

AML/CTF Policy - HERMES CONSULTING COMPANY N.V.

Revision No.: 4

Approved by: Director, CAPITAL TRUST CORPORATION N.V.

Responsible Officer: Volodymyr Bakotskyi

Effective Date: May 26, 2025

Next Review Date: May 26, 2026



Table of Contents:

1. Policy Statement	2
2. Purpose	2
3. Audience	2
General Stakeholders	2
Compliance Officer (MLRO)	3
4. Definitions	3
5. Policy Implementation	4
5.1 Business Risk Assessment	4
5.2 Customer Risk Assessment	5
5.3 Customer Acceptance Policy	5
5.4 Customer Due Diligence	7
Standard CDD	7
Enhanced Due Diligence (EDD)	8
Politically Exposed Persons (PEPs) Handling	8
Product, Service, and Transaction Risks	8
Sanctions	9
Ongoing Due Diligence	11
5.5 Ongoing Monitoring	12
Monitoring Customer Identity	13
Transaction Monitoring	13
5.6 Reliance on Third Parties	14
5.7 Reporting of Unusual Transactions	14
5.8 AML Compliance Program	16
6. Compliance and Consequences of Non-Compliance	17
7. Related Information	18
International and Regional Legal Instruments	18
National Legislation – Curaçao (CW)	18
National Legislation – Belgium (BE)	19
Other Reference Tools and Systems	19
8. Contact Information	19
9. Version History	20



1. Policy Statement

HERMES CONSULTING COMPANY N.V., registered under number 145995 with its office at Chuchubiweg 17, Willemstad, Curacao (hereinafter referred to as the "Company"), is committed to combating money laundering (ML), terrorist financing (TF), and proliferation financing (PF) through a comprehensive set of policies, procedures, monitoring tools, and training programs. This policy outlines the measures taken to ensure full compliance with the applicable AML/CTF laws of Curaçao and international standards.

2. Purpose

Historically, criminals across jurisdictions have been using money laundering practices to conceal and alter the true origin and ownership of the proceeds from their illegal activities, with the aim of avoiding prosecution, conviction, and the confiscation of funds derived from unlawful sources. Similarly, terrorist financing schemes have been using funds that may be legitimately sourced, but are intended to support terrorist operations. The ability to launder illicit proceeds through global financial systems is crucial for the success of criminal enterprises. Money serves as the essential resource for terrorist organizations, enabling them to fund and carry out their activities.

To combat these practices, an international AML/CFT framework has been established, and the Company strives to be a part of it by adopting a set of clear standards and procedures outlined in this Policy. The purpose of these Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) standards and procedures is identifying, preventing, and reporting money laundering, terrorist financing, and other illicit financial activities which may be attempted by using services offered by the Company. This Policy ensures compliance with the applicable laws and regulations of Curaçao.

The definitive legal requirements which the Company adheres to is laid out in the following laws and regulations:

3. Audience

This Policy affects all stakeholders of the Company.

General Stakeholders

The Policy shall be adhered to, carried out by and applied to:

- direct and indirect shareholders,
- directors, managers and other key persons and decision makers,
- employees of the Company,
- any individuals or entities acting on behalf of the Company.

The Policy shall also be applied to third party stakeholders, and in order to have business relations with the Company, they shall agree and be subjected to the procedures outlined in this Policy. These include:

- individual and corporate customers,
- contractors, subcontractors, suppliers and service providers, partners and agents.,
- other parties supporting or benefiting from the Company's operations.

Compliance Officer (MLRO)

The Compliance Officer (MLRO) appointed by the company is the key person for managing AML/CFT procedures and this Policy. Their responsibilities in this regard include:

- formulate, approve, and implement the Company's AML/CFT Policy and update it with an appropriate frequency, at least once every 12 months
- establishment and control of appropriate internal procedures to prevent activities related to ML and CF
- investigating, analyzing the Company's operations in relation to AML/CFT, submission of reports and information to the Financial Intelligence Unit Curaçao as appropriate
- training of relevant employees on the AML/CFT provisions and procedure currently in force
- monitoring all amendments in the Legislation aimed at prevention of money laundering and/or terrorist financing and updating internal instructions according to up-to-date information.

