

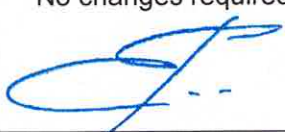
ANTI-MONEY LAUNDERING, COUNTER- TERRORISM FINANCING AND COUNTER- PROLIFERATION FINANCING POLICY

1Win N.V.

Document Information:

Approval	Board of Directors
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	April 10, 2026
Next Review Date	April 10, 2027

Version History:

Date	Version	Summary Changes	Approved by Management
April 10, 2026	1.1	Policy implementation	No changes required 

(SMES)
Solutions for Management
and Employment Support N.V.

Table of Contents

1. INTRODUCTION	5
POLICY STATEMENT	5
PURPOSE OF THIS AML POLICY	5
DEFINITION OF MONEY LAUNDERING	6
DEFINITION OF FINANCING OF TERRORISM	7
DEFINITION OF FINANCING THE PROLIFERATION OF WEAPONS	7
CONSEQUENCES OF NON-COMPLIANCE	7
2. THE RISK-BASED APPROACH	8
EXPLANATION OF THE RISK-BASED APPROACH	8
BUSINESS RISK ASSESSMENT	8
CUSTOMER RISK ASSESSMENT	8
CUSTOMER RISK	9
PRODUCT/SERVICE RISK:	9
GEOGRAPHIC RISK:	10
DELIVERY CHANNEL RISK:	10
3. CUSTOMER ACCEPTANCE POLICY	11
4. CUSTOMER DUE DILIGENCE (CDD)	13
ENHANCED DUE DILIGENCE (EDD)	14
TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS	16
TARGETED FINANCIAL SANCTIONS	17
POLITICALLY EXPOSED PERSONS (PEPs)	17
CDD MEASURES SPECIFIC TO PEPS	18
5. ONGOING MONITORING	20
ONGOING CUSTOMER PROFILE MONITORING	20
ONGOING TRANSACTION MONITORING	20
6. RELIANCE ON THIRD PARTIES TO PERFORM CDD	21
CONDITIONS FOR RELIANCE ON THIRD PARTIES	21
DISTINCTION FROM OUTSOURCING	22
RESPONSIBILITIES FOR CUSTOMER ONBOARDING	22
7. REPORTING OF UNUSUAL TRANSACTIONS	23
RECOGNITION OF UNUSUAL TRANSACTIONS	23
REPORTING OBLIGATIONS	24
PROHIBITION OF DISCLOSURE	25
RECORD KEEPING	25
8. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	27
APPOINTMENT OF A COMPLIANCE OFFICER	27
DUTIES OF THE COMPLIANCE OFFICER	27

EMPLOYEE SCREENING AND TRAINING PROGRAMS.....	27
EMPLOYEE DUE DILIGENCE.....	27
TRAINING.....	28
INDEPENDENT AUDIT FUNCTION.....	29
EXAMINATION BY THE GAMING CONTROL BOARD	30
9. APPENDIX I: COUNTRY RISK LIST.....	31

1. INTRODUCTION

POLICY STATEMENT

1Win N.V. (hereinafter “1Win” or the “Company”), is licensed and regulated by Curaçao Gaming Authority (CGA) to offer remote (online) games on the internet, under the License No. OGL/2024/587/0621. In accordance with the license conditions, 1Win has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (hereinafter “AML, CTF and CPF”) policy (hereinafter the “Policy”).

As a responsible gaming enterprise operating in Curaçao, 1Win acknowledges the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

PURPOSE OF THIS AML POLICY

The purpose of this Policy is to ensure the Company's compliance with the relevant legal and regulatory requirements from the authorities in charge of the supervision of AML, CTF and CPF matters for the gaming sector are the CGA and the Curaçao Financial Intelligence Unit (FIU), while simultaneously ensuring the integrity and sustainability of the operations of the Company.

