

AML/CTF Policy

Winna B.V.

Key Information

Approving Official(s):

Senior administrator(s) responsible for approving the policy.

Responsible Office:

Office responsible for policy dissemination, updates, and reviews.

Effective Date:

Month, day, and year the policy (or revision) takes effect.

Next Review Date:

Month, day, and year for the initial or next scheduled review. New policies or major revisions should be reviewed within one year; subsequent reviews should occur at least once every three years.

1. Policy Statement

This policy sets out Winna B.V.'s commitment to actively prevent and take measures to guard against being used as a medium for money laundering activities, terrorism financing activities, criminal activities and any other activity of a similar nature.

To these ends:

- The identities of all new and existing users will be verified to a reasonable level of certainty;
- A risk-based approach will be taken to the monitoring of user transactions and activities; and
- Any suspicious activity will be reported, and all AML activities recorded.

We do not condone and have a zero-tolerance approach to the process of taking profits from crime and corruption and transforming them into legitimate assets and are committed to minimise our risks in relation to money laundering.

2. Purpose

The purpose of this policy is to ensure that Winna B.V. complies with the Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), and proliferation financing requirements applicable to the gaming sector under the jurisdiction of Curaçao.

As of February 15, 2019, the Curaçao Gaming Control Board (GCB) was officially appointed as the designated supervisory authority responsible for overseeing AML/CFT compliance for the entire gaming industry, with its authority retroactively effective from January 1, 2016. The GCB is tasked with ensuring that all license holders

implement effective measures to prevent the use of their operations for money laundering, terrorist financing, or the proliferation of weapons of mass destruction.

This policy outlines the internal controls, procedures, and responsibilities adopted by Winna B.V. to meet its legal obligations under the following key laws and regulations:

- National Ordinance on the Identification when Rendering Services (NOIS)
- National Ordinance on the Reporting of Unusual Transactions (NORUT)
- Sanctions National Ordinance
- Kingdom Sanction Act
- Regulations issued by the GCB effective January 9, 2025, with mandatory compliance by April 10, 2025

Additionally, this policy reflects international standards as set out by the Financial Action Task Force (FATF) and its regional body, the Caribbean Financial Action Task Force (CFATF), of which Curaçao is a member. These standards form the global framework for combating financial crime.

By implementing this policy, Winna B.V. demonstrates its commitment to:

- Preventing its operations from being used to launder criminal proceeds
- Detecting and reporting unusual or suspicious transactions
- Complying with national and international sanctions
- Establishing a strong culture of compliance and ethical business conduct

This policy forms an integral part of Winna B.V.'s licensing obligations and risk management framework and applies to all employees, management, and relevant third parties.

3. Audience

This policy applies to all employees of Winna B.V., as well as contractors, consultants and any third-party suppliers or service providers who may be involved in activities that fall within the scope of this policy. All relevant stakeholders are required to comply with the principles and procedures set out in this document.

4. Definitions

For the purposes of this policy:

Casino: in these Regulations includes both land-based and online casinos.

Anti-Money Laundering (AML): measures, controls and procedures to prevent and detect money

laundering and terrorist financing.

Know Your Customer (KYC): the process of verifying the identify of a customer to ensure they are who they claim to be, forming part of CDD.

Money Laundering (ML): the process through which the proceeds of crime are processed and converted into assets that appear to have a legitimate origin.

The Caribbean Financial Action Taskforce (CFATF): an organization of twenty-four states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.

Financing of Terrorism (FT): the financing of terrorist acts, of terrorists and terrorist organizations.

Financing of proliferation of weapons: the provision of funds 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.

Customer Due Diligence (CDD): the process of identifying and verifying the identify of customers.

Enhanced Due Diligence (EDD): additional checks applied to higher-risk customers, such as Politically Exposed Persons (PEPs).

Politically Exposed Persons (PEP): an individual who holds, or has held, a prominent public position or function, including their immediate family members and close associates, and who may present a higher risk of involvement in bribery, corruption, or money laundering

Sanctions Screening: the process of checking customers and their transactions against international and national sanctions list to ensure that the company does not engage with prohibited individuals, entities, or countries.

