated as High based on the risk assessment in place, the Company has developed and implemented Enhanced Due Diligence measures ("EDD") to be applied for such Customers as part of its mitigation and minimization measures. Enhanced Due Diligence measures to be applied will depend on the high-risk scenarios portrayed by that particular Customer/Partner and will be different on a case by case basis.

Examples of such risk factors that the Company is taking into account to assess Customer/Partner as an increased risk of ML/TF and for which an Enhanced Due Diligence is applied, are:

- the home country or country of residence or registration;
- the country of birth / incorporation;
- the nationality;
- the profession;
- the economic activity;
- the appearance on sanction lists;
- the PEP-status (Politically Exposed Persons) of Customer and representatives;
- the delivery channel (face-to-face or remotely with or without safeguards);
- the source of wealth;
- the type and size of payments that could be expected.

Customers Acceptance Policy

The Company refuses to establish or to maintain a Business Relationship if the ML/TF risk related to the Business Relationship appears too high. Therefore, the Company will not enter into/maintain Business Relationships if:

- It concerns PEPs residing in high risk countries as per Transparency International's Corruption Perception Index (<https://www.transparency.org>);
- It concerns cash, cheques or physical securities without the Customer being identified face-to-face or identified remotely with safeguards;
- It concerns unlicensed/unregulated cryptocurrency platforms, custodial wallet providers or startups launching ICO's;
- It concerns arms/munitions dealers;
- It concerns unlicensed gambling entities.
- It is not satisfied that the ML/TF risk can be effectively managed, such as no or insufficient identification and verification of the identity of the Customer/Partner, his representative(s);
- The Customer's source of wealth or source of funds cannot be explained (for example through their occupation, inheritance or investments);
- The Customer, its representative is a person or institution appearing on an embargo or terrorist list issued by EU , OFAC or local authorities;
- The Customer or anyone associated with him have handled the proceeds from crime;
- There is in-house negative information about the Customer's/Partner's integrity, obtained, for example, in the course of a long-standing Business Relationship;
- The Customer/Partner, its representative is a person with whom the Company discontinued the Business Relationship in the past for AML/TF reasons;
- The Customer is under 18 years old;
- The Customer's home country or country of residence or registration is: Afghanistan, Albania, Angola, Australia, Bahamas, Botswana, Cambodia, Cyprus, Curacao, Aruba, Sint Maarten, Bonaire, Sint Eustatius, Saba, Dutch West Indies, Statia, France, Germany, Guyana, Hong Kong, Iran, Iraq, Israel, Kuwait, Myanmar, the Netherlands, North Korea, Panama, Papua New Guinea, Singapore, Spain, Sri Lanka, Taiwan, Trinidad and Tobago, Union of Comoros, the United Kingdom, the United States of America, Yemen, Zimbabwe, and All FATF Blacklisted countries, any other jurisdictions deemed prohibited by regulatory authority.

The Company shall terminate any business relationship if the identification and verification of the Customer cannot be completed or where sufficient information is not obtained. The business relation should be terminated after 30 days (might be exceeded on exceptional basis) of no response by the Customer or where there is any suspicion related to the sufficiency and accuracy/authenticity of the previously obtained identity details of the Customer.

There are four risk areas that the business risk assessment and the Customer-specific risk assessment have to cover. These are:

Customer risk

Customer risk is the risk of ML/TF that arises from maintaining relations with a given person. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. Categories of Customers whose activities may indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with Company's information about Customer's known source of income/assets);
- Casual Customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple accounts to hinder the Company to track their gambling activities;

To verify the source of funds (SOF) the Customer can be asked to provide evidence of origin of the money involved in a Transaction — bank statements, pay slips, or documents confirming the sale of an asset—that shows the funds come from a legitimate source.

If the funds come from the Customer's business, statements or records of recent Transactions showing the money was earned legally shall be provided. If the money was a gift, the Customer might need to provide a letter from the person who gave it.

During ongoing Customer Due Diligence Source of wealth (SOW) check can be required to understand a Customers' overall financial status, financial history and ensure their wealth is consistent with their background and income source. It shows how Customers accumulated their total wealth over time, including their past earnings, investments, inheritance, and any business dealings that have contributed to their current wealth. This information can be verified through employment records, investment statements, tax declaration or inheritance paperwork.