The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- 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 Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);

- National Decree for general measures, of the 10 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 10 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 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 Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

DEFINITION OF MONEY LAUNDERING

Money Laundering (ML) is the process of concealing the true origins of illegally obtained funds, making them appear to originate from legitimate sources. ML encompasses a broad range of activities, including attempts to turn criminally obtained money into 'clean' money, transferring the benefits of crimes like theft or fraud, and facilitating the laundering of criminal or terrorist property. This process typically occurs in three stages:

- *Placement*, where illegal proceeds are introduced into the financial system through financial institutions, casinos, or cash-intensive businesses, often by converting cash into monetary instruments or gaming chips. In the gambling industry, this is occasionally achieved by purchasing chips with cash and subsequently redeeming their value without engaging in actual gameplay or with minimal play. It can also involve funding casino accounts using credit and debit cards, prepaid cards, checks, and cryptocurrency, followed by requests for payouts or inserting funds into gaming machines and immediately claiming those funds as credits.
- *Layering*, which involves transferring or moving these funds across various accounts or financial institutions to obscure their criminal origins. In the gambling industry, this may include transactions such as transferring funds between accounts, occasionally involving other casinos or jurisdictions, currency exchanges, structuring and refining transactions, as well as maintaining gambling accounts to store money and conceal it from regulatory authorities; and
- *Integration*, where the laundered funds are reintroduced into the economy, enabling their use in legitimate transactions such as purchasing luxury assets or investing in businesses.

DEFINITION OF FINANCING OF TERRORISM

Terrorism Financing (TF) refers to the provision of funds or financial support for terrorist acts, individuals, or organizations, and is characterized by the intent to intimidate populations or compel governments and international bodies to act or refrain from acting. Unlike ML, which always involves proceeds from illegal activities, terrorist financing may not necessarily derive from illicit sources; instead, it often utilizes legitimate funds from charitable donations, business profits, or foreign government sponsorships. While both terrorism financing and money laundering may employ similar methods – such as cash smuggling, structuring, wire transfers, and the use of debit and credit cards – the primary concern of TF is to obscure the intended use or end recipient of the funds rather than their origin. Additionally, funding for terrorist activities does not always require large sums of money, as it can accumulate over time through simple transactions.

DEFINITION OF FINANCING THE PROLIFERATION OF WEAPONS

Proliferation Financing (PF) is 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.

CONSEQUENCES OF NON-COMPLIANCE

Violations of this Policy may result in severe consequences, including disciplinary actions up to and including termination of employment for staff members found in breach of these regulations. Additionally, non-compliance can expose the casino to significant legal implications, including fines, sanctions, and potential criminal charges, which could severely impact our reputation and operational viability. Furthermore, failure to adhere to AML regulations may lead to increased scrutiny from regulatory authorities, loss of licenses, and damage to our business relationships.

2. THE RISK-BASED APPROACH

EXPLANATION OF THE RISK-BASED APPROACH

1Win adopts a risk-based approach in our AML compliance program, as recommended by FATF guidelines. This approach is essential for identifying and mitigating ML/TF/PF risks specific to the online gaming industry. When developing its AML compliance program, the Company assesses risks in such a way that higher risks necessitate more robust measures to mitigate them. Conversely, for lower-risk scenarios, the Company may employ simplified measures.

To effectively apply the risk-based approach, the Company conducts a preliminary assessment of the risks associated with ML/TF/PF within the organization, and based thereon develops and implements suitable policies, procedures, and controls to manage and mitigate these identified risks, including the present Policy.

1Win shall continuously monitor and enhance the effectiveness of these policies, procedures, and controls, ensuring that it maintains thorough documentation of its risk assessments, detailing all actions taken and the rationale behind them. 1Win shall also assess and manage risks associated with emerging technologies and new gaming products that may facilitate ML/TF/PF activities.

BUSINESS RISK ASSESSMENT

The Business Risk Assessment (BRA) framework is a crucial component of 1Win's AML, CTF, and CPF compliance program. It provides a systematic, risk-based approach for identifying, assessing, and mitigating ML/TF/PF risks within the Company's operations.

1Win performs thorough BRAs, evaluating potential risk factors related to customers, products and services, geographic locations, and delivery channels. Each risk factor is assessed for its likelihood and potential impact. Tailored controls and measures are then implemented to address these risks. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to maintain an accurate risk profile, with comprehensive assessments performed regularly. Additional assessments may be triggered by significant events, such as the introduction of new products, regulatory changes, or major shifts in the business environment. Thus, situations such as a widening of the customer-base or the addition of games and payment methods which present a different risk profile from those already offered should lead to a revision of the business risk assessment.

CUSTOMER RISK ASSESSMENT

The Customer Risk Assessment assesses the particular risks the Company will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile. The determination of the Customer Risk Rating is first assigned when a new customer applies for an account. This rating helps decide how often and in what way the customer will be reviewed in the future: the higher the risk, the more frequent and robust the ongoing monitoring of the customer would be. In accordance with the risk-based approach, a risk assessment regarding potential ML, TF and PF risks posed by the customer will be conducted during the establishing of the business relationship based on the information provided and established checks.