Suspicious Activity Report (SAR): a report submitted internally or to a competent authority when a suspicious transaction or behaviour is detected.

AML Compliance Officer: the designated person responsible for implementing and overseeing all anti-money laundering measures within Winna B.V.

Source of funds: refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.

Source of wealth: the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.

5. Policy Implementation

The AML policy will be implemented through:

- Governance: oversight by the AML Compliance Officer, who is responsible for monitoring, reporting, and ensuring compliance.
- Procedures: customer identification (KYC), risk assessments, monitoring of transactions, reporting of suspicious activity, record keeping, and staff training.
- Risk management measures: including Customer Acceptance Policies (CAP), Customer Risk Assessment (CRA) procedures, internal control, compliance management and communication of such policies, procedures and controls, employee training and employee screening policies and procedures.

These measures will be clearly documented and approved by Winna B.V.'s board of directors. Winna B.V. will monitor the implementation of these controls and enhance them if necessary to manage and mitigate the risks where higher risks are identified.

5.1 Business Risk Assessment

Winna B.V. has a nominated officer, the AML Compliance Officer, who is responsible of conducting risk assessments and reviewing disclosures in respect of suspected transactions or activities on our platform www.winnables.com.

Our risk report assesses money laundering risks in terms of the risk-level of the user, their activities, and transactions on our platform, and are made by the AML Compliance Officer.

In accordance with the regulations issued by the Curaçao Gaming Control Board (GCB), effective January 9, 2025, and based on the requirements set forth in the National Ordinance on the Identification when Rendering Services (NOIS), the National Ordinance on Reporting of Unusual Transactions (NORUT), and other applicable sanctions legislation, Winna B.V. is required to conduct a formal Business Risk Assessment (BRA).

This BRA is designed to identify, understand, and mitigate the inherent and residual risks of Money Laundering (ML), Terrorist Financing (TF), and the Financing of the Proliferation of Weapons of Mass Destruction (PF).

The risk assessment must address the ways in which Winna B.V.'s platform could be used to launder money, finance terrorism, or finance proliferation, and evaluate the extent of those risks. All relevant risk factors must be considered, including customer types, products and services, delivery channels, and geographic factors. Winna B.V. also integrates outcomes and recommendations from the National Risk Assessment into its BRA. Once the business risk is assessed, Winna B.V. sets a risk appetite to determine the level of risk it is prepared to accept, which guides the structure of its AML compliance program. The BRA is documented, approved by the Board of

Directors, and made available to the GCB upon request. It includes the risk assessment methodology, justification for assigned risk levels (low, medium, high), the outcome of the BRA, and sources of information used. Winna B.V. also remains up to date with developments in ML and TF trends to ensure a risk-based approach.

The Business Risk Assessment considers the following factors, in line with GCB guidance and FATF Recommendations:

- The nature and behaviour of our customers (customer risk);
- The products and services offered, including online raffles and promotional mechanics (product/service risk);
- The delivery channels used (e.g., remote, online, mobile platforms) (delivery channel risk);
- The geographic locations of users and transactions, particularly involving high-risk jurisdictions (geographic risk).

The methodology used to assess these risks assigns a risk level (low, medium, or high) and is based on internal transaction data, FATF typologies, and relevant information from the National Risk Assessment of Curaçao.

This includes, but is not limited to:

1. **Collusion:** working together with another player to gain an unfair advantage over other players or the platform.
2. **Unfair winning:** using unfair methods to increase your chances of winning a raffle, such as using software or devices or influence the random number generator.
3. **Charge-back transactions:** dispute a payment for an online raffle ticket that results in a reversal of payment and a loss for the platform.
4. **Advantage Play:** using unethical methods to gain an edge over the platform or other players. For example, using stolen cards, creating more than one account, providing incorrect registration data, or forged document to purchase online raffle tickets or claim prizes. *Any player who tries to gain advantage of welcome offers or other promotions agrees that we reserve the right to void bonuses and any winnings from such bonuses.*
5. **Bankruptcy:** declare bankruptcy in your country of residence after purchasing online raffle tickets or claiming prizes.
6. Any fraudulent actions against other online casinos or payment providers.