Geographical risk

The geographical risk is the risk posed to the Company by the geographical location of the Customer and the source of wealth of the Business Relationship. The nationality, residence and place of birth of the Customer have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered as high risk.

Product, service and Transaction risk

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the Customer to influence the outcome of a game, be it individually or in collusion with others. The use by Customers and the acceptance by the Company of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
- Anonymous payment methods such as pre-paid cards and virtual assets;
- Use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
- Types of specific games (e.g. roulette, craps, even bets);
- Peer to peer gaming;
- The use by Customer of accounts held or cards issued in the name of third parties;
- The transfer of funds from one gaming account to another;
- Types of financial services (credit/marker, currency exchange, check cashing);
- Multiple accounts or wallets;
- Changes to financial institution accounts to fund casino account;
- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- Using cash to fund a pre-paid card poses similar risks as cash;
- Games involving multiple operators (Poker on platforms shared by multiple operators);
- Electronic wallets (e- wallets).

Distribution channels risk

The channels through which the Company establishes a Business Relationship or through which Transactions are carried out may also have an impact on the risk profile of a Business Relationship or a Transaction:

- Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;

- Where there is the involvement of a third party in the interactions between the Customer and the Company, there is also an increase of risk. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations.

Ongoing Due Diligence

Periodic and risk-based reviews are carried out to ensure that Customer-related documents, data or information are kept up-to-date.

In order to implement effective ongoing monitoring of Customer Transactions Company has implemented certain automated live time alerts. These include:

- Deposit's amount threshold alert starting from 2000 Euros;
- Withdrawal Request alert;
- Financial changes (2000/5000/10000 deposits triggers, bonus releases, big wins, Net loss players, deposit limits reached);
- Duplicated accounts flags;
- Payment IQ monitoring (Transaction monitoring, Rules System/Velocity/Fraud blockage);
- Anti-fraud alerts.

These alerts require Compliance Officer assessment and further actions as follows:

- Compliance Officer review
- Request for additional information/documents.

Pre-execution alerts, requiring manual investigation, will have to be reviewed and processed as soon as possible but no later than 3 working days once triggered.

Post-transaction monitoring alerts, requiring manual reviews and investigation, should be checked, escalated (if necessary) and closed within 3 working days from the day when they were triggered.

Periodic and risk-based reviews are carried out to ensure that Partner-related documents, data or information are kept up-to-date. The Partner-related documents shall be renewed/updated every year.

Monitoring of Transactions

Compliance department functions ensure that ongoing Transaction monitoring is conducted to detect Transactions which are unusual or suspicious compared to the Customer's/Partner's risk profile (expected versus real transactional behavior).

An Internal AML Report ("AML Report") is drawn up from respective employees by providing detail on the suspicious Transaction or activity of the Customer/Partner, and is submitted to the Compliance Officer for his further analysis and evaluation.

In relation to the scope of suspicious Transaction identification and reporting, Company's ongoing monitoring procedures:

- Require that AML function have an understanding of the normal and reasonable account activity of each Customer (i.e. correlation with the monthly income of the Customer if available) and day-to-day activities of the Partner;
- Require immediate submission of internal suspicious AML reporting to the Compliance Officer for further investigation, whenever an employee generally dealing/communicating with the Customer/Partner discovers signs of a Transaction/activity being suspicious and determine that such Transaction:
- Could be related to funds derived from criminal activities or be designed to hide or disguise funds or assets derived from such activities;
- Could compromise funds which directly or indirectly are to be used, totally or partially, to commit terrorism activities;
- Are divided or structured to evade the reporting or record-keeping requirements of the applicable AML and TF laws and regulations.



- Compliance Officer decision on reporting/non-reporting to the relevant governmental agencies and execution/non-execution of the Transaction is clearly documented on the AML Report;
- In case of suspicion or knowledge or the Transaction being related to ML/TF, Suspicious Activity Report (SAR) / Suspicious Transaction Report (STR) report is submitted by Compliance Officer to relevant governmental agency 'promptly' (1 working day) through applicable channel (goAML portal), in accordance with respective procedure implemented by the authorities.

