

**Anti-Money Laundering and Financing of
Terrorism Policy**

Novi B.V.

Key Information

Name	Description
Document Name	Anti-Money Laundering and Financing of Terrorism Policy
Version	3.1
Author	Novi B.V. – Compliance Dep.
Authorised By	Novi B.V. – Board of Directors
Distribution Date	01.09.2025
Next Review Date	30.01.2026

Table of Contents

Key Information	2
1. Policy Statement	4
2. Purpose.....	5
3. Audience.....	5
4. Definitions	5
4.1 The Company understands money laundering as:	5
4.2 The Company understands Terrorist financing as:.....	6
4.3 The Company understands Proliferation financing as:.....	6
5. Policy Implementation	6
5.1 Business Risk Assessment.....	6
5.2 Customer Risk Assessment.....	7
5.3 Customer Acceptance Policy (CAP)	8
5.3.1 Risk appetite of the Company	8
5.3.2 Refusing Business Relationship	8
5.3.3 Politically Exposed Person (PEP) Definition and Screening	9
5.3.4 Sanctions Screening.....	9
5.4 Customer Due diligence	10
5.4.1 Account - Identity Verification	10
5.4.2 Verification Process.....	10
5.4.3 Enhanced Due Diligence (EDD).....	11
5.5 Ongoing Monitoring	12
5.6 Reliance on Third Parties for Customer Due Diligence.....	13
5.7 Reporting Unusual Transactions.....	14
5.8 Anti-Money Laundering Compliance Program	15
5.8.1 Money Laundering Reporting Officer ("MLRO")	15
5.8.2 Duties and Responsibilities of the MLRO	16
5.8.3 Ongoing Training and Development.....	16
5.8.4 Management of Policy.....	17
5.8.5 Data Retention	17
5.8.6 Cooperation and Exchange of Information	17
6. Compliance and Consequences of Non-Compliance	17
7. Related Information	18
7.1 High Risk Countries.....	18
7.2 Non Serviced Countries (FATF & CFATF & International Sanctions).....	20
7.3 Suspicious Transaction Report	23
7.4 Abbreviations	24
8. Contact Information	25
9. Version History	25

1. Policy Statement

Novi B.V (the “Company”) maintains a zero-tolerance policy toward money laundering, terrorist financing, and any other form of illicit financial activity. The Company is committed to full compliance with applicable anti-money laundering (AML) and counter-terrorist financing (CFT) obligations under the laws of Curaçao and relevant international standards. This policy is the part of the Anti-Money Laundering (“**AML**”), Combating Proliferation Financing and Countering the Financing of Terrorism (“**CFT**”) framework for Novi B.V (“**Company**”) and should be considered as the governance policy of said framework and serves as a clear statement of company’s intent that can be communicated to:

- Employees;
- Clients and customers;
- Regulatory and other interested bodies.

Such policies serve as a valuable indicator of effective corporate governance. A company’s attitude towards combating Money Laundering (“**ML**”), Proliferation Financing (“**PF**”) and Terrorist Financing (“**TF**”) is increasingly viewed as indicative of the ethics with which it conducts its business. It is company’s intent that policies, procedures and processes will be developed and implemented to help combat ML/PF/TF and help maintain a safe, crime free environment for its customers to enjoy its products.

As part of its continuous improvement implementations Novi B.V is dedicated to putting in place the necessary steps needed to ensure that all employees, full-time or part-time, participate actively in preventing any of the Company’s services and/or outlets for the sole or partial purpose of money laundering and/or the financing of terrorist undertakings. The Company’s AML program is designed to be compliant with applicable legislation, regulations and directives (“**codes**”) which include but not limited to, among others, and with the following:

- Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering.
- EU Regulation 2015/847 on information accompanying transfer of funds.
- L188(I)2007 - Prevention and Suppression of Money Laundering Activities Law as amended up to March 17th, 2021
- Various EU Regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods.
- European Business Law of 18 September 2017 on the prevention of money laundering limitation of the use of cash.
- FATF Recommendations for International Standards on combating Money Laundering and the financing of terrorism and proliferation (AML/CFT)
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations’ Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations’ Security
- Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions
- Decree People’s Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

2. Purpose

The purpose of this Anti-Money Laundering and Counter-Terrorist Financing Policy is to establish a clear and consistent framework for the prevention, detection, and reporting of money laundering, terrorist financing, and other forms of financial crime within company's operations. This policy is designed to protect the Company from being used, intentionally or unintentionally, as a vehicle for financial crime and to ensure compliance with applicable codes and relevant international standards.

Through the implementation of this policy, the Company aims to:

- Prevent its services from being exploited for laundering the proceeds of crime or for financing terrorism;
- Fulfil its legal and regulatory obligations under the National Ordinance on the Reporting of Unusual Transactions and related AML/CFT laws;
- Promote a culture of compliance, integrity, and transparency throughout the organization;
- Safeguard its business operations, reputation, and the interests of its customers and stakeholders.

This policy also serves to guide employees in understanding their responsibilities and to demonstrate to regulators the Company's commitment to maintaining a robust and effective AML/CFT program.

3. Audience

The policy applies to all individuals and entities involved in the operations of Novi B.V, including but not limited to:

- All employees, including full-time, part-time, and temporary staff;
- Senior management and board members;
- Consultants and third-party service providers acting on behalf of the Company;
- Any other individuals or entities who have access to customer data, financial transactions related to the delivery of Novi B.V's services.

All covered persons are expected to be familiar with and comply fully with the requirements set out in this policy. Management is responsible for ensuring that relevant employees receive appropriate training and understand their obligations under the AML/CFT framework.