If any of the above actions are undertaken, we reserve the right to terminate such user's account and suspend and/or cancel all pay-outs to the user.

In the event of a chargeback, we reserve the right to;

1. Recover any losses or damages that were suffered as a result of the chargeback by charging the user a sum equivalent to the user's available balance funds;
2. Claim further damages and financial losses from the user by contacting them via one of the methods provided during the registration process (i.e., phone or e-mail); and
3. Terminate the user's account and access to the platform.

We will not be required to disclose to the user the reasons for closing their account and will inform the relevant regulatory bodies of their actions.

5.2 Customer Risk Assessment

Winna B.V. will carry out a Customer Risk Assessment (CRA) when establishing a business relationship. The CRA evaluates the particular risks the company may be exposed to when providing its services. The information collected will be used to determine the customer's overall risk profile and the appropriate level of due diligence required.

The customer-specific risk assessment must be conducted either prior to executing an occasional transaction or at the time of establishing the business relationship. This initial assessment may need to be revised later if new risks emerge or circumstances change during the course of the relationship.

Based on the outcome of the CRA, Winna B.V. will apply the appropriate level of Customer Due Diligence (CDD) measures in accordance with its Customer Acceptance Policy (CAP).

To support this, Winna B.V. has adopted a Customer Acceptance Policy that outlines:

- The types of customers who are likely to pose higher-than-average risks of Money Laundering (ML), Terrorist Financing (TF), or Financing of Proliferation (PF);
- The risk indicators used to categorize customers as low, medium, or high risk;
- The level of CDD measures, including enhanced due diligence and ongoing monitoring, to be applied for each risk level;
- The circumstances under which services will be denied or terminated.

When developing and applying the CAP, Winna B.V. ensures compliance with its obligations related to Politically Exposed Persons (PEPs) and sanctions screening, as required by applicable AML/CFT legislation.

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

1. 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 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); 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 and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
 - Customers using multiple casino player rating accounts to hinder a casino to track their gambling activities;
 - Unknown customers (redeeming large amounts of chips);
 - Junkets (junket operators monitor player activity and issues and collect credit)
2. Geographical risk - the risk posed to the casino by the geographical location of the player and the source of wealth of the business relationship. The nationality, residence and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk.

It is advisable to take into account a variety of sources of information produced by the FATF and well-known non-governmental well-known bodies.

Some sources to use are:

- Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action
- Countries on the FATF list of Jurisdictions under Increased Monitoring
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of ;
12 their AML/CFT regime
- Countries sanctioned by the OFAC
- Countries identified by credible sources as providing funding or support for terrorist activities or having terrorist organizations operating within them
- Countries on the Corruption Perception Index compiled by Transparency International.

Winna B.V. has a list of countries that are considered high risk and those that are considered low risk.

3. 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.
4. Distribution channels risk - the channels through which a casino 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
 - While situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes unless the casino adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations
 - Where there is the involvement of a third party in the interactions between the customer and the casino, 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.

Technological developments risk assessment – Winna B.V maintains appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism.

It identifies and assesses the money laundering or terrorist financing risks that may arise whenever:

- A new product is developed
- A new business practice emerges
- A new delivery mechanism becomes available
- A new or developing technology is used for both new and pre-existing products.

In those cases, a risk assessment takes place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism. Such risk assessments are documented. Where risks are identified, measures are taken to mitigate these risks.

5.3 Customer Acceptance Policy

Based on the outcome of the CRA, Winna B.V. applies its Customer Acceptance Policy (CAP) to decide whether to proceed with the relationship. Customers identified as higher-risk may be subject to Enhanced Due Diligence. The CAP also requires compliance with obligations related to Politically Exposed Persons (PEPs) and Sanctions Screening. The AML Compliance Officer monitors and screens users against sanction lists by using a variety of databases, including the Office of Foreign National Control (OFAC) sanctions list screening software and global regulatory databases.

