



ANTI-MONEY LAUNDERING AND PREVENTION OF CRIME POLICY: THE PREVENTION OF MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

(**"POLICY"**)

Contents

1. OBJECTIVES	2
2. PURPOSE OF THE POLICY	4
3. AUDIENCE	4
4. DEFINITIONS	4
5. GOVERNANCE AND RESPONSABILITIES	6
5.1 Senior Management Responsibility.....	6
5.2 Appointment and Role of the MLRO	7
5.3 Compliance Team.....	7
5.4 Responsibilities of Employees and Third Parties.....	8
6. POLICY IMPLEMENTATION	9
6.1 Business Risk Assessment (BRA)	9
6.2 Customer Risk Assessment (CRA)	10
6.3 Customer Acceptance Policy (CAP).....	11
6.3.1 PEP.....	12
6.4 Customer Due Diligence (CDD)	13
6.5 Ongoing Monitoring	16
6.6 Reliance on Third Parties to Perform Customer Due Diligence	17
6.7 Reporting of Unusual Transactions	18
6.8 AML Compliance Program	19
COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	21
7. Independent Audit Function	22
8. Examination by the Gaming Control Board	22
9. RELATED INFORMATION	24
10. CONTACT INFORMATION.....	24
11. POLICY HISTORY.....	26
Appendix I: Country Risk List.....	27
Appendix II: Business Affiliate and Supplier Due Diligence.....	29
Appendix III: Internal Unusual Activity Report.....	30

1. OBJECTIVES

This document defines the Policy and procedures related to risk assessment and management. It involves several discrete steps in assessing how to manage and mitigate the money laundering and terrorist financing risks to be faced by **One Internet B.V.** ("**One Internet**" or the "**Company**").

One Internet is fully committed to being constantly vigilant to prevent money laundering and combat the financing of terrorism to minimize and manage risks. It is also committed to its social duty to prevent serious crime and not to allow its systems to be abused to further these crimes.

One Internet will endeavor to keep itself updated with developments at the national and international levels on any initiatives to prevent money laundering and the financing of terrorism. It commits itself to always protecting the organization and its operations and safeguarding its reputation from the threat of money laundering and the funding of terrorist and other criminal activities.

This Policy also applies to the financing of the proliferation of weapons of mass destruction (WMD), in line with Curaçao's AML/CFT/CPF regulatory framework.

The objective of this policy is to ensure compliance with:

- 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

This Policy is part of the Company's internal compliance program and shall be reviewed at least every 3 years or upon significant regulatory changes.



2. PURPOSE OF THE POLICY

This anti-money Laundering and Counter-Terrorism Financing Policy establishes a structured approach to identifying, assessing, mitigating, and reporting risks associated with money laundering, terrorist financing, and proliferation financing.

The Policy ensures that the Company complies with all applicable laws and regulations, protects its reputation and operations, supports the financial system's integrity, and fulfills its social responsibility to prevent serious crime.

3. AUDIENCE

This Policy applies to all employees, senior management, directors, contractors, agents, consultants, and third-party service providers who are engaged by **One Internet B.V.** in any capacity.

Anyone performing services for or on behalf of the Company must comply with the obligations and principles outlined herein.

Failure to adhere to this Policy may result in disciplinary action, termination of employment or contracts, and legal consequences, as appropriate.

4. DEFINITIONS

For this AML/CFT Policy, the following definitions shall apply:

- **Business Risk Assessment (“BRA”)**: A formal process conducted by the Company to identify, assess, and manage the money laundering (“ML”), terrorist financing (“TF”), and proliferation financing (“PF”) risks associated with its operations, products, customer base, delivery channels, and jurisdictions.
- **Customer Acceptance Policy (“CAP”)**: A set of criteria and procedures established by the Company to determine the conditions under which a Player may be onboarded or rejected, based on their risk profile and compliance with AML/CTF requirements.