4. Definitions

4.1 The Company understands money laundering as:

- a) the conversion or transfer of funds, knowing that such funds are 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 funds 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;
- b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such funds are derived from criminal activity or from an act of participation in such an activity;
- c) the acquisition, possession or use of funds, knowing, at the time of receipt, that such funds were derived from criminal activity or from an act of participation in such an activity;
- d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

4.2 The Company understands Terrorist financing as:

Funds provided to fund terrorist activities, from a legal standpoint it means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences.

Terrorist activity has as its main objective to intimidate a population or compel a government to do something. This is done by intentionally killing, seriously harming or endangering a person, causing substantial property damage that is likely to seriously harm people or by seriously interfering with or disrupting essential services, facilities or systems.

4.3 The Company understands Proliferation financing as:

Proliferation refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

In order to effectively prevent Proliferation financing (“PF”), it is essential to disrupt the financial flows available to and used by proliferators and to obstruct the procurement of the illicit material/goods and services needed for the development of WMDs and their means of delivery.

It can be very difficult to distinguish proliferation and PF activities from ordinary trade and commerce and the financing of such trade and commerce, as those involved in proliferation and PF can go to great efforts to seek to disguise their activities. One example of this through dual-use goods, which are components used for proliferation purposes which also have a perfectly legitimate use. Examples of dual-use goods include:

- Chemicals such as chlorine, which is used in a range of household cleaning products and has industrial uses such as the sanitation of water. Chlorine can also be used to produce chlorine gas, which can be used in chemical weapons;
- Materials such as aluminium alloys and steel, which are used in the manufacture of a range of products and can be used in the development of missiles;
- Electronics such as GPS systems, gyroscopes and accelerometers, which can be used in missile systems;
- Components such as valves and vacuum pumps, which have a range of potential uses, including in the oil and gas industry, but may also be used in a WMD programme.

5. Policy Implementation

The Policy will be distributed to all staff (frontline, leads, managers and owners) and will be redistributed when updated.

The MLRO is responsible for providing a report to the Executive Management team for review of effectiveness of the Policy in every twelve (12) months.

5.1 Business Risk Assessment

Novi B.V is required to conduct a Business Risk Assessment (BRA) to identify the risks of money laundering, terrorist financing, and proliferation financing (ML/TF/PF) to which the business is exposed. This assessment helps ensure that the Company’s policies, procedures, and controls are adequate and proportionate to prevent and mitigate these risks.

The BRA considers how the Company’s products and services may be misused for ML/TF/PF, and evaluates all relevant risk factors, including:

- The type of customers;
- The nature of products and services offered;
- Delivery channels used;
- Geographic risk factors.

The Company also takes into account the findings and recommendations from Curaçao’s National Risk Assessment (NRA). Based on the results, the Company defines its risk appetite—that is, the level of risk it is willing to accept—and adjusts its AML/CFT measures accordingly.

The BRA is:

- Reviewed and updated at least annually, or whenever there are significant business or regulatory changes (e.g., new technologies, products or markets);
- Documented in full, including the methodology used, the reasons for assigning risk levels, the sources of information considered, and the outcomes;
- Approved by the Board of Directors;

The effectiveness of existing controls is monitored, and improvements are implemented as needed or least annually by MLRO. The Company remains alert to emerging ML/TF/PF threats and continuously updates its risk understanding to maintain a risk-based approach in line with regulatory expectations.

5.2 Customer Risk Assessment

The policy aims to effectively monitor the Company's customers and to enhance compliance of the Company with the policies and regulatory requirements pertaining to Client acceptance procedures.

Upon reaching the threshold (base set to Naf 4,000) the client details will be verified unless verification is not conducted at registration or first pay-out stage using E- ID/Bank ID or other equivalent technology.

Country/geographic risks, product risks, customer risks, and transaction risks will be factored into risk assessment to assign a risk score as low, medium, or high.

Figure 1. Customer Risk Assessment

	CUSTOMER -BUSINESS / CORPORATE PARTICIPANTS – LEGAL PERSONS	JURISDICTION	PRODUCT & SERVICES	CASH	TRANSACTION
High Enhanced-PEP	PEP or have a close association with a PEP & any other relevant matters or warning notices	Country subject to sanctions, embargoes	Peer to Peer e.g. Poker (not applicable)	Use of check, nominee or SPV account	Single Deposit or withdrawal ≥ Naf. 50,000
High	Criminal or adverse information in the public domain	Non-reputable/high-risk jurisdiction	Skill games etc. (not applicable)	Use of anonymous or cash payments	Single Deposit or withdrawal > Naf. 5000
Medium	Adverse publicity in the public domain	Reputable jurisdiction	Live Casino, Sportsbook	Use of an E-Wallet	Deposit or withdrawal (Lifetime) > Naf. 4000
Low	Individuals - natural persons	Full FATF AML/CFT compliance EU, Domestic)	Casino (RNG) games	Debit Card or Credit Card, Bank Transfer	Deposit or withdrawal (Lifetime) < Naf. 4000
	Nature of Participant	Jurisdiction	Product & Services	Source of Funds	Transaction

In order to deal with the different risks and different states of wealth in different jurisdictions on the international basis, the Company will categorize every jurisdiction in three different regions of risk according to identified jurisdiction risk assessments.

Region I- Low risk: For every nation from the region one in verification is done as described in section 5, and users will be subject to SDD. The company may opt to apply CDD (not simplified) even if the ML/FT risk is low.