4. Definitions

- **Compliance Officer (MLRO):**
Money Laundering Reporting Officer — the designated person responsible for implementing the AML/CTF policy, conducting internal investigations, and liaising with regulatory authorities, including the Financial Intelligence Unit (FIU).
- **CDD (Customer Due Diligence):**
A standard verification process involving the collection and verification of customer identity, understanding the purpose of the business relationship, and ongoing monitoring of transactions.
- **EDD (Enhanced Due Diligence):**
A more intensive form of due diligence applied in higher-risk situations. It includes collecting additional documentation, verifying the source of wealth/funds, and obtaining approval from senior management.
- **PEP (Politically Exposed Person):**
An individual who holds or has held a prominent public position, or a close relative or associate of such a person, and therefore presents a higher risk of involvement in bribery or corruption.

- **FIU (Financial Intelligence Unit):**
A government authority responsible for receiving, analyzing, and acting upon reports of suspicious financial activity to combat money laundering and terrorist financing.
- **SDN (Specially Designated Nationals):**
Individuals or entities listed on sanctions lists (e.g., OFAC) with whom transactions and business relationships are prohibited.
- **ODD (Ongoing Due Diligence):**
Continuous monitoring of clients and their transactions after the business relationship is established to detect deviations from normal activity or suspicious behavior.
- **SoW/SoF (Source of Wealth / Source of Funds):**
Documentation or information used to verify the legal origin of a customer's assets or incoming funds.
- **ML/TF (Money Laundering / Terrorist Financing):**
Criminal activities aimed at disguising the origins of illicitly obtained money (money laundering) or providing financial support for terrorist operations (terrorist financing).
- **Customer (client):**
A customer who is of the approved age and participates in a game of chance.

5. Policy Implementation

5.1 Business Risk Assessment

The Company conducts regular business risk assessments to identify potential vulnerabilities in its operations, particularly in the context of online gaming. High-risk scenarios include complex financial flows, the use of anonymizing tools, or players from sanctioned jurisdictions. Products and services are reviewed to evaluate their susceptibility to ML/TF.

For the purpose of identification, assessment, and analysis of risks of money laundering and terrorist financing related to their activities, the Company conducts a risk assessment. Steps are taken to identify, assess, and analyze risks that are proportionate to the nature and level of complexity of the economic and professional activities of the Company. The following are taken into account at least in the following risk categories:

- Risks relating to customers.
- Risks relating to countries, geographic areas, or jurisdictions.
- Risks relating to products, services, or transactions.

Risk relating to communication, mediation, or products, services, transactions, or delivery channels between the Company and customers.

The steps taken to identify, assess and analyze risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of the Company and/or the players.

AML screening is conducted on existing or potential customers to assess their risk. When conducting screenings, the Company seeks to achieve the following objectives:

- Conduct a risk assessment
- Avoid violating sanctions
- Protect from regulatory fines

The Company performs AML screening of its customers upon account opening and/or upon their first withdrawal requests and/or when customers engage in financial transactions equal to or above XCG 4,000 (or prior thereto) and/or when risk levels of customers change. With AML screening, the Company ensures that existing or potential customers are not present on any of the sanctions lists, banned or wanted lists, are not classified as PEPs, and do not have any adverse media data on file. To perform AML screening, the Company first obtains the full name, date of birth, address, and contact details of the customer. PEPs and sanctioned individuals are not allowed as customers. Further, the Company does not allow anonymous gambling.

5.2 Customer Risk Assessment

The Company maintains the following risk classification:

Medium risk. Players who fail to provide the requested documentation at a stage where this is required (for example, where it has been requested due to defined triggers, PEPs, increase in volume of transactions), the account will be under increased monitoring.

High risk. The player's activity is the determining factor for the classification of a Player as High Risk. Any Player for whom an automated alert has been generated, or an inappropriate activity has been detected, will be categorized as High Risk, for which an Enhanced Due diligence procedure is applied. The instances in which a High-risk classification is assigned include, but are not limited to, those instances as mentioned in the section below.