- **Customer Due Diligence (“CDD”)**: The process of verifying the identity of a Player, assessing their risk profile, and conducting background checks to ensure compliance with AML/CTF regulations.
- **Customer Risk Assessment (“CRA”)**: The evaluation conducted during Player onboarding to determine the Player’s individual risk level (low, medium, or high) based on factors such as nationality, occupation, transaction behavior, and links to high-risk jurisdictions or activities.
- **Money Laundering (“ML”)**: The process of concealing or disguising the illicit origin of financial resources to make them appear legitimate.
- **Money Laundering Reporting Officer (“MLRO”)**: The designated individual responsible for overseeing the Company’s compliance with applicable anti-money laundering (“AML”) and counter-terrorism financing (“CTF”) regulations. The MLRO acts as the main point of contact with regulatory and law enforcement authorities, analyzes internal reports of suspicious activity, ensures timely reporting to the Financial Intelligence Unit of Curaçao (“FIU-Curaçao”), and supports the implementation of the AML/CTF

Compliance Program.

- **Ongoing Monitoring**: The continuous surveillance of Players’ behavior and transactions to ensure alignment with their risk profiles and to detect unusual or suspicious activities that may indicate money laundering, terrorist financing, or proliferation financing.
- **Player**: A natural person registered as a user on any **One Internet** platform to participate in sports betting and online gaming.
- **Politically Exposed Person (“PEP”)**: An individual who currently holds or has held, within the past five years, a prominent public position, as well as their immediate family members (up to the second degree), representatives, and close associates.
- **Proliferation of Weapons of Mass Destruction (“PF”)**: Activities that promote, facilitate, or contribute to the development, acquisition, possession, transfer, or dissemination of nuclear, chemical, or biological weapons, as well as materials, equipment, technologies, or components intended for the production, maintenance, or use of such armaments, and that may result in financial sanctions under international frameworks.



- **Reliance on Third Parties:** The use of external service providers to perform certain aspects of the Customer Due Diligence (“CDD”) process, such as identity verification and sanctions screening, under strict contractual arrangements and with continued oversight by the Company.
- **Risk Matrix (also referred to as the Risk Assessment Framework):** A document that identifies, categorizes, and assesses ML/TF/PF risks, establishing probability levels, potential impacts, and mitigation measures for each risk factor.
- **Suspicious Operations:** Financial transactions or betting behaviors that deviate from the Player’s expected pattern, as defined by internal criteria, and which may indicate potential involvement in money laundering, terrorist financing, or proliferation financing.
- **Terrorist Financing (“TF”):** The act of promoting or gathering financial resources intended to be used, in whole or in part, to commission terrorist acts.
- **Transaction:** Any financial or betting movement conducted by a Player registered on any **One Internet** platform, including deposits, withdrawals, bets, and transfers.
- **Unusual Operation:** Any betting movement that, although not immediately indicative of a crime, presents characteristics that are uncommon relative to the Player’s expected profile and/or behavior.

5. GOVERNANCE AND RESPONSABILITIES

5.1 Senior Management Responsibility

Senior Management is fully engaged in the processes surrounding the Company’s assessment of money laundering (“ML”), terrorist financing (“TF”), and proliferation financing (“PF”) risks.

Senior Management actively participates in the decision-making related to developing, approving, and implementing appropriate policies, procedures, and controls to ensure compliance with applicable laws, regulations, and best practices.

It is ultimately responsible for promoting a strong compliance culture across the organization and ensuring that the Company effectively meets its Anti-Money Laundering and Counter-Terrorism Financing (“AML/CTF”) obligations.



Senior Management ensures that sufficient resources, authority, autonomy, and access to information are provided to the Compliance Team and the Money Laundering Reporting Officer ("MLRO").

5.2 Appointment and Role of the MLRO

Senior Management appoints a qualified senior officer and/or a specialized third-party service provider to act as the designated Money Laundering Reporting Officer ("MLRO"), responsible for overseeing the implementation and maintenance of the Company's AML/CTF Compliance Program.

The MLRO's core responsibilities include:

- Monitoring the Company's compliance with applicable AML/CTF/CPF obligations;
- Analyzing internal reports of unusual or suspicious activity;
- Filing Suspicious Transaction Reports ("STRs") and Suspicious Activity Reports ("SARs") with the Financial Intelligence Unit of Curaçao ("FIU-Curaçao"), where applicable;
- Acting as the point of contact with regulatory and law enforcement authorities regarding AML/CTF matters;
- Ensuring that all relevant records and documentation are appropriately maintained and made available for regulatory inspection;
- Promoting ongoing awareness and training on AML/CTF/CPF issues within the Company. The MLRO operates independently and reports directly to Senior Management.