Region II- Medium risk: For every nation from region two, CDD verification might be conducted of lower deposit/withdrawal thresholds. Specifically, ID-Account verification process will be triggered after depositing or withdrawing 2000 (two thousand Euros). Additionally, the risk level of users can upgrade to higher level in case of crypto currency in any other currency will increase the risk level and be treated as user/customers from a medium risk and users will be subject to CDD including source of payments verifications.

Region III- High risk (FATF & CFATF non-reputable & under monitoring): The users from non-reputable jurisdictions will be banned immediately. High risk regions will be regularly updated to keep up with the changing environment according to FATF/CFATF lists, Sanction lists, international embargos etc. High risk users will be subject to EDD including SOW (Source of wealth) including source of payments verifications.

CDD and/or EDD can be triggered for any jurisdiction where there is suspicion or knowledge of ML or TF, regardless of the monetary thresholds.

5.3 Customer Acceptance Policy (CAP)

5.3.1 Risk appetite of the Company

Risk appetite is an expression of the maximum level of risk that the company is prepared to accept in order to achieve our business objectives. The company's risk appetite statement translates the strategy into measurable short to medium term targets and thresholds across material risk categories and enables intra-year performance monitoring and management which aims to identify optimal growth options considering the risk involved and the allocation of available capital resources to drive sustainable performance.

The Management Board reviews and approves the risk appetite on an annual basis to ensure that it is consistent with the company's strategy, business environment and stakeholder requirements. Setting risk appetite aims to ensure that risk is proactively managed to the level desired and approved by the Management Board. Risk appetite tolerance levels are set at different trigger levels, with clearly defined escalation requirements which enable appropriate actions to be defined and implemented as required. In cases where the tolerance levels are breached, it is the responsibility of the Strategic Risk and Enterprise-wide Risk Management function to bring it to the attention of the Head of Legal and Compliance, respective risk committees, and ultimately to the Management Board.

5.3.2 Refusing Business Relationship

Players who are not registered will not be permitted to play for real money. One of the main drivers is to protect its operation from fraudulent transactions. The other key driver is preventing players from being able to launder money using our services; such money-laundering could take the form of either;

- (a) a customer gambling using funds which they have obtained through criminal conduct – proceeds of crime; or
- (b) a customer seeking to disguise the fact that they have obtained money from criminal conduct by passing it through our account in an attempt to 'clean' it.

The following categories of players will not be accepted at registration/post registration checks:

- Individuals residing in non-reputable jurisdiction,
- IP login registered in a non-reputable jurisdiction,
- Sanctioned individuals,
- Individuals under the age of 18,
- Individuals that don't provide the identification information requested by Company.

Company will not accept a and will block the users that:

- Provide fake identification documents;
- Doesn't provide CDD and/or EDD documents upon reaching the threshold in 30 days;
- Are from restricted or prohibited jurisdictions; or
- Are subjected to United States, United Nations, European Union, UK or other global sanctions or watch lists;
- Are gambling addicted or have mental health issues;
- Its source of funds originated from exchanges in restricted jurisdictions.

5.3.3 Politically Exposed Person (PEP) Definition and Screening

Politically Exposed Persons ("PEP") (as well as their families and persons known to be close associates, as described below) are required to be subject to enhanced scrutiny by the company. This is because international standards issued by the Financial Action Task Force recognize ("FATF") that a PEP may be in a position to abuse their public office for private gain and a PEP may use the financial system to launder the proceeds of this abuse of office.

PEP means a natural person who is or who has been entrusted with prominent public functions including:

- Head of State;
- Head of government;
- Minister and deputy or assistant minister;
- a member of parliament or of a similar legislative body;
- a member of a governing body of a political party;
- a member of a supreme court;
- a member of a court of auditors or of the board of a central bank;
- an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces;
- a member of an administrative, management or supervisory body of a State-owned enterprise;
- a director, deputy director and member of the board or equivalent function of an international organisation,

PEPs do not include middle-ranking or more junior officials. Family member of a PEP means the spouse, or a person considered to be equivalent to a spouse, of a PEP; a child and their spouse, or a person considered to be equivalent to a spouse, of a PEP; or a parent of a PEP.

A person known to be a close associate of a PEP means a natural person who is known to be in close business relations with a PEP.

If an account is identified as a potential match to a PEP list, it shall be immediately frozen pending escalation and review by the Risk & Fraud Department. The MLRO will be promptly notified, and no further activity shall be permitted on the account until a full assessment is conducted, and appropriate approval is obtained.

Enhanced due diligence measures will be applied which involve not only available customer-submitted information but checks of existing PEP lists and a range of news sources, including online and traditional media outlets. The Compliance Officer will reach out to the appropriate department and offer his/her recommendations regarding the account.

5.3.4 Sanctions Screening

Dealing with persons against which imposed international sanctions poses a great risk to the Company, its Directors, Officers and Owners.

The Company will perform sanction screening of its customers on the same matching rules, as for PEP screening.

The Company will perform screening, at minimum, against the following sanctions lists:

- UN Sanctions;
- EU Sanctions;
- Sanctions administered by the Office of Financial Sanctions Implementation ("OFSI-UK")
- Sanctions administered by the Office of Foreign Assets Control ("OFAC-US");
- Sanctions imposed under the International Sanction Act.

All matches (true positive hits) will be reviewed by the MLRO for further action and processing.

5.4 Customer Due diligence

5.4.1 Identification

As an identity verification measure, the company must identify and verify its customers to flag potentially risky users and monitor for suspicious activity. Verification processes are designed to help reduce the risks of illicit activity by identifying customers and verifying that this identity is correct. Doing so, suspicious characters and potentially high risk users can be flagged and monitored or banned.