The investigation commenced by Compliance Officer shall include:

- Detailed analysis of the profile of the Customer/Partner, its activity
- Analysis of supporting and related documentation (proof of wealth, source of funds etc.)
- Screening publicly or commercially available information
- Analysis of conformity or lack thereof between Customer's/Partner's profile and Transaction.

Recordkeeping

Records of personal data obtained for the purposes of the prevention of Money Laundering and Terrorist Financing are processed and kept in accordance with the EU and local requirements and shall not be further processed in a way that is incompatible with those purposes.

Company shall maintain the below-listed documents for at least 5 years, unless a longer period is specified by special national legal requirements or as required by the FIU, relevant supervisory authorities or law enforcement agencies when necessary for the purposes of the prevention, detection, analysis and investigation of ML/FT activities. Should the latter be the case, the period required by can never exceed 10 years.

The following documentation to be kept are:

- Documents containing information on the identification and knowledge of the Customer/Partner;
- Records with full details of Customers/Partners or groups of connected Customers/Partners;
- Register of all cases of prospective Customers/Partners for which the Company declines the establishment of Business Relationship;
- Register of terminated Customers/Partners;
- Investigations and Reports made to the government authorities concerning suspicious Customer/Partner activity relating to possible Money Laundering and/or Terrorist Financing, accompanying with supporting documents;
- Records of all courses and training given on the prevention of Money Laundering and Terrorist Financing; and,
- Any other documents and registers required to be retained by the special provisions of the local AML laws and regulations.

Documentation held may either be in physical format, electronically or both. In cases where documents certified by third parties, the physical document bearing the original third-party certification should be retained on file and not a copy thereof.

10. MONITORING ACCOUNTS FOR SUSPICIOUS ACTIVITY

The Company will monitor Customer's account activity for unusual size, volume, pattern or type of Transactions, taking into account risk factors and red flags that are appropriate to Company's business.

The Red flags are:

- the Transaction amount is more than 2000 EUR or equivalent of this amount;
- money withdrawal from the account is more than 2000 EUR or equivalent of this amount;
- wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent reason;
- Transactions patterns show a sudden change inconsistent with normal activities;
- A Customer provides insufficient, false or suspicious information or is reluctant to provide complete information;
- Methods or volumes of payment that are not consistent with the payment policy or that are not customarily used in the course of business, e.g., payments with money orders, traveler's checks, and/or multiple instruments, and payments from unrelated third parties;

- Receipts of multiple negotiable instruments to pay a single invoice;
- Requests by a Customer or Partner to pay in cash;
- Early repayments of a loan, especially if payment is from an unrelated third party or involves another unacceptable form of payment;
- Orders or purchases that are inconsistent with the Customer's trade or business;
- Payments to or from third parties that have no apparent or logical connection with the Customer or Transaction;
- Payment to or from countries considered high risk for Money Laundering or Terrorist Financing;
- Payments to or from countries considered to be tax havens or offshore jurisdictions;
- Payments from countries unrelated to the Transaction or not logical for the Customer;
- A Customer's business formation documents are from a tax haven, or a country that poses a high risk for Money Laundering, or Terrorist Financing, or a country that is not logical for the Customer;
- Overpayments followed by directions to refund a payment, especially if requested to send the payment to a third party;
- Any Customer for whom you cannot determine the true Beneficial Owner;
- Structuring Transactions to avoid government reporting or record keeping requirements;
- Unusually complex business structures, payment patterns that reflect no real business purpose;
- Wire transfer activity that is not consistent with the business activities of the Customer, or which originates or terminates with parties unrelated to the Transaction;
- Unexpected spikes in a Customer's activities.

The Customer risk profile will serve as a baseline for assessing potentially suspicious activity. The Compliance department will be responsible for this monitoring, will review any suspicious activity that Company's monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

11. ORGANISATION OF INTERNAL CONTROL

Suspicious Transactions Reporting

Compliance department is appointed to ensure that unusual Transactions that have been detected are reported to the appropriate authority. The reporting of suspicious Transactions must comply with the laws and regulations of the respective local jurisdiction.