Customer Risk Assessment is thus carried out based on the information collected on the customer during establishing a business relationship to formulate their Risk Profile. The latter is then used to assign an appropriate level of Customer Due Diligence (see clause 5.4).

5.3 Customer Acceptance Policy

The Customer Acceptance Policy of the Company is based on what is required under applicable legislation. The following persons are not accepted as customers:

- Under 18
- Individuals on the FATF, UN, EU, UK, or OFAC sanctions lists

- Residents in countries classified and/or prohibited as high risk by the applicable competent authorities
- Individuals suspected of ML/ TF involvement or other types of criminal activity
- Self-excluded customers
- Individuals who have submitted documentation or information which we have reasonable grounds to suspect is fake or fraudulent

Categories of customers whose activities may indicate a higher risk include:

- customers who have multiple sources of income
- customers with irregular income streams
- PEPs
- high spenders
- disproportionate spenders
- casual customers like locals or tourists, especially when spending patterns change
- improper use of third parties
- customers using multiple casino player rating accounts

The Company also takes into consideration geographical risks, which are assessed by the location of the player and the source of wealth in the business relationship. Nationality, residence, and place of birth of the player are taken into account.

Based on the results of the CRA the following levels of Customer Due Diligence are applied to customers with different risk levels:

- **Medium-Risk Clients:**
Subject to **Standard CDD** procedures, including identity verification, verification of the beneficial owner (if applicable), and transaction monitoring. Ongoing Due Diligence (ODD) is performed **once every 6 months**.
- **High-Risk Clients:**
Subject to **Enhanced Due Diligence (EDD)** measures. This includes the collection of additional documentation (e.g., source of wealth), senior management approval, and enhanced monitoring. ODD is carried out **once per month**.

The decision to accept or continue a relationship with high-risk clients must be approved by the Compliance Officer (MLRO) and documented accordingly. All risk ratings are reviewed periodically and adjusted based on the client's activity, transactional behavior, or external changes such as updated sanctions or regulatory status.

Risk Level	CDD Type	Key Measures	Ongoing Review
Medium Risk	Standard CDD	Full identity and BO verification, standard transaction monitoring	Once every 6 months
High Risk	Enhanced Due Diligence (EDD)	Additional documentation (SoW/SoF), senior management approval, enhanced review	Once per month

4

5.4 Customer Due Diligence

The Company applies Customer Due Diligence (CDD) not as a one-time obligation, but as a continuous process throughout the entire customer relationship lifecycle. By embedding periodic reviews and dynamic risk evaluations into its broader compliance framework, the company ensures sustained alignment with Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) requirements. This practice forms part of the Company's overarching risk-based strategy, which is designed to adapt to emerging risks and maintain the integrity of its operations.

The Company enforces Customer Due Diligence (CDD) measures swiftly and in alignment with established obligations under Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. These measures are designed to ensure that all customer identities are accurately established and verified before significant financial interaction occurs.

Standard CDD

Upon the creation of a player account, the Company collects key identity details from each user, including:

- Full legal name
- Residential address
- Date of birth
- Place of birth
- Nationality
- Identity number
- Politically Exposed Person (PEP) status
- Sanctions screening

As part of the company's risk-based compliance framework, identity verification is initiated prior to processing any financial transaction that meets or exceeds a threshold of XCG 4,000. This threshold is applied in the following scenarios:

- A single transaction equal to or above XCG 4,000
- A combination of transactions (such as multiple deposits, withdrawals, or internal transfers) that cumulatively reach this amount

Daily transaction data is monitored and aggregated per customer, enabling the company to identify when thresholds are met and respond in real time. Once the XCG 4,000 mark is reached, a full risk evaluation of the customer is conducted, and any remaining CDD steps are completed without delay.

The Company emphasizes early completion of CDD. This preemptive strategy is intended to prevent the entry of illicit funds into the system by ensuring that no user is granted full platform access without having first undergone due diligence.