5.4 Customer Due diligence

Winna B.V. is prohibited from maintaining anonymous or fictitious player accounts and must identify all players engaging in financial activity. The establishment and maintenance of a business relationship or occasional transaction requires sufficient knowledge of the player's identity, the nature of the relationship, and an appropriate Customer Risk Assessment (CRA).

Customer Due Diligence (CDD) measures must be applied in the following cases:

- When a player conducts a transaction of NAf. 4,000 or more;
- When multiple linked transactions cumulatively exceed NAf. 4,000;
- When there is suspicion of money laundering (ML) or terrorist financing (TF); or
- When doubts arise about the validity of previously collected customer identification data.

Timing of CDD Measures

- Winna B.V. establishes business relationships when customers open accounts or join player clubs, implying an ongoing relationship.
- Basic customer information (name, surname, permanent residential address, date of birth) and PEP/sanctions screening must be collected at onboarding.
- Full identity verification is required when a player's financial transactions reach or exceed NAf. 4,000, calculated daily, including deposits, withdrawals, and peer-to-peer transfers.
- Until the NAf. 4,000 threshold is met, customers may continue gaming while CDD is ongoing; however,

deposit and withdrawal restrictions apply once the threshold is reached.

- If requested information or documentation is not received within 30 days of reaching the threshold, we will terminate the relationship and, if suspicion of money laundering or terrorist financing (ML/TF) exists, report to the FIU. Funds should be returned to the original source if no suspicion exists, or blocked according to internal procedures.

CDD measures include:

- Identifying and verifying the player using reliable and independent documents (e.g., government-issued ID, proof of address);
- Identifying the beneficial owner and verifying ownership/control structures where applicable;
- Understanding the purpose and intended nature of the business relationship;
- Conducting ongoing monitoring to ensure activity aligns with the customer's risk profile and source of funds.

Enhanced Due Diligence (EDD) must be applied where a high ML/TF risk is identified.

Winna B.V. must also:

- Perform sanctions and PEP screening using official lists (UN, EU, and local);
- Report suspicious or unusual transactions to the FIU without tipping off the player;
- Ensure physical establishments acting on their behalf adhere to the same AML/CFT standards.

Simplified Due Diligence (SDD)

- SDD may be applied in lower-risk cases, adjusting the extent of identification, verification, and ongoing monitoring accordingly.
- Examples include limiting the collection of detailed information, verifying identity after account establishment, or reducing the frequency of updates and monitoring.
- SDD is not permitted if there is suspicion of ML/TF or in specific higher-risk situations.

Politically Exposed Persons (PEPs)

- Winna B.V. must identify PEPs at onboarding and regularly thereafter.
- Senior management approval is required to establish or continue business relationships with PEPs.
- Source of funds and wealth must be reasonably verified via independent and reliable sources.
- Enhanced ongoing monitoring is mandatory.
- These measures apply equally to family members and close associates of PEPs.

- Failure to implement required measures within 30 days of identifying a PEP necessitates termination of the business relationship.

Application to Existing Customers

- Winna B.V. will apply CDD to existing customers based on materiality and risk.
- Ongoing risk assessments should determine whether current procedures are sufficient or require enhancement.
- If no prior procedures existed, we will perform CDD on existing relationships as soon as reasonably possible.

Termination of Business Relationship

- If customers fail to provide necessary identification or documentation, we will terminate or suspend the account, documenting all efforts made.
- We will assess if delays or refusal to provide information increase ML/TF risk but should not automatically equate reluctance with suspicion.
- If suspicion arises, an unusual transaction report must be submitted to the FIU.
- If no suspicion exists, funds should be returned through the original channels.

Customer risk profiling is critical for transaction monitoring. Information gathered must be proportionate to the level of ML/TF risk. In low-risk cases, a declaration of employment and income may suffice; in high-risk scenarios, independent verification of source of wealth is required. Winna B.V. may also use statistical data and internal behaviour models to support risk assessments, though this method is not suitable for high-risk profiles.