5.3 Compliance team

The Compliance Team supports the MLRO in implementing the Company's AML/CTF Compliance Program by:

- Conducting Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") reviews;
- Monitoring Player activities and transactions for unusual or suspicious behavior;
- Ensuring that Players are screened against sanctions and Politically Exposed Persons ("PEP") lists;
- Documenting and investigating internal alerts related to potential ML/TF/PF risks;
- Maintaining up-to-date internal policies, procedures, and AML/CTF compliance manuals. The Compliance Team acts under the supervision and direction of the MLRO.



5.4 Responsibilities of Employees and Third Parties

All employees, contractors, agents, consultants, and third-party service providers engaged by the Company must comply fully with this AML/CTF Policy and all associated procedures.

Each individual is responsible for:

- Remaining vigilant for signs of money laundering, terrorist financing, or other financial crimes;
- Escalating unusual or suspicious activities promptly to the MLRO through the internal reporting channels;
- Participating in mandatory AML/CTF training programs;
- Maintaining the confidentiality of any internal reports and avoiding any tipping-off behavior.

Non-compliance with AML/CTF responsibilities may result in disciplinary actions, termination of employment or contracts, and legal consequences, as further detailed in this Policy.

If the customer cannot provide compliant documents within 30 days from the moment the XCG 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 XCG 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.

6. POLICY IMPLEMENTATION

This section describes how this Policy is implemented within One Internet B.V., including the key responsibilities, procedures, and oversight mechanisms established to ensure effective compliance.

The Company adopts a risk-based approach to identify, mitigate, and manage the risks of money laundering (“ML”), terrorist financing (“TF”), and the financing of proliferation (“PF”) by applicable laws, regulations, and guidelines issued by the Curaçao Gaming Control Board (“GCB”) and the Financial Intelligence Unit of Curaçao (“FIU-Curaçao”).

The Policy is implemented through the following pillars:

- Business Risk Assessment (BRA);
- Customer Risk Assessment (CRA);
- Customer Acceptance Policy (CAP);
- Customer Due Diligence (CDD);
- Ongoing Monitoring of customers and transactions;
- Reliance on third parties, where applicable;
- Reporting of unusual transactions;
- Maintenance of a comprehensive AML Compliance Program.

These elements are established and applied as detailed in the sub-sections below.

6.1 *Business Risk Assessment (BRA)*

The Company conducts a Business Risk Assessment (“BRA”) to identify, evaluate, and understand the money laundering (“ML”), terrorist financing (“TF”), and proliferation financing (“PF”) risks to which its operations are exposed.



The BRA considers the specific vulnerabilities associated with:

- The types of gaming products and services offered.
- The methods of delivery, including online platforms and payment channels.
- The geographical locations of customers.
- The categories and behaviors of customers.
- Technological infrastructure is used to facilitate transactions.

The BRA assesses inherent and residual risks and evaluates the effectiveness of the implemented controls to mitigate these risks.

The assessment is formally documented, approved by senior management, and made available for review by regulatory authorities upon request.

The Company reviews and updates the BRA at least once per year or whenever significant changes to its operations, customer profile, regulatory environment, or risk exposure exist.

The BRA forms the foundation of the Company's Anti-Money Laundering Compliance Program and guides the development of specific policies, procedures, and controls.

6.2 Customer Risk Assessment (CRA)

The Company conducts a Customer Risk Assessment ("CRA") for each Player at the time of onboarding to determine the level of money laundering ("ML"), terrorist financing ("TF"), and proliferation financing ("PF") risk associated with the individual.

The CRA is based on information collected during the registration and Customer Due Diligence ("CDD") processes and considers factors such as:

- The Player's nationality and country of residence;
- The Player's occupation and source of income;
- The volume and frequency of the Player's transactions;



- The use of high-risk payment methods;
- Behavioral patterns that may indicate higher risk activities.

The Company assigns each player a risk classification (low, medium, or high) based on the outcome of the CRA.

Players classified as high-risk, including Politically Exposed Persons ("PEPs") and individuals associated with high-risk jurisdictions or sectors, are subject to Enhanced Due Diligence ("EDD") measures.

The CRA is updated whenever there are material changes in the Player's behavior, profile, or transaction patterns or as part of the Company's ongoing monitoring activities.

The CRA supports the Company's broader risk management framework and ensures that controls are proportionate to each Player's risks.