Identity theft is a big problem in online gambling. Users can fraudulently obtain credit card details and use these payment methods to enter games using someone else's funds. Similarly, users can submit fraudulent documents, playing under other people's identity to avoid the repercussions from terrible losses.

Perhaps one of the most damaging forms of fraud for online gambling is multiple account fraud, where users create fake accounts to play and violate the company's bonus policy.

The procedure forms must be an integral mechanism for protecting the company from malicious actors and financial crime as well as ensuring that the company is complying with AML regulations.

In order to effectively meet counter the abovementioned issues, the company has implemented an Identification and Account Verification processes for all of the users/customers in order to ensure and confirm that the details of the users and customers registered are accurate and correspond to the particular individual and also to confirm that the payment details and methods used are not stolen or used by someone else, which is to create the general framework for the fight against money laundering and financing terrorism.

Formal Identification of users and customers on registration and entry into commercial relations is a mandatory requirement for increasing security and protection against fraud.

The Company requires this procedure as it forms part and parcel of gambling responsibly along with fraud and financial crime prevention and required by the codes.

Upon the registration of a new account, the company collects the personal details of the customer, third party declaration, acceptance of the Terms and Conditions of the company's site(s) and confirmation that the person is above 18 years old. Additionally, if a person enters date of birth which shows they are underage, the registration cannot be completed.

Information requested on registration includes:

- Full Name
 - Date of Brith
 - Residential
- Address

5.4.2 Identity Verification Process

At latest, upon reaching the Naf 4,000 threshold, every customer will need to verify his/her personal details such as name, address, age, country.

When the account is created, full Identity verification must be performed, and the following details need to be confirmed with documents:

- Full Name as it appears on the passport (photo and cover page), driver's license, or national ID card.
- Nationality as it appears on the passport or national ID card
- Gender
- Date of Birth
- Full Address - recent utility bill, bank statement or council tax bill (not less than 6 months)

Payment Method – scan of the front and back of the card used to fund the player bank account, e-wallet or bank statement.

Full ID verification/re-verification will also be required in the following circumstances:

- When a user deposits to withdraw above the nominated threshold which is set to Naf 4,000. This can be either one withdrawal, or cumulatively.
- If the address of a user's first deposit method does not match the address used when registering the account.
- If there is a change in the pattern of deposits or withdrawals.
- When a name matches or is similar to that of someone with a history of criminal activity or a PEP.

Source of Payment Verification/Proof of Payment:

- Company account registered Credit or Debit card
- Copy of Credit or Debit card account statement of a card registered on with Company account (less than 3 months old)
- Copy of bank statement - must have Company transaction or card number visible on it (less than 3 months old)

Source of Funds/Wealth consisting of the following:

- Payslips
- Employment Contracts
- Proof of Deposits
- Bank Statements
- Inheritance Confirmations/Wills
- Deed of Donation

Other Identification and Verifications:

- Biometric checks (liveness);
- Selfie/Declaration with ID document;
- Bank Statement;
- Bank Card;
- E-wallets.

The KYC, Finance or Risk&Fraud departments may require additional checks if deemed necessary based on the situation. When requesting such documentation, the customer must always be informed that:

- The card number must be blanked out leaving only the first six and last four digits visible together with the start and expiry date.
- The documents must be clear and legible.
- The documents should show the residential address, name and date of issue.
- Scans should preferably be in PDF, JPEG, BMP, WORD or GIF file formats only with a maximum size of 5MB per page.

Account verification is a required part of the onboarding process and may vary in duration depending on individual circumstances. However, in line with applicable codes, verification must be completed within 30 days from the moment the cumulative transaction value reaches the equivalent of Naf. 4,000. Failure to provide the necessary documentation within this timeframe may result in account restrictions, termination of the business relationship, or further action in accordance with the Policy.

5.4.3 Enhanced Due Diligence (EDD)

In certain cases, there is the possibility certain customer relationships and large transactions demonstrate higher ML/TF or fraud risks to the Company. In such instances and in addition to its regular customer due diligence procedures, the Company shall carry out Enhanced Due Diligence ("EDD") for further risk investigation.

Risky customers and transactions pose a greater ML/TF risk and Customer Due Diligence ("CDD") procedures won't suffice to mitigate exposed risk by high risk users. In this case, EDD procedures will be applied in order to

create a higher identity assurance by taking the customer identity and addressing and evaluating the customer's risk category.

During the enhanced due diligence process, the Company will take additional required steps in order to aid the identification of a potential customer, including (but not limited to) personal and financial background. This may involve obtaining additional steps in verifying the individual in question. This may include obtaining evidence to verify particular aspects of the customer's identity and verified confirmation in order to establish the source of funds of the customer.

The Company's Fraud Department will have access to a variety of tools through suppliers and databases which are used to verify submitted documentation (e.g. Drivers Licenses, and Passports).

The circumstances that may trigger additional concern and may require Enhanced Due Diligence (EDD) are noted below:

- The customer or potential customer is situated in a country of territory that does not apply to the Company's geographical market.
- The customer or potential customer is situated in a country blacklisted or a country supporting terrorist activities.
- The customer or potential customer is or appears to be a Politically Exposed Person or close spouse or family member (outlined below).
- Any other circumstances as the Company reasonably perceives to be a High Risk of Money Laundering or Terrorist Financing.

Under the above circumstances different documents may be requested from the Customer as well as third party sources for Enhanced Due Diligence purposes.