The Company will report any unusual Transaction or any intended unusual Transaction to the FIU without delay.

The Company is responsible for the identification and reporting to the FIU of Transactions that can be qualified as unusual Transactions.

The following Transactions or intended Transactions are deemed unusual:

- a. Transactions which in connection with Money Laundering or Terrorist Financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance ("Sanctielandsverordening", N.G. 1997, 336 as last amended).
- c. Transactions in the amount of 2000 EUR (or equivalent) = or more, regardless whether the Transaction is made in cash, by check or other form of payment, or through electronic or other nonphysical means.
- d. Presumed Money Laundering Transactions or Terrorist Financing: Transactions where there is cause to presume that they can be related to Money Laundering or Terrorist Financing.

In the event multiple places appear to be acting in unison, the amounts of their individual Transactions shall be added together to evaluate whether the Transactions need to be reported.

The Company will examine, as far as reasonably possible, the background and purpose of all complex, unusual large Transactions, and all unusual patterns of Transactions, which have no apparent economic or lawful purpose, in order to decide whether or not to report the Transactions as unusual Transaction to the FIU.

The Company will maintain records, containing the information and documentation necessary to decide whether or not to report the Transaction or pattern of Transactions to the FIU, for at least five years after the Business Relationship is ended, or after the date of the occasional Transaction or Transaction pattern).

Procedures

All the Company's departments have implemented AML/CFT rules into operational procedures taking into account their type of activities, their volume and their size together with the local legal and regulatory requirements.

Training

The Company developed a coherent training program, including follow-up trainings on a regular basis (in-class trainings, E-learning, webinars), in order to create and maintain a satisfying AML/CFT awareness.

The Compliance Officer shall ensure that this Policy is made available to all employees and across all business lines. Where technical implementation is required, the relevant personnel is responsible for ensuring that internal working documents are established and the recommendations of the Compliance Officer are implemented and operate to meet the provided requirements.

Compliance Monitoring Program

In order to assure the effectiveness of instructions, procedures and processes, recurrent quality controls are performed in the AML/CFT-domain pursuant to a Compliance Monitoring Program.

The policy will be reviewed regularly by the compliance function and the Compliance Officer, at minimum annually, and as set out by the following criteria;

- Annually: no later than 12 months from the date upon which the Policy was last reviewed;
- Upon the change of any relevant law or regulation which applies to the Policy;
- Upon the finding by any regulator, external or internal audit that an amendment to the Policy is required;
- Upon the award of any new gambling license in any new jurisdiction;
- Upon a new product implementation or acquiring a new product / vertical;
- Whenever significant changes occur in the business, that will have a direct or indirect impact on the area this document concerns.

Ecorpp Management N.V. Boy Hendriks

On behalf of Svideloco N.V.:



Annex 1: APPLICABLE LEGISLATION, REGULATIONS & GUIDANCE

Curaçao Legislation

- National Ordinance on Games of Chance (LOK) 2024
 - a. Establishes the legal framework for gaming operators in Curaçao.
 - b. Defines AML/CFT compliance obligations, including Customer Due Diligence, reporting, and risk assessments.
 - c. Mandates internal controls and governance measures to prevent financial crime.
- National Ordinance Reporting Unusual Transactions (NORUT)
 - a. Requires operators to identify and report Unusual Transaction Reports (UTRs) to the Financial Intelligence Unit (FIU).
 - b. Establishes legal requirements for record-keeping, sanctions screening, and Compliance Officer responsibilities.
- National Ordinance on Identification when Rendering Services (NOIS)
 - a. Mandates strict identity verification procedures for gaming operators.
 - b. Outlines requirements for CDD, EDD, and beneficial ownership transparency.
- Financial Intelligence Unit (FIU) Directives
 - a. Specifies the format and procedures for submitting UTRs/SARs via the goAML platform.
 - b. Requires enhanced monitoring and reporting for Transactions linked to high-risk jurisdictions.

International Regulations & Standards

- Financial Action Task Force (FATF) Recommendations
 - a. Establishes global AML/CFT best practices for identifying and mitigating financial crime risks.
 - b. Requires a risk-based approach to compliance, sanctions screening, and Transaction monitoring.