The Business and Customer Risk Assessment processes take into consideration the following general categories of risk factors:

CUSTOMER RISK

This involves assessing the customer's background, occupation, and transaction patterns. Categories of customers whose activities indicate a higher risk include:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders;
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- 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.

PRODUCT/SERVICE RISK:

This factor evaluates the risks associated with the products and services offered, including gaming products or services where customers can influence game outcomes, either on their own or in collaboration with others. Additionally, certain payment methods used by customers and accepted by casinos are seen as riskier for ML and TF. The following is a non-exhaustive list of high-risk factors:

- Anonymous payment methods (e.g. pre-paid cards and virtual assets);
- Unusual casino account usage;
- Specific game types, where bets are made even;
- Peer-to-peer gaming;
- Third-party accounts;
- Moving money from one gaming account to another;
- Multiple accounts or wallets;
- Additions or changes to associated payment methods.
- Identity fraud: Stolen financial account details used on websites, including stolen identities used to open financial accounts that are then used for gambling.

- Games with multiple operators: For example, poker platforms shared by different operators.
- Electronic wallets: Not all e-wallets are licensed in trustworthy countries, and some accept cash deposits. Moreover, e-wallets that only accept funds from financial accounts may not show the transaction to the online casino, which could help dishonest customers hide their gambling activities.

GEOGRAPHIC RISK:

This assessment considers the geographic location of the customer and the transaction, with countries that have weak AML, CTF and CPF regulations or high levels of corruption being deemed higher risk. The nationality, residence and place of birth of the player have to be considered as these might be indicative of a heightened geographical risk. 1Win regards the following sources of information produced by the FATF and other well-known non-governmental bodies (not limited):

- 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 State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML, CTF and CPF regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

1Win consistently monitors updates to the lists above and adjusts its CDD process to reflect relevant changes. Please see [Appendix I](#).

DELIVERY CHANNEL RISK:

This factor looks at the risks associated with the methods used to establish a business relationship or through which transactions are carried out. 1Win considers the increased risk of ML/TF/PF of the use of channels that favor anonymity and interactions on a non-face-to-face basis and, to the extent possible, shall take all reasonable measures to address and mitigate said risks.

3. CUSTOMER ACCEPTANCE POLICY

1Win's Customer Acceptance Policy is formulated in accordance with legal requirements and aligns with the Company's risk appetite as well as the BRA. In alignment with our commitment to maintaining the integrity of our operations, 1Win adopts a zero-tolerance stance towards financial crime and any illegal activities. We will not onboard customers who are engaged, directly or indirectly, in any form of illegal conduct. To uphold this standard, the Company implements various levels of due diligence to ensure all customers are reputable and compliant with applicable laws.

Prior to account creation, it is mandatory to conduct due diligence of potential customers to ensure they are not associated with financial criminal activities or barred from participation in the gaming industry. The Company will consider all relevant factors pertaining to the applicant's activities before granting access to our services.

Screening for Politically Exposed Persons (PEPs), and sanction checks is conducted at registration. Accounts in obviously fake or fictitious names will not be accepted.

1Win will accept customers only if they meet the following criteria:

- The applicant is a natural person. 1Win does not accept companies or other legal entities.
- The applicant has read and agreed to the latest applicable terms and conditions, including privacy policies and other relevant policies.
- The applicant consistently complies with the terms and conditions.
- The applicant registers and transacts on any 1Win platform on their own behalf.
- The applicant uses payment methods for which they are the legal and beneficial owner.
- The applicant is over 18 years of age.
- The applicant resides in a jurisdiction that is not [prohibited](#).
- The applicant is satisfactorily identified and verified under the Company's AML compliance program and AML policy.
- The applicant meets due diligence requirements, including source of wealth and source of funds checks, where applicable.
- The applicant provides all requested information and documentation as per the Company's AML compliance program.
- The applicant is not:
 - Listed on any sanctions list from recognized authorities, including the UN, EU and OFAC.
 - Linked to jurisdictions subject to comprehensive sanctions.
 - Identified with a risk profile that exceeds the Company's risk tolerance.
 - Customers who refuse to comply with documentation requests or fail to provide required information within the prescribed timelines in this Policy.
 - Customers who submit false or forged documentation, including fictitious identities.
 - Customers of unknown identity or those whose identity cannot be verified.

- Individuals attempting to create multiple accounts to evade due diligence requirements.
- Customers with any suspicion of involvement in money laundering or terrorism financing.
- Self-excluded customers who are barred from our websites as stipulated by licensing conditions.