Our platform adheres to these standards by applying CDD and transaction monitoring measures proportionate to the identified risk. Our KYC policy ensures that identity verification is completed for all customers before account registration is finalized. We operate with systems and controls to mitigate financial crime risks in line with international AML regulations.

We have policies and procedures for performing customer due diligence and the transaction monitoring arrangements on a risk-managed basis with systems and controls in place to mitigate any financial crime risks.

Our customer due diligence follows the principles of Know Your Customer (KYC), one of the fundamental precepts of global anti-money laundering regulations.

This due diligence process ensures that identification and verification measures are taken for all customers who register on the platform and participate in our competitions. It ascertains relevant information whereby the

identity of a new user must be established before a registration can be completed. *See our Know Your Customer (KYC) policy to read our KYC components and procedures in more detail.*

5.5 Ongoing Monitoring

The AML Compliance Officer will regularly monitor the following procedures to ensure they are being carried out in accordance with our AML policy and procedures:

1. User identity verification
2. Reporting suspicious transactions and activity
3. Record keeping

In addition to the above, we will conduct ongoing due diligence on all business relationships and continuously monitor transactions to ensure they remain consistent with the customer's known profile and Winna B.V.'s risk appetite. This includes:

- Ongoing monitoring of Identity

We will maintain accurate and up-to-date identification data for all customers. Since identity details may change, we must be able to detect such changes and re-evidence identity as required. This may involve:

- Periodically refreshing identity documents;
- Updating data upon key events (e.g., change of payment method); and
- Monitoring expiry dates of identity documentation.

On a risk-sensitive basis, any significant changes in identification or behaviour may trigger a re-assessment of the customer's risk profile.

- Ongoing monitoring of Transactions

Transactions must be scrutinized on an ongoing basis to detect inconsistencies or unusual activity that may indicate money laundering or terrorist financing (ML/TF). If a customer's transactions deviate from their known behaviour, average transaction profile, or declared source of funds, we will:

- Investigate the reason for deviation;
- Obtain sufficient supporting information and documentation;
- Reassess the customer's risk profile, if warranted;
- Determine whether the transaction qualifies as unusual and needs to be reported to the FIU.

Even in low-risk cases, some level of monitoring is always required to confirm that the customer continues to

qualify as low risk.

All employees must understand this AML policy and consult the AML Compliance Officer if in doubt. Any suspicious activity must be reported directly to the AML Compliance Officer and must not be discussed with the customer involved.

The AML Compliance Officer will continuously monitor legal and regulatory developments and update Winna B.V.'s AML policy and procedures accordingly. All employees are trained on:

- Their legal responsibilities under money laundering legislation;
- Winna B.V.'s due diligence procedures; and
- How to report suspicious activity effectively.

5.6 Reliance on third parties to perform customer due diligence.

Winna B.V. may rely on third parties to carry out certain elements of Customer Due Diligence (CDD), specifically identification, verification, and understanding the nature of the business relationship (elements a–c). This is allowed only if the following conditions are met:

1. Immediate Access to CDD Information

Winna B.V. must obtain the necessary CDD information from the third party immediately upon request.

2. Access to Documentation

There must be a formal agreement in place with the third party to provide copies of identification documents and other CDD records whenever requested. This arrangement must be tested regularly to ensure it works properly.

3. Regulated and Compliant Third Party

The third party must be:

- Regulated, supervised, or monitored for AML/CFT compliance;
- Subject to CDD and record-keeping requirements similar to those applicable to Winna B.V.;
- Applying its own CDD procedures and having an independent business relationship with the customer.

4. Country Risk Assessment

Winna B.V. must consider country risk when deciding whether to rely on a third party based in another jurisdiction.

Even when relying on a third party, Winna B.V. remains fully responsible for CDD, including:

- Conducting a risk assessment of the customer;
- Determining if the customer is a Politically Exposed Person (PEP);
- Performing ongoing monitoring of the business relationship.

Difference Between Third Party Reliance and Outsourcing

- Third Party Reliance: The third party has its own relationship with the customer and carries out CDD on that basis. We will rely on the CDD info but we remain responsible for compliance.
- Outsourcing/Agency: The third party (agent or group company) acts on behalf of Winna B.V., using our procedures. Any customer on-boarded through an agent is considered to be on-boarded by us directly.