United Nations & European Union Sanctions

- Prohibits Transactions with sanctioned individuals, countries, or organizations linked to ML/TF.

Annex 2: KYC procedures and checks (CONFIDENTIAL, FOR INTERNAL USE ONLY)

Customer pre-checks procedures	
Name	Description
IP address analysis	Analysis of an Applicant's IP address using multiple factors (whether it belongs to public/private ranges, residential proxy, anonymous VPN providers or anonymous networks, or Tor exit nodes). The geodata attributed to the IP address (e.g., country, city, coordinates) is extracted, and the IP address itself is assigned a risk label.
Identity Enrichment using email and/or phone number linked data	By analyzing the email and phone number provided by the applicant, we can find the data linked to this email and phone number. It returns DoB, Gender, Name, and address based primarily on telco and social media data.
Phone Risk Assessment	Opportunity to screen applicant's phone number to get the risk labels based on its registrations on the web, domain name, delivery option and other parameters. The risk label can be used as a condition for further checks.
Email Risk Assessment	Opportunity to screen applicant's email address and get the risk labels based on its registrations on the web, domain name, delivery option and other parameters. The risk label can be used as a condition for further checks.
Video Identification	
Name	Description
Video Identification	Platform (third party service) to carry out identity verification procedures (incl. collection of documents) via video interviews conducted by operators engaged by the Company.
Fraud Network Detection	
Name	Description
Fraud Network Detection	Continuous monitoring of Applicants' personal data, behavior and connections to detect potentially fraudulent networks, reviewing potentially fraudulent networks of Applicants and, where the suspicion is confirmed, presenting the investigation results. The Platform (third party service) groups suspicious Applicants based on shared facial images, documents, proof of address templates, IPs and device fingerprints, geo-location and address, personal information, or behavioral patterns.
Payment Method Check	
Name	Description
Payment Method Check	Verification that a bank card, crypto wallet, online payment platforms, and wire transfer truly belong to a user. Chargebacks, fraudulent Transactions, sending funds to third parties, and sending funds from suspicious accounts

	are eliminated by identifying the payment source before Transactions are made.
KYC	
Name (Steps)	Description
Identity Document Verification	Determination of whether an identity document is authentic, legitimate, and free of forgery or alteration.
Ongoing ID document monitoring	Daily re-check of the validity of an identity document previously submitted by the Applicant, based on its expiry date. This includes sending automated requests for replacements if a document expires.
Additional fields extraction	Extraction of custom fields, depending on regulatory requirements and/or business needs. These may include gender, tax number, address, additional number, etc.
Liveness & Face match	Biometric analysis of an Applicant's facial movements compared with photographs on the submitted identity documents in order to ensure that the Applicant is alive and present at the time of the identity verification.
Known face search	Determination of whether an Applicant's facial data is already present in the Company's databases.
Proof of Address Verification	Verification of address and residency through analysis of the following documents:- IDs bearing residential address;- Tax bills;- Utility bills;- Voter rolls;- Bank statements;- Other documents commonly accepted as proof of address.
Geolocation as Proof of Address Check	Detection of an Applicant's location using geolocation data from their device and verifying it against the pre-set rules.
AML Screening: PEPs, sanctions, watchlists and adverse media	Determination of an Applicant's presence on or absence from global sanctions lists, PEP lists, watchlists, blocklists, or adverse media (OFAC, UN, HMT, EU, DFT etc.). The results of this Check are solely based on potential matches between an Applicant's personal data and the data contained in databases available.
Ongoing AML monitoring (KYC)	Daily re-check of an Applicant's full name and date of birth against the available sanctions lists, PEP lists, adverse media, and other data sources as specified in the AML Screening description.
Email Verification	Verification of email addresses to ensure whether they are valid and belong to a real person. This includes:- Authentication with a code to ensure that the Applicant has access to their mailbox;- Cross- validation of the Applicant's name, email address, IP address country and phone number country;- Duplicate search, where possible (e.g. different persons have the same email address);- Review whether an Applicant with this email address was involved into a fraudulent activity, where possible;- Overall risk assessment of the email address, scored on a scale of zero to one.
Phone Verification	Verification of phone numbers to ensure whether they are valid and belong to a real person. This includes:- Authentication with a code to ensure that the Applicant can be reached at this phone number;- Cross-validation of the Applicant's name, email address, IP address country and phone number country;- Duplicate name search, where possible (e.g. different persons have the same phone number);- Review whether an Applicant with this phone number was involved into a fraudulent activity, where possible;- Overall risk assessment of the phone number, scored on a scale of zero to one.