If a customer is accepted, 1Win may require further information in line with this Policy and as deemed necessary for compliance. Failure to submit the requested information within the specified timeframe as per this Policy may result in termination of the business relationship and account closure.

4. CUSTOMER DUE DILIGENCE (CDD)

1Win is required to perform (CDD) under specific circumstances to ensure compliance with AML regulations and to protect the integrity of its operations. The Company must undertake CDD measures when players engage in financial transactions¹ that amount to Cg. 4,000 or more. This includes any deposits or withdrawals made by the player.

Furthermore, if there is any suspicion of money laundering or terrorist financing, the casino is obligated to conduct CDD. This also applies in situations where there are doubts about the accuracy or completeness of previously obtained identification information from the player.

To effectively monitor and determine when a player reaches the Cg. 4,000 threshold for CDD purposes, 1Win will evaluate not only individual transactions but also any series, combination, or pattern of transactions that exceed this amount. This evaluation will be conducted daily and will include all deposits, withdrawals, and peer-to-peer transfers made by the player.

Moreover, 1Win maintains a strict policy against anonymous accounts or accounts held under fictitious names. The casino is committed to identifying each player by collecting their name and other relevant information, which is essential for determining the purpose and nature of the business relationship.

1Win's CDD procedures require prospective customers to create a full profile at the point of registration. Mandatory information required at registration stage includes:

- i. Full name;
- ii. Date of birth;
- iii. Permanent residential address

The below information may be additionally requested for high-risk scenarios

- iv. Place of birth;
- v. Nationality; and
- vi. Identity number.

To complete the required customer verification process, 1Win asks its customers to upload a copy of valid identification documents (passport, identity card, driver's license or an equivalent document). This request is sent to the customer's registered email address (or other means of contact). If the documents are in a different language, the Company will take necessary steps to ensure that the documents adequately prove the customer's identity, such as

¹ Financial transactions are defined specifically as deposits and withdrawals; bonuses are obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation.

obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation.

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. Government-issued documents that lack a photograph can be used to confirm the customer's current address, provided the address is included in the document. 1Win accepts as proof of permanent residential address copy of utility bill (e.g. electricity, water, gas, telephone landline)² or bank statements, as long as they are not older than 6 months at the time they are received.

1Win is legally obligated to identify and verify the beneficial owner by confirming that customers are registering accounts to play and transact solely on their own behalf.

Furthermore, players must declare that they are not acting on behalf of any third parties. 1Win will not solely rely on this declaration. We are committed to actively monitoring player activity to detect any instances where a player may be using the account to play on behalf of others. This ongoing vigilance is essential to maintaining the integrity of our operations and ensuring compliance with AML-TF regulations.

To effectively manage this responsibility, the Company has implemented the following safeguards designed to prevent access to our services by individuals deemed suspicious. These safeguards include:

- Payment Method Verification: Ensuring that the payment method used for deposits is in the name to the player, insofar as possible.
- Denial of Service: Preventing transactions for players attempting to use payment methods not in their own name.

ENHANCED DUE DILIGENCE (EDD)

1Win shall implement Enhanced Due Diligence (EDD) measures for customers identified as higher risk, with actions tailored to the specific risks identified during the assessment process. These measures aim to intensify monitoring of the business relationship to detect any unusual or suspicious transactions or activities. EDD is required in situations where the risk of ML, TF or PF is heightened.

² Bills issued for mobile phone services are not acceptable, as they are generally not tied to a fixed location.

In any case, the following scenarios are subject to EDD:

- *Residents of High-Risk Geographic Areas:* Customers residing in jurisdictions associated with higher levels of corruption or inadequate AML, CTF, and CPF regulations.
- *Politically Exposed Persons (PEPs):* Individuals who hold prominent public positions or are closely connected to such individuals, which may elevate the risk of corruption.
- *Anonymity-Favoring Products or Transactions:* Services or products that allow for a higher degree of anonymity, potentially facilitating illicit activities.
- *New Products and Business Practices:* The introduction of new services, technologies, or delivery mechanisms that may present unforeseen risks.

The measures applied during EDD must align with the identified risks and may include, but are not limited to:

- *Additional Customer Information:* Collect comprehensive information about the customer, including occupation, previous addresses, and relevant data from public databases and online resources.
- *Clarification of Business Relationship Intent:* Obtain further information regarding the intended nature of the business relationship to better understand the customer's gaming habits and expectations.
- *Source of Funds and Wealth (SOF/SOW):* Gather detailed information on the source of funds or wealth for the player. Examples include:
 - Personal savings
 - Employment income
 - Pension releases
 - Share sales and dividends
 - Property sales
 - Gambling winnings
 - Inheritances and gifts
 - Compensation from legal rulings

In higher-risk situations, 1Win will periodically request SOF information, even if there has been no change in the customer's activity pattern. This ongoing diligence is essential for proactively addressing any potential concerns.