The company associates solely with trusted and approved Providers and Partners whom all have effective AML policies in place as to prevent the large majority of suspicious deposits from taking place without proper execution of KYC procedures onto the potential customer.

Figure 2. Due Diligence Matrix

Source of Wealth (corroborated)				X
Certified evidence of identity/Picture with passport/Certified by VIP manager				X
3 rd Party Background Check (case by case basis)				X
Source of Wealth			X	X
Evidence of Identity (Photo ID + Proof of Address + Funding Method)		X	X	X
Identification of users and automatic/Manual ID verification (where the 3 rd party IDV tool available)	X	X	X	X
PEP & Sanction Screening	X	X	X	X
	Low	Medium	High	PEPs

5.5 Ongoing Monitoring

Ongoing monitoring is one of the methods used for risk assessment of existing or potential customers of organizations under the AML obligation.

During the customer's journey, automated and/or manual screenings will be conducted to identify potentially linked or other suspect account activities compared to the customer profile. The main purpose of the company is to control their existing and potential customers in sanctions, PEP, banned lists, wanted lists, and adverse media data to obstruct false positives and false negatives by classifying their customers according to their risk levels and also for the company to be protected from regulatory penalties as well as to avoid violating various sanctions.

As customer risk levels may change over time, the Company conducts regular screenings to reassess and update the risk classification of existing customers accordingly. Monitoring frequency is determined based on the assigned risk level to ensure an appropriate and proportionate level of oversight. The review intervals are as follows:

- Low Risk: Every three (3) years
- Medium Risk: Every two (2) years
- High Risk: Every year or upon any transaction alerts
- High Risk – Enhanced: Monthly or upon any transaction alerts

This risk-based review cycle ensures that the Company adapts its customer due diligence measures in line with evolving risk profiles and maintains compliance with Curaçao AML/CFT regulations.

The company will be maintaining an updated record of customers by performing online verification on them. All AML procedures, policies and controls are regularly reviewed and updated to ensure that they take into consideration new risks that may arise.

Such screening searches for potentially suspect elements, include the following,

- Accounts that may depict similar information;
- Two or more accounts utilizing the same email address upon creation;
- Customer has more than one account;
- Customer who originates income from High Risk or Sanctioned countries
- Any other suspicious information / activity identified or suspected by the Fraud or Financial Services teams.

In the event that any of the above screenings identify potential issues, the Risk and Fraud team will be automatically notified. Upon notification, the team will investigate the matter and determine the appropriate course of action in accordance with internal business rules and regulatory obligations. Depending on the outcome, potential risk mitigation measures may include account closure, escalation for enhanced due diligence, restrictions on deposit or withdrawal methods, imposition of transactional limits, or notification/report to the MLRO for further review.

5.6 Reliance on Third Parties for Customer Due Diligence

Novi B.V may rely on third parties to carry out certain aspects of the Customer Due Diligence (CDD), Enhanced Due Diligence (CDD) or PEP/Sanction screening processes, such as customer identification, verification, name screening and obtaining information on the purpose and intended nature of the business relationship. While doing so, the Company remains fully responsible for ensuring that all CDD obligations are properly fulfilled.

When relying on a third party, the Company ensures:

- It has immediate access to the CDD information and documents collected by the third party;
- A written agreement is in place that guarantees all identification data and supporting documentation will be provided without delay upon request;
- The third party is subject to appropriate AML/CFT supervision and operates under obligations equivalent to those of Novi B.V;

The Company uses Sumsb to facilitate the collection and review of CDD/EDD documentation or watchlist screenings. All verifications are reviewed by KYC officers to ensure compliance with internal standards and regulatory expectations.

5.7 Reporting Unusual Transactions

Where the Company identifies an activity or facts whose characteristics refer to the use of criminal proceeds or terrorist financing or other criminal offences or an attempt thereof or with regard to which the Company suspects or knows that it constitutes money laundering or terrorist financing or the commission of another criminal offence, MLRO of the Company must be informed within 24 hours. MLRO should investigate the transaction maximum of 10 business days, and report to FIU immediately, but not later than within two working days (48 hours) after identifying the activity or facts or after getting the suspicion.

The Company and all its employees, officers and directors are prohibited to inform a person, its beneficial owner, representative or third party about a report submitted on them to the FIU, or an intention to submit such a report as well as about the commencement of criminal proceedings.

The following transactions or intended transactions are deemed unusual:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- 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 (N.G. 2014 no. 55);
- Transactions in the amount of Naf. 5,000 or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:

Examples of situations that may be possibly related to ML or TF:

- Setting up multiple betting accounts, with deposits well below reporting threshold to withdraw the money after a short while;
- Regularly depositing or transacting similar amount of cash;
- Funding casino account with prepaid cards, checks and cryptocurrency and then ask for pay out without gameplay;
- Unexplained income inconsistent with financial situation/customer profile;
- User provides source of wealth that income was generated in non-reputable countries.
- Association with multiple accounts under multiple names;
- Frequent betting transactions just under threshold;
- Placing safe bets;
- Chargebacks;
- Betting against associates/Intentional losses, where money launderers deliberately lose to one of the parties who is able to receive a casino issued check or wire transfer of legitimate winnings;
- Wire transfers /currency exchanges just under threshold.

If the Company believes that there is some degree of suspiciousness after a transaction has taken place and after an internal investigation confirms as such - the Company will freeze the account and will inform the relevant authorities immediately and disclose all the necessary information at the company's possession required by law to do so. The MLRO or an authorized staff will report the activity through the reporting form (Appendix C) and submit it to the FIU.