Face Authentication	Biometric analysis of a person's facial movements that is compared with photographs on submitted ID documents or previous selfies. This is to ensure that a person is alive and to make sure of their presence at the time of the authentication.
Facial Age Estimation	The third-party solution automatically gives an approximate estimate of an Applicant's age based on the results of the Liveness Check previously passed by that Applicant. Received age estimate can be compared to the internal age limit established by the Company for its service (if any).
Document Processing	
Name	Description
ID data extraction	Automated extraction of data from identity documents for further processing. Five fields are extracted: First name, Last name, Date of birth, Document number, Date of expiry.
Bank card data extraction and sensitive data masking	Automated extraction of data from bank cards, including third-party technology that protects sensitive data in accordance with data privacy and protection laws and PCI DSS.
Proof of Address data extraction	Automated extraction of address data from documents for further processing. By default, three fields are extracted: Full name,- Address,- Date of issue.
Fraud Prevention	
Name	Description
Higher-risk applicant control and alert	Where identity theft is suspected or proven for the following reasons: Document forgery (physical or digital); Documents of another person; Stolen/leaked documents; Deepfake; Account abuse from one device; Registration coerced by another person; Account registration without the document owner's knowledge, etc.
Duplicate search	Search for Applicants with the same personal data
Behavioral risk score	Calculation of an Applicant's behavioral risk score based on various parameters: Device Fingerprinting (IP, country),- Data inconsistency,- Suspicious behavior factors.
Anti-photoshop check	Checking if graphic editors were used to change the data on the submitted images.
Security features check	Checking various parameters of a document to identify fraud patterns: fonts,- holograms,- comparing a document with its template,- reviewing the required elements of the document.

Annex 3: DETERMINING A HIGH RISK OF MONEY LAUNDING

Factors to be considered when assessing whether there is high risk of ML or TF include whether:

- The Business Relationship is conducted in unusual circumstances;
- A Business Relationship or Transaction involves a high-risk third country;
- The Customer is resident in a geographical area of high risk;
- The Partner is incorporated in a country and/or geographical area of high risk;
- The product or Transaction might favour anonymity;
- The situation involves non-face-to-face Business Relationships or Transactions (as in the case of remote casinos), without certain safeguards, such as electronic signatures;
- Payments will be received from unknown or unassociated third parties of the Customer;
- New products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies (such as virtual currencies) for both existing and new product;
- The Business Relationship or Transaction involves countries:
 - a. Identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter Money Laundering or Terrorist Financing;
 - b. Identified by credible sources as having significant levels of corruption or other Criminal Activity, such as Money Laundering, terrorism, and the production and supply of illicit drugs, or subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations;
 - c. Providing funding or support for terrorism;
 - d. That have organisations operating within their territory which have been designated, by the government of Curacao, as proscribed organisations under the Terrorist Act or, by other countries, international organisations or the European Union as terrorist organisations; or
 - e. Identified by credible sources (such as evaluations, detailed assessment reports or follow-up reports published by FATF, the International Monetary Fund, the World Bank, the organisation for Economic Cooperation and Development or other international bodies or non-governmental organisations) as not implementing requirements to counter Money Laundering and Terrorist Financing that are consistent with the FATF recommendations.
- The Customer transacts with significant amounts of cash;
- The Customer provides false, forged or stolen identification documentation upon establishing a Business Relationship;
- The Customer transacts with multiple remote gambling operators, particularly where this occurs across multiple geographical areas;
- The product, service or Transaction involves peer-to-peer gaming;
- The product is electronic roulette; and
- The product, service or Transaction involves Ticket In/Ticket Out (TITO) or similar technology.