- *Transaction Purpose*: Ask for information regarding the reasons for intended or performed transactions to ascertain their legitimacy and ensure they align with the customer's profile.
- *Senior Management Approval*: Require approval from senior management before commencing or continuing the business relationship with higher-risk customers.
- *Enhanced Monitoring*: Implement increased scrutiny of the business relationship, which may involve more frequent reviews of transactions and account activities.
- *Account Verification for Initial Payments*: Require that the initial payment is made through an account in the customer's name with a bank that adheres to similar CDD standards.

TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS

If the customer cannot provide compliant documents within 30 days from the moment the Cg. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU, provided that a presumption of ML or TF exists.

During the CDD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the Cg. 4,000 thresholds, the customer will be prohibited from further deposits or withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

If a document submitted by a (potential) customer does not meet the verification standards, the designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

TARGETED FINANCIAL SANCTIONS

1Win is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with 1Win's legal obligations. This includes, but is not limited to, the following:

- 1Win shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.
- 1Win shall perform ongoing sanctions screening on customers and also perform trigger-based sanctions screening of customers at least in the following scenarios:
 - At the moment of registration;
 - At the moment of withdrawal request;
 - At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered and confirmed, 1Win must follow the established Process for the freezing of resources as per the Sanctions Ordinance, and must immediately file a report with the FIU.

POLITICALLY EXPOSED PERSONS (PEPs)

A PEP is an individual who is entrusted with a prominent public function, other than middle ranking or more junior officials, including but not limited to the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers,
- members of parliament or of similar legislative bodies,
- members of the governing bodies of political parties,
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances,
- members of courts of auditors or of the boards of central banks,
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces,
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organization.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents

- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.

CDD MEASURES SPECIFIC TO PEPs

1Win implements appropriate risk management systems to identify whether a customer or beneficial owner is a PEP, or a relative or close associate of one. This includes, at first instance, conducting comprehensive screening against reliable databases and lists to determine the PEP status of new customers during the onboarding process.

No business relationship shall be established or continued with a PEP before obtaining senior management ³ approval to service the PEP. This applies to new customers, ongoing relationships, and any occasional transactions.

In addition, the Company takes reasonable measures to ascertain the source of wealth and source of funds of the PEP. This involves:

- Requesting a statement from the PEP regarding their Source of Wealth.
- Verifying the statement through independent and reliable sources. Public sources will be consulted first, and if insufficient, additional documentation may be requested from the customer.

Additionally, the Company shall conduct enhanced ongoing monitoring of the business relationship, including analysis of the PEP's spending patterns to ensure they align with their declared legal sources of funds and the information on file.

In accordance with the risk-based approach that the Company employs, measures are tailored to the risk of the PEP, where the following are taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

PEP status screening will be conducted periodically throughout the business relationship. If a player who was not identified as a PEP at onboarding later becomes one, the Company is required to implement the EDD measures outlined in this Policy within a thirty-day window of

³ Senior management refers to individuals responsible for day-to-day operations or their immediate subordinates. Approval may also be sought from the Compliance Department manager.

this determination. Failure to implement the required measures for newly identified PEPs within the specified timeframe will result in the termination of the relationship with that customer.

5. ONGOING MONITORING

ONGOING CUSTOMER PROFILE MONITORING

During the periodic review of a customer, 1Win verifies and confirms that the CDD information about the client, nature and purpose of the business relationship, and SOF is still accurate and up to date, evaluate if there are external signals (bad press/adverse news, incidents) that could give rise to a change in the business risk profile of the customer and ensure to perform screening against sanctions lists and PEP lists. The periodic review also includes an overall review of the transaction behavior of the client to determine if unusual activities have taken place, for instance in case of transactions which normally would not be expected.

The periodical review of the customer is based on the risk profile of the customer:

- For high-risk customers – once per year;
- For medium risk customers – once every 2 years;
- For low-risk customers – once every 3 years.

ONGOING TRANSACTION MONITORING

1Win performs both real-time monitoring of transactions, as well as post-event monitoring, to ensure that such transactions and activity are consistent with the Company's knowledge of the client and their expected activity. More attention is paid to high amounts, high-risk clients and high-risk jurisdictions.