6.3 Customer Acceptance Policy (CAP)

The Company maintains and applies a formal Customer Acceptance Policy ("CAP") to determine which individuals may be onboarded as Players based on their risk classification and compliance with applicable AML/CTF requirements.

The CAP is directly linked to the Customer Risk Assessment ("CRA") and ensures that Players presenting unacceptable or unmanageable levels of risk are not accepted or are promptly offboarded.

The CAP outlines specific acceptance and refusal criteria, which include but are not limited to:

- Players identified as presenting a high risk of money laundering, terrorist financing, or proliferation financing without sufficient mitigating documentation or justification;
- Players listed in sanctions databases or known to be associated with jurisdictions subject to international financial restrictions;
- Players who fail to provide complete or verifiable identification documents;

- Players who attempt to circumvent controls or provide inconsistent or misleading information.

According to Curaçao regulations, the CAP ensures that all politically exposed persons (“PEPs”) are identified and subject to Enhanced Due Diligence (“EDD”) measures before acceptance.

The CAP also prohibits onboarding individuals under 18 or any Player who is found to be using third-party identities, false documentation, or engaging in behavior suggestive of identity fraud.

The Compliance Team monitors the application of the CAP under the oversight of the Money Laundering Reporting Officer (“MLRO”) and reviews it periodically to reflect emerging risks and changes in the regulatory framework.

6.3.1 PEP

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

The Company implemented 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 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 regularly 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 enhanced due diligence measures outlined above within a thirty-day window of 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.

6.4 Customer Due Diligence (CDD)

The Company applies Customer Due Diligence ("CDD") procedures to verify the identity of all Players and ensure that they are eligible to use its services by applicable AML/CTF regulations.



The CDD process begins at the time of registration, when Players must provide:

- Full name;
- Date of birth;
- Permanent residential address;
- Place of birth;
- Nationality; and
- Identity number.
- Country of residence;
- Tax Identification Number (e.g., CPF);
- Mobile phone number.

The Company verifies this information through a third-party validation tool, which checks the date of birth to confirm that the Player is at least 18.

If the system identifies that the Player is underage, the registration is automatically canceled.

To complete the onboarding process, the Player must validate their mobile number via SMS. Without this confirmation, the account cannot be activated.

To complete the required customer identification and verification process, The Company 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. 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 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. The Company accepts as proof of permanent residential address copy of utility bill (e.g. electricity, water, gas, telephone landline) or bank statements, as long as they are not older than 3 months at the time they are received.

The Company applies identity verification ("KYC") measures based on thresholds:

- Upon one or more withdrawals totaling XCG 4,000, the Player must upload a copy of their identification document and a selfie holding it.

- When monthly transactions total XCG 20,000, the Player must also submit a utility bill and their most recent income tax return.

If the required documentation is not provided or verified, the Player's account remains restricted, and withdrawals are blocked.

In addition to identity verification, all Players are screened against:

- Sanctions lists (UN, EU, OFAC, Kingdom Sanctions Act, etc.);
- Databases for Politically Exposed Persons ("PEPs");
- Adverse media and third-party watchlists.

Players flagged during screening are subject to additional analysis by the Compliance Team and may be escalated for Enhanced Due Diligence ("EDD") or rejected entirely.

All CDD records are retained for at least five years after the end of the business relationship or the last transaction.

IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER

The Company 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. The Company 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.



- Withdrawal Identity Verification: Confirming the identity of players before processing withdrawals

6.5 Ongoing Monitoring

The Company continuously monitors the activities of its Players to ensure that their behavior remains consistent with their risk profile and to detect any indication of money laundering ("ML"), terrorist financing ("TF"), or proliferation financing ("PF").

Ongoing Monitoring is applied on a risk-sensitive basis, meaning that Players classified as high risk, such as Politically Exposed Persons ("PEPs"), are subject to more frequent and detailed scrutiny.

Monitoring is conducted both automatically and manually. The Company uses automated systems and internal procedures to track:

- Betting behavior and patterns;
- Deposit and withdrawal frequency and volumes;
- Use of multiple accounts or devices;
- Interactions with high-risk jurisdictions;
- Attempts to bypass identity verification or system controls.

Relevant staff members monitor real-time activity, escalate red flags to the Compliance Team, and register internal alerts when unusual or suspicious activity is detected.