Annex 4: CRYPTO POLICY

Introduction

The Company accepts cryptocurrency as a method of payment. This Crypto Policy establishes the framework governing the use of cryptocurrencies in order to mitigate risks related to Money Laundering (ML), Terrorist Financing (TF), fraud, and sanctions violations.

The Company applies a **risk-based approach** to all cryptocurrency-related activities and ensures full compliance with applicable AML/CFT laws, FATF recommendations (including the Travel Rule), and internal AML/KYC policies.

Definitions

Cryptocurrency - digital or virtual currencies that use cryptography for security. Accepted cryptocurrencies include, but are not limited to: Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Dogecoin (DOGE), Bitcoin Cash (BCH), Ripple (XRP), TRON (TRX), Binance Coin (BNB).

Wallet - a software or hardware-based digital storage system used by users to manage cryptocurrency funds.

Blockchain Analytics Provider - a third-party service used to assess the risk level of cryptocurrency wallets and transactions (e.g., identifying links to darknet, sanctions, fraud, or illicit activity).

Risk-Based Approach

Cryptocurrency transactions are considered **high-risk by default** due to:

- Pseudonymity
- Cross-border nature
- Irreversibility of transactions

The Company applies:

- Enhanced monitoring
- Wallet risk scoring
- Transaction tracing

High-risk transactions are subject to **Enhanced Due Diligence (EDD)**.

Accepted Cryptocurrencies and Conversion

The Company reserves the right to:

- Modify the list of accepted cryptocurrencies at any time
- Reject specific cryptocurrencies based on risk assessment

All cryptocurrency transactions:

- Are subject to real-time exchange rates
- Are processed based on market conditions at the time of execution

The Company bears no responsibility for:

- Price volatility
- Network delays
- Blockchain congestion

Deposits

- Customers may deposit funds using approved cryptocurrencies only
- Each deposit is credited after sufficient blockchain confirmations
- The required number of confirmations varies by blockchain

The Company reserves the right to:

- Delay or reject deposits flagged as high-risk
- Request additional verification prior to crediting funds

Deposits from:

- Mixing/tumbling services

- Privacy-enhancing tools
- Sanctioned or blacklisted wallets

will be rejected and reported where applicable.

Withdrawals

Cryptocurrency withdrawals are subject to:

- Full KYC verification
- AML screening
- Internal approval procedures

Additional controls:

- Withdrawal wallet must belong to the Customer (where technically feasible)
- First-time withdrawal addresses may require verification (e.g., ownership proof)

The Company reserves the right to:

- Delay, suspend, or refuse withdrawals
- Request Source of Funds (SOF) or Source of Wealth (SOW) documentation

The Company is not responsible for:

- Incorrect wallet addresses provided by the Customer
- Loss of funds due to user error

Wallet Screening and Blockchain Analytics

All cryptocurrency transactions are subject to **wallet screening** using third-party blockchain analytics tools.

The Company performs:

- Risk scoring of wallets
- Transaction tracing
- Exposure analysis (direct and indirect links)

Transactions may be flagged if linked to:

- Sanctioned entities (OFAC, EU, UN lists)
- Darknet marketplaces
- Fraud, scams, ransomware
- Mixing services or obfuscation tools

High-risk scores trigger:

- Manual review
- Enhanced Due Diligence
- Possible account restriction

Prohibited Activities

The Company strictly prohibits:

- Use of cryptocurrency derived from illegal activities
- Attempts to obscure transaction origin (e.g., mixers, tumblers)
- Use of third-party wallets without justification
- Structuring transactions to evade AML controls

Any such activity will result in:

- Account suspension or termination
- Freezing of funds (where legally permitted)
- Reporting to relevant authorities

Transaction Monitoring

All cryptocurrency transactions are monitored in real time and post-transaction.

Red flags include:

- Rapid deposits and withdrawals with minimal gameplay

- High transaction volume inconsistent with customer profile
- Use of multiple wallets
- Frequent address changes
- Links to high-risk jurisdictions

Threshold-based monitoring applies (e.g., €2000+ or equivalent).