In all cases, Winna B.V. must ensure its AML/CFT policies and controls are followed. Decisions to accept or continue customer relationships cannot be outsourced.

5.7 Reporting of unusual transactions

Winna B.V., through the appointed AML Compliance Officer, has established procedures for reporting and assessing internal suspicious activity and on the decision-making process for external reporting.

Our platform users can report concerns for investigation by the AML Compliance Officer to determine whether there is knowledge or a suspicion of money laundering.

Where an employee knows or suspects that money laundering activity is taking place, or has taken place, or they are concerned that a transaction may be in breach of regulations, they must disclose this immediately.

Winna B.V., through the AML Compliance Officer, will take all reasonable steps to identify and report suspicious transactions or activities of all types.

In line with the National Ordinance for Identification of Services and NORUT legislation, Winna B.V. must detect and report all unusual transactions—whether completed or merely intended—without delay to the Financial Intelligence Unit (FIU) via the goAML reporting portal.

To support this, Winna B.V. maintains procedures that ensure:

- The recognition of unusual transactions based on both objective and subjective indicators;
- Adequate internal documentation of such transactions, including supporting materials such as identification documents, cash-out slips, or other relevant records;
- Immediate internal reporting of unusual activity in the format approved by management;
- That the AML Compliance Officer prepares and submits external reports to the FIU as required, including all supporting documentation in English.

Unusual transactions include (but are not limited to):

- Transactions of NAf. 5,000 or more (single or cumulative per gaming day), including chip purchases, cash-outs, deposits, and cashless transfers;
- Transactions involving persons or entities listed under the Sanctions National Ordinance;
- Transactions reported to police or justice departments in connection with ML/TF;
- Transactions that are unusually large, complex, or lack a clear lawful or economic purpose;
- Presumed ML/TF-related activity.

If an internally reported transaction is not escalated to the FIU, the reasons must be documented and signed off by the AML Compliance Officer and/or management.

All employees are protected from criminal or civil liability for breaching any confidentiality obligations when reporting transactions in good faith to the FIU.

Records will be maintained for up to 5 years after the user is no longer registered on our platform, including records of user risk assessment, user identity and verification, and user ongoing monitoring. This includes records on transactions (both domestic and international), to enable compliance with information requests from competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity. All records obtained through CDD measures (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files, and business correspondence must be kept for at least five years after the business relationship is ended, or after the date of the occasional transaction. The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority.

5.8 Anti-Money Laundering Compliance program

Winna B.V. has established an AML Compliance Program that is risk-based and designed to mitigate money laundering and terrorist financing risks. The program sets minimum standards to ensure compliance with applicable laws and regulations, including those of Curacao. The AML program includes a system of internal policies, procedures, and controls; a designated compliance officer with day-to-day oversight; an employee screening and ongoing training program; and an independent audit function to test the program's effectiveness.

It also ensures compliance with obligations related to customer due diligence, reporting of unusual transactions, retention of records, data protection, and training. Winna B.V. systematically tests and updates its AML program to address evolving risks within its operations. The program has been approved by senior management.

Furthermore, Winna B.V. ensures that any foreign branches or subsidiaries implement AML/CFT/CFP measures that are consistent with the requirements of Curaçao. Before designing and structuring the AML program, the company thoroughly assessed the legal and regulatory obligations applicable to the institution, its employees, and its customers under Curaçao law.

6. Compliance and Consequences of Non-Compliance

Violation of these laws and regulations are subject to administrative and criminal sanctions.

7. Related Information

[Winnables - Anti-Money Laundering & Anti-Fraud Policy](#)

8. Contact Information

If you have any questions regarding this policy, please contact our AML Compliance Officer by e-mail dm@winnables.com or by telephone on +33 680865890 for further information.

9. Policy History

10. Policy URL (if applicable)

[Winnables - Anti-Money Laundering & Anti-Fraud Policy](#)