Particular risk factors will be closely monitored concerning business relationships and transactions, including:

- Gambling or transaction patterns that diverge from what is considered normal or what the customer initially indicated when establishing the business relationship.
- Execution of unusually large transactions by the customer.
- Requests for withdrawals to accounts other than those verified to belong to the customer (such withdrawals are prohibited).
- Requests to transfer gambling accounts or winnings to third parties (such transfers are also prohibited).

6. RELIANCE ON THIRD PARTIES TO PERFORM CDD

1Win recognizes the importance of effective Customer Due Diligence (CDD) in preventing money laundering and terrorist financing. In certain circumstances, the casino may rely on third parties to perform specific elements of the CDD process. This chapter outlines the conditions under which such reliance is permitted and the responsibilities that remain with the casino.

CONDITIONS FOR RELIANCE ON THIRD PARTIES

1Win may rely on third parties to perform the following elements of the CDD measures:

- Identifying the player and verifying the customer's identity using reliable, independent source documents, data, or information.
- Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, ensuring the casino is satisfied that it knows who the beneficial owner is. For legal entities, this includes understanding the ownership and control structure.
- Understanding and obtaining information on the purpose and intended nature of the business relationship.

When relying on a third party for the above CDD elements, 1Win must obtain the relevant information concerning these measures immediately from the third party. 1Win will establish a formal agreement with the third party that ensures:

- Copies of identification data and other relevant documentation related to CDD will be made available upon request.
- The arrangement will be periodically tested to ensure it functions as outlined in the agreement.

Despite this reliance, 1Win retains ultimate responsibility for conducting customer-based risk assessments, determining whether a customer is a PEP, and performing ongoing transaction monitoring.

1Win must ensure that the third party is regulated, supervised, or monitored for compliance with CDD and record-keeping requirements, as well as equipped with proper measures in place to comply with relevant regulations.

The third party should have an existing business relationship with the customer, independent of the relationship formed with 1Win, and must apply its own procedures to carry out CDD measures.

When selecting third parties for CDD reliance, 1Win will assess the country risk associated with the third party's location. This assessment ensures that the third party operates in a jurisdiction with acceptable standards for AML/CFT compliance.

DISTINCTION FROM OUTSOURCING

It is essential to differentiate reliance on third parties from outsourcing CDD measures. In an outsourcing scenario, the outsourced entity performs CDD on behalf of 1Win according to its own procedures and under 1Win's oversight. The casino remains responsible for compliance with AML regulations at all times. The decision to onboard a customer or to maintain a business relationship based on risk remains the sole responsibility of 1Win.

Additional conditions are also to be applied to outsourcing arrangements, including, but not limited to, ensuring that:

- The service provider engaged is in good-standing and has the necessary resources to fulfil the requirements being outsourced;
- The outsourcing arrangement has to be in writing and clearly lay down what are the respective obligations of the subject person and of the Company;
- There will be periodical assessments of how the service provider is fulfilling its obligations under the outsourcing arrangement both quantitatively as well as qualitatively; and
- The subject person has at all times immediate and unrestricted access to any information and documentation obtained by the Company in carrying out the outsourced functions.

RESPONSIBILITIES FOR CUSTOMER ONBOARDING

Any activity performed by an agent or group company of 1Win is considered an activity conducted by the casino itself. Therefore, any customer onboarded by an agent or affiliated group company must undergo the same CDD checks and controls applied to customers directly onboarded by 1Win.

1Win is responsible for ensuring that its AML/CFT controls, policies, measures, and procedures are consistently applied by all agents and group companies involved in the CDD process.

7. REPORTING OF UNUSUAL TRANSACTIONS

RECOGNITION OF UNUSUAL TRANSACTIONS

The Company trains its staff to recognize unusual transactions based on customer profiles and specific indicators and has established reporting procedures to the compliance officer.

In accordance with relevant legislation, 1Win is observing both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. Indicators a. to c. are referred to as "objective indicators", while d. is referred to as "subjective indicator". While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client.

All such transactions must be reported to the Compliance Officer in a format approved by management. Additionally, any supporting documentation, such as copies of identification, cash-out slips, and other relevant records, must also be submitted as supplements.

The Compliance Officer is tasked with maintaining an organized filing system for these records. If the Company fails to report internally identified transactions to the FIU, the rationale for this decision must be thoroughly documented and signed by the Compliance Officer and/or management. In accordance with the FATF Recommendations, the Company and its employees pay particular attention to all complex or unusually large transactions, as well as any unusual transaction patterns that lack a clear economic or legitimate purpose.