Travel Rule Compliance

Where applicable, the Company complies with the **FATF Travel Rule**, requiring:

- Collection and transmission of originator and beneficiary information
- Cooperation with Virtual Asset Service Providers (VASPs)

Transactions involving VASPs may require:

- Additional verification
- Data exchange compliance

Enhanced Due Diligence (EDD)

EDD is applied where:

- High-risk wallets are identified
- Customer uses large volumes of crypto
- Activity is inconsistent with profile

EDD measures may include:

- Source of funds verification
- Blockchain transaction history analysis
- Additional identity verification

Record Keeping

The Company retains:

- Wallet addresses
- Transaction hashes
- Risk scoring results
- Investigation records

Retention period: Minimum 5 years (or longer if required by law)

Security Measures

The Company implements:

- Secure wallet infrastructure (hot/cold wallet segregation where applicable)
- Encryption and access controls
- Fraud detection systems

The Company may suspend transactions if:

- Security risks are identified
- System integrity is compromised

Reporting Obligations

Suspicious cryptocurrency transactions are:

- Escalated internally
- Reported to the FIU (via SAR/STR) within required timelines

The Company cooperates with:

- Law enforcement
- Regulatory authorities

Annex 5: RISK APPETITE STATEMENT**Purpose**

This Risk Appetite Statement defines the level and types of risk that the “Company is willing to accept in pursuit of its strategic objectives, while ensuring compliance with applicable Anti-Money Laundering (AML), Counter-Terrorist Financing (CFT), and regulatory requirements.

The Statement provides a framework for consistent risk-based decision-making across all business activities, including Customer onboarding, transaction monitoring, and partnerships.

Risk Appetite Overview

The Company adopts a **conservative risk appetite** with respect to financial crime risks, including Money Laundering (ML), Terrorist Financing (TF), fraud, and sanctions violations.

The Company has **zero tolerance** for:

- Knowingly facilitating ML/TF activities
- Breaches of international sanctions (EU, UN, OFAC)
- Engagement with prohibited or blacklisted entities
- Use of shell banks or anonymous accounts

The Company has **limited tolerance** for:

- High-risk Customers (subject to Enhanced Due Diligence)
- Complex ownership structures (with transparency requirements)
- High-risk jurisdictions (case-by-case approval)

The Company has **moderate tolerance** for:

- Medium-risk Customers with verifiable source of funds
- Use of digital payment methods, including cryptocurrencies (subject to monitoring)

Risk Categories and Appetite Levels

a. Customer Risk

<u>RISK LEVEL</u>	<u>APPETITE</u>	<u>APPROACH</u>
Low	High	Simplified Due Diligence (SDD)
Medium	Moderate	Standard CDD
High	Low	EDD
Prohibited	None	Rejected

b. Geographic Risk

<u>RISK LEVEL</u>	<u>APPETITE</u>	<u>APPROACH</u>
Low-risk countries	High	Standard onboarding
Medium-risk countries	Moderate	Enhanced monitoring
High-risk	Low	EDD
Prohibited/Sanctioned	None	Rejected

c. Transaction Risk

The Company has **low tolerance** for:

- Structuring (smurfing)
- Rapid deposits and withdrawals without gameplay
- Third-party payments

Transactions exceeding defined thresholds (e.g., €2000+) are subject to enhanced monitoring and review.

Risk Acceptance Criteria

The Company will only accept Customers and Partners where:

- Identity is verified

- Source of funds/wealth is understood
- Risk level is manageable within internal controls

The Company will **reject or terminate relationships** where:

- Risk exceeds defined thresholds
- Required information is not provided
- Suspicious activity is identified

Monitoring and Reporting

The Company ensures:

- Continuous transaction monitoring
- Automated and manual alerts
- Escalation of suspicious activity

Where risk exceeds appetite:

- Immediate review is triggered
- Relationship may be suspended or terminated
- Suspicious Activity Reports (SAR/STR) are filed

Alignment with AML/CFT Framework

This Statement is aligned with:

- AML/KYC Policy
- FATF Recommendations
- Curaçao regulatory requirements (LOK, NOIS, NORUT)
- EU AML Directives (where applicable)