Operational Limits for Incomplete CDD

In situations where a player reaches the XCG 4,000 threshold prior to completing CDD, specific limitations are imposed:

- If triggered by a deposit: Further deposits and withdrawals are restricted; however, the customer may continue to participate in gaming using their current account balance.
- If triggered by a withdrawal request: The player's account is temporarily frozen, and all gameplay is suspended until full verification is completed.
- These safeguards help preserve the integrity of the platform and prevent unauthorized movement of funds during the verification window.

Enhanced Due Diligence (EDD)

For high-risk scenarios, EDD measures are applied, including:

- In-depth investigation into the player's background.
- Verification of the source of funds and wealth.
- Close examination of transaction patterns.
- Regular updates of identification information.

EDD also applies to politically exposed persons (PEPs), requiring thorough risk assessments and ongoing monitoring.

Politically Exposed Persons (PEPs) Handling

The company's AML/CTF/CPF policy requires heightened scrutiny for PEPs, their family members, and close associates. Enhanced Due Diligence (EDD) measures include obtaining senior management approval, understanding the source of funds and wealth, and conducting rigorous ongoing monitoring.

Product, Service, and Transaction Risks

Certain gaming services, financial instruments, and transaction types inherently present greater risks of being exploited for money laundering and terrorism financing. Criminal actors often target weak points within gaming ecosystems to manipulate outcomes or obscure the origins of illicit proceeds.

Illicit funds derived from activities such as fraud, narcotics trade, or theft may be funneled through gambling platforms to disguise their origin. The use of anonymous payment tools—such as prepaid cards and digital assets like cryptocurrencies or tokens—presents heightened risks due to limited traceability.

The misuse of player accounts for non-gaming purposes, such as acting as temporary repositories for financial transactions, also raises compliance concerns. Similarly, peer-to-peer transfers among players can facilitate unauthorized movement of funds.

Criminals may attempt to exploit third-party financial instruments, such as bank accounts or cards registered under different identities, or transfer funds across multiple gaming accounts,

further complicating traceability. Financial services linked to gambling, such as currency exchanges, credit facilities, or the use of multi-operator platforms, present an additional layer of risk.

To counter these threats, the Company enforces stringent transaction monitoring protocols, applies EDD processes where appropriate, and maintains full compliance with global AML/CTF/CPF regulations.

Sanctions

The company's AML/CTF/CPF policy mandates rigorous compliance with both international sanctions and regulatory standards. To ensure we meet these obligations, we implement comprehensive procedures focused on adhering to all sanctions imposed by national and international authorities. This process involves conducting thorough due diligence on every client and transaction to prevent any interactions with sanctioned individuals, entities, or regions.

Monitoring and reporting are critical components of the company's AML/CTF/CPF policy. The company continuously observes all transactions for any suspicious activities that could breach sanctions. Any anomalies detected are reported immediately to the relevant authorities. Furthermore, the company's commitment to compliance is reinforced through ongoing staff training, which ensures that all personnel are up-to-date with current sanctions regulations. This approach safeguards our operations and helps mitigate potential risks.

In addition, the company is dedicated to ensuring that all client interactions and transactions are meticulously checked against the most recent Sanctions Lists. Where applicable, automated systems may perform real-time verifications, and our database is regularly updated to reflect the latest sanctions information. When a match or suspicious activity is identified, it is promptly reported to the appropriate authorities. The company takes decisive action, such as freezing accounts or blocking transactions, to address and manage compliance risks.

The company's sanctions compliance procedures are subject to frequent reviews and updates to align with evolving legislation. This includes monitoring lists such as:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55); Kingdom Sanction Act (N.G. 2016, no. 54); GCB announcements.
- EU Sanctions.
- UK OFSI Sanctions.
- UN Security Council Consolidated List.
- US List of Foreign Terrorist Organizations.
- OFAC Sanctions.

Geographical Risk:

Geographical risk refers to the potential money laundering (ML), terrorism financing (TF), and proliferation financing (PF) risks associated with the player's location and the origin of their financial resources. A player's nationality, country of residence, and place of birth are

key factors in determining risk exposure, as some jurisdictions pose higher financial crime risks than others.