If any inconsistency is identified between the Player's behavior and their risk profile, the Company may:

- Request additional documentation or information;
- Reclassify the Player's risk level;
- Restrict access to the account or block transactions;



- Initiate an internal review that may lead to a Suspicious Transaction Report (“STR”) filed with the FIU.

Ongoing monitoring is an integral part of the company’s risk management strategy, and it directly detects unusual or suspicious behavior over time.

6.6 *Reliance on Third Parties to Perform Customer Due Diligence*

The Company relies on third-party service providers to perform some aspects of the Customer Due Diligence (“CDD”) process, including identity verification and screening against sanctions and Politically Exposed Persons (“PEP”) databases.

Such reliance is strictly governed by contractual agreements and internal oversight procedures to ensure full compliance with Curaçao’s AML/CFT legal framework.

The third-party providers engaged by the Company:

- Are duly qualified and operate under-recognized compliance and data protection standards;
- Utilize reliable technological tools to validate customer identity and age through official documents and biometric verification;
- Perform real-time screening against global sanctions and PEP lists, as well as adverse media checks;
- Provide audit trails and reports for each verification performed, which are stored and accessible to the Company’s Compliance Team.

Despite delegating technical functions, the Company retains full responsibility for ensuring that CDD is conducted in accordance with applicable regulations and internal policies.

The MLRO is responsible for verifying the quality and consistency of third-party services and ensuring that any red flags raised during the outsourced process are appropriately addressed.

The effectiveness of the third-party arrangements is reviewed periodically and may be subject to internal or external audits.



6.7 Reporting of Unusual Transactions

The Company has established procedures to identify, assess, and report transactions or behaviors that may be indicative of money laundering ("ML"), terrorist financing ("TF"), or proliferation financing ("PF").

All employees are required to remain alert to signs of suspicious or unusual activity and to escalate concerns internally to the Money Laundering Reporting Officer ("MLRO") through a formal Suspicious Transaction Report ("STR").

In addition to subjective indicators, the Company also monitors for objective indicators as defined under Curaçao's National Ordinance on the Reporting of Unusual Transactions (NORUT), including:

- Any single or cumulative transaction equal to or exceeding USD 2,500 (or equivalent in local currency, XCG 5,000);
- Transactions involving high-risk jurisdictions or counterparties;
- Abnormal betting patterns or repetitive behavior inconsistent with the Player's risk profile.

All transactions that meet objective thresholds are reported to the Financial Intelligence Unit of Curaçao ("FIU-Curaçao") through the official GOAML portal.

The MLRO analyzes each STR received internally and determines whether a Suspicious Activity Report ("SAR") must be submitted to the FIU.

When applicable, the MLRO will also request prior authorization ("consent") from the FIU before completing any transaction involving a suspected case.

The identity of the employee submitting the internal report and the content of the STR are treated as confidential. The Company prohibits tipping off or any action that may alert the report's subject.

All reports submitted to the FIU are documented, securely stored, and available for audit or regulatory inspection.



6.8 AML Compliance Program

The Company maintains a formal Anti-Money Laundering and Counter-Terrorism Financing (“AML/CTF”) Compliance Program designed to identify, prevent, and mitigate the risks of money laundering (“ML”), terrorist financing (“TF”), and proliferation financing (“PF”).

The Compliance Program takes a risk-based approach and integrates policies, procedures, controls, monitoring activities, training, and reporting obligations.

The main components of the AML/CTF Compliance Program include:

- Implementation of Customer Due Diligence (“CDD”) and Enhanced Due Diligence (“EDD”) procedures in line with the Player’s risk classification;
- Ongoing monitoring of Player activities and transaction patterns;
- Identification and reporting of unusual and suspicious transactions to the FIU-Curaçao;
- Screening of Players against sanctions lists and Politically Exposed Persons (“PEPs”) databases;
- Risk assessments conducted both at business level (Business Risk Assessment – BRA) and at the customer level (Customer Risk Assessment – CRA);
- Use of qualified third-party providers for identity verification and sanctions screening under the supervision of the Company’s Compliance Team;
- Training and awareness programs are provided to all relevant staff at onboarding and on an annual basis;
- Regular independent audits or reviews to evaluate the effectiveness of the AML/CTF controls.

The Compliance Program is managed by the Money Laundering Reporting Officer (“MLRO”), who ensures that all regulatory obligations are fulfilled and that policies and procedures are updated whenever necessary to reflect regulatory changes, evolving risks, or operational developments.