The following transactions or intended transactions are deemed unusual:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing of terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Cg. 5,000.00⁴ or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 1. A cashless transaction in the amount of Cg. 5,000.00 or more.
 2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.

⁴ For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

4. A cash out in the amount of Cg. 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Some examples of player activity that constitute unusual, potentially reportable activity are:

- The customer is uncooperative during the Customer Due Diligence (CDD) process.
- The customer attempts to create multiple accounts with the same operator.
- The customer makes substantial deposits in a single session using multiple prepaid cards.
- The customer deposits amounts significantly higher than what is typical for their betting behavior.
- The customer places small bets despite having deposited large sums, followed by a request to withdraw an amount far exceeding any winnings.
- The customer frequently deposits and withdraws funds without a plausible explanation.
- There are noticeable shifts in the customer's gaming behavior, such as engaging in transactions that are much larger than their usual activity.
- The customer inquires about transferring funds between accounts that belong to the same gaming group.
- The customer conducts transactions that appear disproportionate to their known wealth, income, or financial circumstances.
- The customer requests to transfer funds to another player's account or to a bank account held in the name of a third party.
- The customer exhibits suspicious behavior while playing high-risk games.

REPORTING OBLIGATIONS

All unusual activities and transactions, including attempted transactions, are initially reported internally. The officers responsible for transaction monitoring must immediately report any unusual activities to the Compliance Officer upon identification, providing a brief description of the specific mitigating measures taken.

All employees who engage with customers or have access to customer information receive anti-money laundering training. This training prepares them to identify actions by customers that may reasonably raise suspicions of money laundering or terrorism financing. Staff members are expected to recognize and understand any gaming or transaction behaviors that might indicate customer involvement in money laundering or terrorism financing. If they know, suspect, or have reasonable grounds to believe they are dealing with the proceeds of crime, they must submit an Internal Unusual Activity Report to the Compliance Officer. This ensures that the employee's legal obligation to report is fulfilled.

Employees are required to report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed. If a more in-depth investigation is necessary, the Compliance Officer will complete this within ten (10) business

days. During this time, the Compliance Officer may request additional information from relevant departments.

If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU Curaçao regarding any unusual monetary operations or transactions within 48 hours. In any cases whereby the report is made under one of the objective indicators, as defined below, the report must be made to the FIU Curaçao no later than 48 hours after the transaction has been executed.

PROHIBITION OF DISCLOSURE

All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

1Win has implemented a system of measures to ensure that employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the FIU Curaçao are safeguarded from threats or hostile actions by other employees, members of the management body, or customers. Additionally, they are protected from adverse or discriminatory employment actions.

RECORD KEEPING

1Win retains all necessary records of transactions, both domestic and international, for a minimum of five (5) years to ensure compliance with information requests from regulatory authorities. These records must be detailed enough to allow for the reconstruction of individual transactions, including the amounts and types of currency involved, if applicable, to provide evidence for potential criminal prosecutions.

All records gathered through CDD measures, such as copies of official identification documents, account files, and business correspondence, will be stored for at least five (5) years after the business relationship has ended or after the date of an occasional transaction.

Records shall be stored in a manner that ensures their integrity, confidentiality, and accessibility. Access is restricted to authorized personnel only. Regular backups of electronic records shall be conducted and stored in a separate, secure location to prevent data loss.

After the retention period, records shall be disposed of securely to prevent unauthorized access or disclosure.

When properly ordered to do so by any enactment, rule of law or court order, the Company shall provide a document, customer due diligence information, or enhanced due diligence

information and the Company will maintain a register of the documents and information provided and will keep a copy of the same.

8. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

APPOINTMENT OF A COMPLIANCE OFFICER

A senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML compliance officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

DUTIES OF THE COMPLIANCE OFFICER

The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the Company's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the Company's efforts against money laundering and financing of terrorism and financing of proliferation.

EMPLOYEE SCREENING AND TRAINING PROGRAMS

EMPLOYEE DUE DILIGENCE

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing 1Win's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual

employees, but also to its contractors and subcontractors. The employee due diligence process is informed by 1Win's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate ML or TF must undergo screening. This requirement applies to prospective employees prior to their hiring for such roles, as well as current employees from time to time. Regular updates and re-evaluations are essential for maintaining an effective compliance program against ML, TF and PF.