Countries are considered high-risk if they:

- Lack a robust AML/CFT framework.
- Have high levels of corruption.
- Are subject to international sanctions due to terrorism financing or involvement in the proliferation of weapons of mass destruction (WMDs).
- Are known to harbor terrorist organizations or provide financial support for terrorism.

Trusted Sources for Identifying High-Risk Jurisdictions

To assess geographical risks, the Company refers to reputable international regulatory bodies and recognized independent organizations, including:

Financial Action Task Force (FATF) Reports:

High-Risk Jurisdictions Subject to a Call for Action.

Jurisdictions Under Increased Monitoring.

Caribbean Financial Action Task Force (CFATF) Public Statements.

U.S. Department of State – International Narcotics Control Strategy Report (INCSR):

Identifies Jurisdictions of Concern and Primary Concern.

European Commission's List of High-Risk Third Countries:

Highlights jurisdictions with strategic deficiencies in AML/CFT regulations.

Office of Foreign Assets Control (OFAC) Sanctions List:

Includes countries subject to U.S. financial restrictions due to terrorism, proliferation activities, or other national security threats.

Reports from Credible Global Organizations:

Countries identified as sponsors of terrorism or as hosting terrorist organizations.

Transparency International's Corruption Perceptions Index (CPI), which ranks countries based on their levels of corruption.

Risk Categorization and Policy Implementation

To effectively manage geographical risk, the Company maintains a structured risk classification system, categorizing countries into high-risk and low-risk groups. This classification is used to:

Apply enhanced due diligence (EDD) measures for players from high-risk jurisdictions.

Consequences of CDD Non-Compliance

If a customer fails to submit the required documentation within 30 days after reaching the transaction threshold, the following measures are taken:

- The business relationship is terminated.
- If there are grounds for suspicion of ML or TF, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU);
- In the absence of suspicion, any remaining funds are returned to the source of deposit (e.g., the original bank account or digital wallet);
- Where suspicion persists, internal policies determine whether funds should be frozen pending further investigation, ensuring compliance with applicable law.
- Records of the terminated relationship are securely stored for at least five years.

Preventing Tipping-Off

The Company is conscious of the legal prohibition against tipping-off under AML/CTF legislation. Measures such as account restrictions or termination are assessed carefully to avoid alerting customers prematurely. Internal procedures guide staff on how to manage communication and actions in a way that respects confidentiality and regulatory obligations.

By integrating timely, risk-based, and proactive CDD practices into its operations, the Company ensures comprehensive adherence to AML/CTF/CPF standards, minimizes exposure to financial crime, and fosters a secure and transparent environment for both digital and physical gaming channels.

Ongoing Due Diligence

CDD procedures are actively applied to both new and existing customers. Central to this approach is the ongoing monitoring of transactions and the periodic reassessment of client risk profiles to ensure that the customer's activity remains within acceptable parameters.

Tailored Risk-Based Measures

For customers who were initially onboarded with incomplete or minimal due diligence, the Company conducts retrospective reviews. This includes:

- Re-evaluating and updating records for customers identified as having elevated risk;
- Scheduling routine updates to ensure that all stored data reflects the latest regulatory requirements and customer status.

The Company re-applies full CDD measures in any of the following circumstances:

- A significant shift in the customer's behavior or profile, such as initiating unusually large or complex transactions, moving into a high-risk jurisdiction, or being reclassified as a Politically Exposed Person (PEP);

- Regulatory or legal updates requiring refreshed or additional customer information;
- When a pre-existing customer initiates a transaction or series of transactions that meet or exceed the company's defined threshold of XCG 4,000, thereby activating the full CDD requirement under the firm's AML policy.

Remediating Gaps in Historical Due Diligence

In cases where clients were initially onboarded without full CDD being completed—often due to historical onboarding practices—the Company undertakes corrective action as follows:

- Customers classified as high-risk are given priority for immediate identity and risk reassessment.
- Full CDD is applied systematically at intervals based on the specific risk rating assigned to the customer.

By ensuring that customer profiles are consistently reviewed and verified over time, The Company strengthens its AML/CTF/CPF compliance posture, mitigates exposure to financial crime, and maintains a secure and transparent environment within its gaming operations.