Additional reporting procedures are put in place in order to mitigate the Company's exposure to various forms of money laundering and sanctions. These consist of in-house and third-party reporting/monitoring tools that run daily and weekly. Furthermore, AML reporting procedures such as Suspicious Transaction Reporting ("STRs") will be conducted and submitted when necessary to the Regulators and also to the appropriate law enforcements should this be required.

A STR should include the following details:

- personal particulars (name, identity card or passport number, date of birth, address, telephone number, bank account number) of the person(s) or company involved in the suspicious transaction;
- details of the suspicious financial activity;
- the reason why the transaction is suspicious - which suspicious activity indicators are present?
- the explanation, if any, given by the person about the transaction

Employees are strictly prohibited from informing a customer or third party that a suspicious transaction report (STR) has been or will be submitted to the FIU. Any violation of this prohibition will be treated as a serious disciplinary breach and may result in termination and potential legal consequences.

5.8 Anti-Money Laundering Compliance Program

Novi B.V has implemented a comprehensive Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) Compliance Program designed to prevent the misuse of its operations for money laundering, terrorism financing, or other forms of financial crime. The program is based on a risk-based approach and complies with the standards set forth under the code, including the National Ordinance on the Reporting of Unusual Transactions, the Sanctions National Ordinance, and applicable guidance issued by the Gaming Control Board and the Financial Intelligence Unit (FIU).

The AML program includes, but is not limited to, the following core components:

- A documented Business Risk Assessment (BRA) to identify and assess ML/TF risks specific to the Company's operations;
- A Customer Risk Assessment (CRA) framework to determine appropriate levels of due diligence based on customer risk profiles;
- Ongoing Know Your Customer (KYC) procedures, including identity verification, enhanced due diligence for high-risk customers, and continuous monitoring;
- Policies and procedures for the identification, review, escalation, and reporting of unusual or suspicious transactions;
- Robust sanctions screening protocols to ensure compliance with local and international sanctions regimes;
- Clearly defined internal escalation procedures and controls, including account restrictions, transaction limits, or blocking of accounts in cases of suspected ML/TF;
- Regular training programs for relevant members to ensure ongoing awareness of AML/CFT responsibilities;
- Oversight by a designated MLRO, who are responsible for the effective implementation, maintenance, and supervision of the AML/CFT framework;
- Maintenance of appropriate records and audit trails in accordance with legal data retention and reporting obligations.

The AML program is subject to periodic review and is updated as necessary to reflect regulatory changes, business developments, and emerging ML/TF risks. It is formally reviewed at least annually to ensure continued effectiveness and compliance with applicable legal requirements. The Company will ensure that appropriate procedures are in place to support the implementation of this Policy, in full compliance with applicable regulations, as well as relevant directives and recommendations issued by international authorities and standard-setting bodies. The Company will also monitor adherence to these procedures on an ongoing basis.

The objectives of this and related policies are:

- Ensuring the Company is compliant with all applicable laws, statutory instruments of regulation;
- Protecting the Company and its staff as individuals from the risks associated with breaches of the law, sanctions, regulations and supervisory requirements;
- Preserving and protecting the Company's reputation against the risk of reputational damage presented by implication in money laundering and terrorist financing activities;
- Making a positive contribution to the fight against crime and terrorism.
- Screening and Monitoring
- AML screening is performed to fulfil three main objectives.
- Establishing an Accurate Risk Assessment
- Avoid violating Sanctions
- Protect the company and its stakeholders from Regulatory Fines

5.8.1 Money Laundering Reporting Officer ("MLRO")

The management board of the Company shall maintain with the company a Compliance Officer, who acts as a contact person with Regulators and performs AML/CTF duties and obligations of the Company. A MLRO reports directly to the management board and has the competence, means and access to relevant information across all the structural units of the Company.

Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties listed below may be appointed as a MLRO.

MLRO contact details:

Email: mlro.curacao@cityuk.email

The MLRO holds no other position within the organization or any affiliated company or supplier and operates independently from all other functions within the organization to ensure that actual or perceived conflicts of interest do not occur.

Subject to oversight by the Board, the MLRO has the authority to act independently from other functions within the organization to fulfil the below noted roles and responsibilities. The MLRO has the full and public support of the executive management team in executing his duties. All staff are required to assist the MLRO in fulfilling the role duties.

5.8.2 Duties and Responsibilities of the MLRO

The Money Laundering Officer is in charge of financial regulations and personal data compliance requirements, making sure the company's AML policy corresponds to the international system. Furthermore, the MLRO is responsible for oversight and management of all compliance related functions within the Company and within its affected suppliers, including the protocols described in this Policy.

MLRO duties include (but not limited to) the following:

- Ensure that procedures are in place to ensure compliance with all applicable legislation, regulations and all associated guidelines, codes of practice and Company policies and procedures;
- Report to the CEO and inform Senior Management the result(s) of any corrective action taken;
- Attend regular Compliance Meetings with selected Senior Management, prepare an agenda therefor, and to take, circulate and maintain the minutes thereof;
- Update and maintain any compliance-related policies, including this AML Policy;
- Plan and co-ordinate training activity for all departments to include key regulatory areas including the significance of regulatory compliance as a whole, ID and age verification, fraud, anti-money laundering, and problem gambling;
- Be the point of contact with the involved Regulator(s);
- Investigate and report any breaches of the applicable laws, regulations, guidelines, codes of practice and company policies and procedures to Senior Management and, as appropriate, to the Regulator;
- Consult with staff representatives and attend staff meetings on compliance topics;
- Manage regular reviews of Company's internal control system to ensure that it accurately reflects the then current operation of the business – and report any discrepancies/oddities to relevant senior management.
- Look after records of high-risk clients and report suspicious activities, if any.
- Assist with the implementation of the Anti-Money Laundering policy.
- Arrange for inspections from third-party organizations and eliminate mistakes in the program, if any.