To screen both current and potential employees, 1Win will:

- Identify the individuals;
- Verify their identity;
- Confirm their employment history, such as through references; and
- Determine their suitability for the position and assess whether they pose any risk to the Company.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. 1Win must evaluate whether:

- The employee has a criminal record, which may be verified through a police check.
- The employee is or has been subject to regulatory, court, or legal actions.
- The employee has leveraged bankruptcy laws for personal gain.

TRAINING

In delivering AML, CTF and CPF training to the designated categories of employees, the Company will consider the necessary knowledge and qualifications required for their duties, responsibilities, and authorizations. As part of the training framework, the Company will outline the AML, CTF and CPF requirements and provide comprehensive information on the measures and activities that staff are expected to undertake within their roles.

1Win will ensure that documentation of the training provided to staff is maintained, capturing the following information:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

1Win will regularly update the training programs to reflect any changes in internal and external regulations, as well as developments in the availability of training programs in the market for external training. Furthermore, extraordinary training in AML, CTF and CPF matters will be provided in specific situations, including:

- The introduction of new internal and external regulations related to AML, CTF and CPF that apply to the Company's staff.
- The launch of new products or services that alter the AML, CTF and CPF risk exposure.
- Instances where an employee breaches internal or external AML, CTF and CPF regulations due to a lack of knowledge during the performance of their duties.

INDEPENDENT AUDIT FUNCTION

An independent audit function will be established for the annual evaluation of the AML program, ensuring audit personnel are qualified and findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate 1Win's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

EXAMINATION BY THE GAMING CONTROL BOARD

1Win shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the GCB during examinations or upon request. The following items must at all times be readily available and accessible:

- The written and approved AML Compliance Program addressing ML/TF/PF.
- Records of the Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for the company's AML policies and procedures.
- Records of reported unusual transactions.
- Records of unusual transactions that required further investigation.
- Records of frozen accounts.
- A schedule of training provided to personnel on ML/TF/PF.
- Assessment reports on the company's policies and procedures regarding money laundering, terrorist financing, and proliferation financing from the internal audit department or an external auditor.
- Customer files, including risk assessments, CDD, customer acceptance, and transaction information.

9. APPENDIX I: COUNTRY RISK LIST

High-risk countries include:

1. Afghanistan
2. Algeria
3. Angola
4. Bangladesh
5. Barbados
6. Belarus
7. Benin
8. Bosnia & Herzegovina
9. Bulgaria
10. Burkina Faso
11. Burundi
12. Cambodia
13. Cameroon
14. Central African Republic
15. Chad
16. China
17. Colombia
18. Cote d'Ivoire
19. Croatia
20. Cuba
21. Cyprus
22. Democratic Republic of the Congo
23. Egypt
24. Eritrea
25. Ethiopia
26. Guinea
27. Guinea-Bissau
28. Haiti
29. Hong Kong
30. India
31. Indonesia
32. Iran
33. Iraq
34. Jamaica
35. Kenya
36. Kyrgyzstan
37. Laos
38. Lebanon
39. Liberia
40. Libya
41. Mali
42. Moldova

43. Monaco
44. Mozambique
45. Myanmar (Burma)
46. Namibia
47. Nepal
48. Nicaragua
49. Niger
50. Nigeria
51. North Korea
52. Pakistan
53. Panama
54. Peru
55. Philippines
56. Russian Federation
57. Senegal
58. Somalia
59. South Africa
60. South Sudan
61. Sudan
62. Syria
63. Tanzania
64. Thailand
65. Togo
66. Trinidad and Tobago
67. Tunisia
68. Türkiye
69. Turkmenistan
70. Uganda
71. Ukraine
72. Ukraine (Crimea, Donetsk, Lugansk)
73. United Arab Emirates
74. United Kingdom
75. Vanuatu
76. Venezuela
77. Vietnam
78. Yemen
79. Zimbabwe

Low-risk countries include:

1. Australia
2. Canada

3. Denmark
4. Estonia
5. Finland
6. Germany
7. Iceland
8. Ireland
9. Luxembourg
10. Netherlands
11. New Zealand
12. Norway
13. Singapore
14. Sweden
15. Switzerland
16. Uruguay

Prohibited markets include, but are not limited to:

1. Aruba
2. Australia
3. Austria
4. Belgium
5. Bonaire
6. Curaçao

7. Cyprus
8. Myanmar (Burma)
9. North Korea
10. Saba
11. Serbia
12. Sint Eustatius
13. Sint Maarten
14. United Kingdom
15. United States of America