The AML/CTF Compliance Program is subject to periodic review and approval by the Company's Senior Management to ensure its adequacy, effectiveness, and alignment with Curacao legislation.

The Company implemented 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.

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, see appendix.
- *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, The Company 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.

COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

All employees, senior management, contractors, and third-party service providers engaged by the Company must comply fully with this Anti-Money Laundering and Counter-Terrorism Financing ("AML/CTF") Policy and all related procedures and obligations.

Failure to comply with the provisions of this Policy may result in disciplinary measures and legal consequences, depending on the severity of the breach.

Examples of non-compliance include, but are not limited to:

- Failure to perform Customer Due Diligence ("CDD") or Enhanced Due Diligence ("EDD") as required;
- Failure to escalate or report suspicious or unusual activity;
- Failure to follow internal procedures regarding customer onboarding, verification, and monitoring;
- Tipping-off or any unauthorized disclosure related to ongoing investigations or reports submitted to the FIU-Curaçao.

Internal staff may be disciplined through formal warnings, suspensions, dismissals, and, where applicable, referrals to law enforcement or regulatory authorities.

Third-party service providers' breaches of contract provisions may result in termination of the contract and notification to relevant supervisory bodies.

In all cases, the Company reserves the right to cooperate with regulatory authorities and to provide any information necessary to support investigations or enforcement actions.

7. 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 Company'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.

8. Examination by the Gaming Control Board

The Company 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. RELATED INFORMATION

This Policy should be read in conjunction with the following documents and legal instruments:

- National Ordinance on the Identification of Clients when Rendering Services ("NOIS"), Curaçao;
- National Ordinance on the Reporting of Unusual Transactions ("NORUT"), Curaçao;
- Sanctions National Ordinance and Kingdom Sanctions Act;
- AML-CFT-CPF Manual 2025 issued by the Gaming Control Board ("GCB") and the Financial Intelligence Unit of Curaçao ("FIU-Curaçao");
- Internal Risk Assessment Procedures (Business Risk Assessment and Customer Risk Assessment);
- Customer Due Diligence ("CDD") and Know Your Customer ("KYC") Procedures;
- Internal Reporting Procedures for Unusual Transactions and Suspicious Activity;
- Sanctions Screening Procedures and PEP Identification Processes;
- Training and Awareness Programs on AML/CFT Compliance.

These documents provide additional operational details and requirements that complement and support the implementation of this Policy.

10. CONTACT INFORMATION

For any questions, concerns, or clarifications regarding this Anti-Money Laundering and Counter-Terrorism Financing (“AML/CTF”) Policy, employees, contractors, and third-party service providers must contact the Compliance Team via the following channels.

- Compliance Officer / Money Laundering Reporting Officer (“MLRO”): Daniel Brito
- E-mail: daniel@oig.company
- Phone: +55 86 98847-7277

Players and external stakeholders who require information about the Company’s AML/CTF commitments may also submit inquiries through the Company’s official website or customer support channels, where applicable.

The Compliance Team is responsible for promptly addressing internal and external inquiries, as required by applicable regulatory obligations and confidentiality requirements.

11. POLICY HISTORY

This Policy is subject to version control to ensure transparency regarding updates, revisions, and enhancements.

The version history of this Anti-Money Laundering and Counter-Terrorism Financing (“AML/CTF”)

Policy is recorded as follows:

Status	Version	Author	Date	Changes
Daft	V1.0	Daniel Brito	20-Aug-2024	First Draft
Final	V1.0	Daniel Brito	28-Aug-2024	Last Adjustments
Approved	V1.0	Daniel Brito	28-Aug-2024	Approved By Fernando Lima
Review	V2.0	Daniel Brito	25 -April-2025	Review and Update
Approved	V2.0	Daniel Brito	25 -April-2025	Approved By Fernando Lima
	V2.1	Compliance	May 30, 2025	Review and Update

Future versions will reflect any additional updates due to regulatory changes, operational improvements, or emerging risks.

Appendix I: Country Risk List

Please note that the risk classification in following list of countries is subject to continuous review. Any changes in risk indicators will be reflected promptly to ensure the list remains current and accurate.