5.8.3 Ongoing Training and Development

The MLRO shall ensure that Company's employees are fully aware of their legal obligations under the AML/CTF regime, by introducing a complete employees' education and training program. All employees in sensitive functions, including KYC, Risk, Finance, and Compliance, will be subject to background screening at the time of hiring.

The timing and content of the training provided is determined according to the needs of the Company. The frequency of the training can vary depending on the amendments of legal and/or regulatory requirements,

employees' duties as well as any other changes in the business model. The training program aims at educating the Company's employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose.

The MLRO will supply the appropriate AML training (which may consist of in-class, video conference, literature, and seminars) in order to provide the involved staff, update on the guidelines and direction on:

- The process in reporting suspicious activity;
- Risk Management practices;
- Identification and Verification Procedures;
- Suspicious transaction identification and reporting;
- Record Keeping;
- The type of activity that should be considered significant and critical in detecting possible money laundering – these may be given in reading materials;
- Distinguishing specific incidences that may require cause for re-assessment of a risk-based approach;
- The Company consistently implements monitoring processes with the addition of potentially new and future products and/or services it provides to its customers;

Implementations and assessments are put in place (and adjusted if required) in order to mitigate any possible risk of money laundering or terrorist financing where the use of new products and/or services may be vulnerable to. These include but not limited to the following,

- Analysis of transactions over specific periods;
- Analysis of new services/products used by the customer;
- Applying limits to activities on new products/services used by the customer for a given time;
- Requests for justification of noticeable irregular activity from the customer.

5.8.4 Management of Policy

The Company is committed to regularly monitoring its AML/CFT compliance program to ensure alignment with all applicable legal and regulatory requirements. This Policy will be reviewed at least annually, and revised as necessary to reflect changes in codes or the Company's products and services.

The effectiveness of the Company's AML/CFT program is regularly evaluated to ensure it remains current and is aligned with business activities, regulatory developments, industry standards and best practices. By doing so, the Company adheres to all applicable laws and regulatory requirements in the jurisdictions in which it operates.

5.8.5 Data Retention

The Company must retain the documents and information which served for identification and verification of clients, no less than 5 (five) years after termination of the business relationship.

The Company is allowed to process personal data gathered upon registration of an account with our company only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

5.8.6 Cooperation and Exchange of Information

The Company cooperates with supervisory and law enforcement authorities in preventing money laundering and terrorist financing, thereby communicating information available to the Company and replying to queries within a reasonable time, following the duties, obligations and restrictions arising from legislation.

6. Compliance and Consequences of Non-Compliance

Novi B.V. is committed to full compliance with all applicable anti-money laundering and counter-terrorist financing obligations under the codes. Compliance with this AML/CFT Policy is mandatory for all employees, management, and third-party service providers engaged with the Company.

Failure to comply with the obligations set out in this Policy—whether through negligence, deliberate misconduct, or lack of awareness—may result in serious consequences for both the Company and the individuals involved. These may include:

- Regulatory sanctions or administrative penalties issued by the Gaming Control Board (GCB) or other competent authorities;
- Suspension or revocation of the Company's gaming license under the LOK;
- Reputational damage and increased regulatory scrutiny;
- Criminal liability, including fines or imprisonment, as provided under applicable legislation.

The Company has established internal monitoring and audit mechanisms to ensure ongoing compliance. Any breaches, suspected breaches, or non-adherence to AML/CFT obligations must be reported immediately to the MLRO for investigation and resolution. Staff and relevant third parties are required to cooperate fully in such investigations and to follow escalation protocols as outlined in this Policy.

7. Related Information

7.1 High Risk Countries

- ALBANIA
- ALGERIA
- ANGOLA
- ANGUILLA
- ANTIGUA
- ARMENIA
- ARUBA
- AZERBAIJAN
- BAHAMAS
- BAHRAIN
- BANGLADESH
- BELIZE
- BENIN
- BERMUDA
- BOLIVIA
- BOSNIA HERZEGOVINA
- BOTSWANA
- BRITISH VIRGIN ISLANDS
- BULGARIA
- BURUNDI
- CAMBODIA
- CABO VERDE ISLANDS
- CENTRAL AFRICAN REPUBLIC
- CHAD
- CHINA
- COLOMBIA
- COMMONWEALTH OF DOMINICA
- COMOROS
- CONGO
- COOK ISLANDS
- COTE D'IVOIRE
- CROATIA

- DJIBOUTI
- DOMINICA
- DOMINICAN REPUBLIC
- ECUADOR
- EGYPT
- EL SALVADOR
- EQUATORIAL GUINEA
- ERITREA
- ETHIOPIA
- FIJI ISLANDS
- GABON
- GAMBIA
- GHANA
- GRENADA
- GUERNSEY
- GUAM
- GUINEA
- GUYANA
- HONDURAS
- INDONESIA
- ISLE OF MAN
- KAZAKSTAN
- KENYA
- KIRIBATI
- KOREA SOUTH
- KOSOVO
- KYRGYZSTAN
- LAOS
- LEBANON
- LESOTHO
- LIBERIA
- LIBYA
- MACAU
- MALAWI
- MALAYSIA
- MALDIVES
- MARSHALL ISLANDS
- MAURITANIA
- MAURITIUS
- MOLDOVA
- MONGOLIA
- MONTENEGRO
- MICRONESIA
- MONACO
- MOROCCO