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

Excluded markets include, but are not limited to:

1. Aruba
2. Australia
3. Austria
4. Belgium
5. Bonaire
6. Curaçao
7. Czech Republic
8. Denmark
9. Estonia
10. France
11. Germany
12. Greece
13. Hungary
14. Israel
15. Italy
16. Latvia

17. Lithuania
18. Netherlands
19. Poland
20. Republic of Ireland
21. Saba
22. Serbia
23. Sint Eustatius
24. Sint Maarten
25. Slovakia
26. Slovenia
27. Spain
28. Sweden
29. Switzerland
30. United Kingdom
31. United States of
America.

Appendix II: Business Affiliate and Supplier Due Diligence

Company information:

Registered name and legal form	
Registration number	
Date of incorporation	
Registered address	
Status	
Ultimate Beneficiary Owners (UBOs)	
Persons with significant control (directors, members of supervisory board)	
Company website (if applicable)	

The documents below must be duly certified (where applicable) and, if they are not in the English language, provided with legalized translation in a language understandable by the Company Name:

Document	Remarks
Certificate of Incumbency showing the Ultimate Beneficial Owner(s) and Director(s)	
Recent Excerpt from the Chamber of Commerce or equivalent	
Certified copy passport of UBO(s) and Director(s)	
Proof of address of the UBO(s) and Director(s) no older than 3 months ¹	
Proof of Licensing	
AML Policy	

¹ For natural persons who live or reside outside of Curaçao, and who are not personally identified by the provider, the NOIS mandates that the identity is established by either (1) a photocopy of an identification document (e.g. passport, ID card, driver's license) accompanied by a certified copy or extract from the Civil Registry of the person's place of permanent residence, or (2) following the electronic receipt of an identity document of the individual, within 2 weeks we receive a certified copy of the document.

Appendix III: Internal Unusual Activity Report

Date of report:		
Client ID:		
Date of account registration:		
Account	status	
(Active/Suspended/Blocked):		
Risk rating:		
Account balance:		
Client details:	Full name:	
	E-mail:	
	Phone number:	
	Brand registration:	
	Date of birth:	
	Nationality/Country of registration:	
	Address:	
	Due diligence documents held:	
Reason for reporting:		< explain what activity / transaction gave rise to the report >
Date of unusual activity/transaction:		
Provide details (e.g. dates and amounts) of any known intended or pending transactions:		
Reporting employee:	Signature:	Date:
Upon completion, please forward the form to the Compliance Officer as soon as possible.		

In witness whereof, One Internet B.V. has caused this Policy to be duly executed this 12th day of August 2025




By: e-Management N.V. as Director of One Internet B.V.

20250528_OneInternetBV_compliance manual_v2.1

Final Audit Report

2025-08-25

Created:	2025-08-12
By:	Sharella Bitoria (sharella.bitoria@hbmgroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAI_36gO7Tmi9DT2thJrJKfB4L4FZ6-5gt

"20250528_OneInternetBV_compliance manual_v2.1" History

-  Document created by Sharella Bitoria (sharella.bitoria@hbmgroup.com)
2025-08-12 - 9:36:48 PM GMT
-  Document emailed to Annesol Melaria (annesol.melaria@hbmgroup.com) for signature
2025-08-12 - 9:36:54 PM GMT
-  Email viewed by Annesol Melaria (annesol.melaria@hbmgroup.com)
2025-08-13 - 7:59:27 PM GMT
-  New document URL requested by Annesol Melaria (annesol.melaria@hbmgroup.com)
2025-08-25 - 8:57:04 PM GMT
-  Email viewed by Annesol Melaria (annesol.melaria@hbmgroup.com)
2025-08-25 - 8:57:24 PM GMT
-  Document e-signed by Annesol Melaria (annesol.melaria@hbmgroup.com)
Signature Date: 2025-08-25 - 8:57:34 PM GMT - Time Source: server
-  Document emailed to Bryon Finies (bryon.finies@hbmgroup.com) for signature
2025-08-25 - 8:57:36 PM GMT
-  Email viewed by Bryon Finies (bryon.finies@hbmgroup.com)
2025-08-25 - 9:13:19 PM GMT
-  Document e-signed by Bryon Finies (bryon.finies@hbmgroup.com)
Signature Date: 2025-08-25 - 9:13:51 PM GMT - Time Source: server
-  Agreement completed.
2025-08-25 - 9:13:51 PM GMT