- NAURU
- OMAN
- PAKISTAN
- PAPUA NEW GUINEA
- PARAGUAY
- PUERTO RICO
- REPUBLIC OF AZERBAIJAN
- REPUBLIC OF GUATEMALA
- REPUBLIC OF GUINEA-BISSAU
- REPUBLIC OF MOZAMBIQUE
- RUSSIA
- RWANDA
- SAO TOME & PRINCIPE
- SAINT LUCIA
- SAMOA
- SAUDI ARABIA
- SERBIA
- SIERRA LEONE
- SOLOMON ISLANDS
- SOMALIA
- SRI LANKA
- ST VINCENT & THE GRENADINES
- ST. KITTS AND NEVIS
- SINT MAARTEN
- SURINAME
- SUDAN
- SWAZILAND
- TAIWAN
- THAILAND
- TOGO
- TUNISIA
- TUVALU
- TURKMENISTAN
- TURKS AND CAICOS ISLANDS
- UKRAINE
- URUGUAY
- US VIRGIN ISLANDS
- VENEZUELA
- WEST BANK
- ZAMBIA
- ZIMBABWE

7.2 Non Serviced Countries (FATF & CFATF & International Sanctions)

- AFGHANISTAN
- BELARUS
- BURKINA FASO
- CAMEROON
- CENTRAL AFRICAN REP
- CONGO, THE DEMOCRATIC REPUBLIC
- CUBA
- GAZA STRIP
- GUATEMALA
- GUYANA
- HAITI
- HONDURAS
- HONG KONG
- IRAN, ISLAMIC REPUBLIC OF - **BLACKLIST**
- IRAQ
- ISRAEL
- KENYA
- LIBYA
- MALI
- MOZAMBIQUE
- MYANMAR - BLACKLIST
- NAMIBIA
- NICARAGUA
- NIGER
- NIGERIA
- NORTH KOREA - **BLACKLIST**
- NORTH MARIANA ISLANDS (USA)
- PAKISTAN
- PHILIPPINES
- RUSSIAN FEDERATION
- SENEGAL
- SOMALIA
- SOUTH AFRICA
- SOUTH SUDAN
- ST MAARTEN
- SUDAN
- SYRIA
- TANZANIA
- TRINIDAD & TOBAGO
- TUNISIA
- UGANDA
- UKRANIE
- VATICAN CITY STATE (HOLY SEE)

- VENEZUELA
- VIETNAM
- WEST BANK (PALESTINIAN TERRITORY)
- YEMEN
- ZIMBABWE

7.3 Suspicious Transaction Report

SUSPICIOUS TRANSACTIONS/ACTIVITY REPORT

Report Prepared by:		Date of Report:	
Team/Department:			
Customer Name:			
Username:		Date of Birth:	
Brand:			
Address:			
Postcode:			
Email Address:			
Telephone Number:			
Current Balance:			
No. of Deposits:		Total Amount of Deposits:	
Deposit Methods Used:			
No. of Withdrawals:		Total Amount of Withdrawals:	
Account Status:	Open (Y/N)	Closed (Y/N)	Suspended (Y/N) Self-Excluded (Y/N)
KYC (Know Your Customer - CDD) Status:			
EDD (Enhanced Due Diligence) Status:			

Reason for Suspicion:	
Please provide a full description outlining:	

Beware of tipping off: do not tell the client or anyone else that you have made this report. You will receive a receipt for your report within 48 hours of submission – remember to ask for your receipt if you do not receive it within this timeframe.

Receipt of the Report Acknowledged:	
Signed, Compliance Officer/MLRO	
Date:	

MLRO INTERNAL RESPONSE

1. OBSERVATIONS:
2. AML PROCEDURES:
3. SUGGESTIONS:
4. Submission STR / SAR:

7.4

Abbreviations

Abbreviation	Meaning
AML	Anti-Money Laundering
CFT	Countering the Financing of Terrorism
ML	Money Laundering
TF	Terrorist Financing
PF	Proliferation Financing
KYC	Know Your Customer
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
SDD	Simplified Due Diligence
CRA	Customer Risk Assessment
BRA	Business Risk Assessment
CAP	Customer Acceptance Policy
MLRO	Money Laundering Reporting Officer
FIU	Financial Intelligence Unit (MOT Curaçao)
STR	Suspicious Transaction Report

PEP	Politically Exposed Person
FATF	Financial Action Task Force
OFAC	Office of Foreign Assets Control (U.S.)
OFSI	Office of Financial Sanctions Implementation (UK)
NRA	National Risk Assessment
SOP	Standard Operating Procedure
NOIS	National Ordinance on Identification when Rendering Services
NORUT	National Ordinance on the Reporting of Unusual Transactions
GCB	Gaming Control Board (Curaçao)
LOK	National Ordinance on Games of Chance (Landsverordening op de kansspelen)

8. Contact Information

For any questions, concerns, or reports related to this Policy, employees and relevant third parties may contact the company. All communications will be handled confidentially and in accordance with applicable data protection and regulatory requirements.

Contact details:

Name:

Email:

Phone:

9. Version History

Version	Description	Date	Initials
1.0	Annual Revision	01.07.2022	CO
2.0	Annual Revision	01.07.2023	CO
3.0	Annual Revision	01.08.2024	CO
3.1	Policy Amendments	01.01.2025	CO

*****End of Document*****