The company's due diligence efforts are designed to uncover indirect or covert attempts to engage with sanctioned parties or jurisdictions. Any discovered evasion tactics are swiftly reported to the relevant authorities, and corrective actions, including transaction suspensions and account reviews, are promptly implemented. Regular audits and ongoing staff training further ensure that the company remains vigilant and compliant with the latest legislative requirements and best practices for preventing sanctions evasion.

5.5 Ongoing Monitoring

Ongoing Monitoring is a critical component of the Company's AML/CTF framework and serves to ensure that customer activity remains consistent with their known risk profile, financial behavior, and source of funds, while their identification information is up-to-date and adequate.

Objectives of Ongoing Monitoring:

- Ensure that transactions conducted are consistent with the customer's known profile, source of funds, and gaming behavior.
- Detect unusual, complex, or structured transactions that may indicate money laundering, terrorist financing, or other financial crime.
- Identify changes in customer behavior that may warrant a re-assessment of risk level and the application of Enhanced Due Diligence (EDD) measures.
- Prevent misuse of outdated or falsified documentation
- Fulfill regulatory obligations under Curaçao's AML legislation and guidance from the Financial Intelligence Unit (FIU).

Monitoring Customer Identity

The Company implements a range of proactive measures to ensure that identification records remain valid and trustworthy:

- Based on a customer's risk rating, the Company may require updated identification documents at regular intervals (e.g., every 6 or 12 months).
- This includes resubmission of personal ID, proof of address, and payment method confirmation.

The Company initiates re-verification of identity data upon key events such as:

- Change of address or contact information;
- Addition of a new payment instrument;
- Reclassification of the customer to a higher risk;
- Expiry of previously submitted documents.

Not all changes require full re-verification. The Compliance Department assesses, on a **risk-sensitive basis**, whether an update in identification data is:

- **Minor** (e.g., phone number update), which may be logged without further action;
- **Substantial** (e.g., name change, new jurisdiction), requiring re-confirmation of identity, possible re-onboarding, or enhanced scrutiny.

Transaction Monitoring

The Company performs continuous surveillance of transactions, account activity, and behavioral indicators to promptly detect any unusual or suspicious patterns.

Monitoring is both automated and manual, utilizing predefined thresholds, behavioral analytics, and IP analysis to identify the following red flags in the customer behavior:

- Unusual betting patterns with players placing large bets on low-risk games or frequently changing betting patterns.
- Frequent large transactions.
- Rapid deposit and withdrawal cycles with criminals depositing large sums to their accounts and withdrawing them quickly.
- Multiple accounts and IP addresses for conducting transactions
- Activities inconsistent with declared income or location

High-risk customers are subject to more frequent and in-depth reviews, with monitoring cycles conducted monthly, while medium- and low-risk customers are reviewed semi-annually or annually, respectively. In cases where anomalies are detected, such as activity inconsistent with declared income or geographic risk indicators, transactions may be temporarily suspended, escalated to the Compliance Officer (MLRO), and, where necessary, reported to the Financial Intelligence Unit (FIU).

Enhanced Ongoing Monitoring is also applied to clients associated with high-risk jurisdictions, PEPs, or those under investigation for previously flagged behavior. This approach ensures early detection of suspicious activity and enables timely intervention in accordance with applicable laws and internal risk mitigation procedures.

5.6 Reliance on Third Parties

The Company does not rely on third parties for CDD unless through pre-approved arrangements where third parties comply with Curaçao's AML standards.

5.7 Reporting of Unusual Transactions

The Company is required to abide by the National Ordinance for Identification of Services and also required to detect and report either intended or completed unusual transactions. The Company pays attention to any activity which they regard as likely, by its nature, to be related to money laundering and/or terrorist financing, and in particular to complex or unusually large transactions, and all unusual patterns of transactions which have no apparent economic or visible lawful purpose, and any relationships or monetary operations with customers from third countries in which, based on the information officially published by international intergovernmental organizations, money laundering and/or terrorist financing prevention measures are insufficient or do not correspond to international standards. The Company examines the basis for and purpose of the execution of such operations or transactions and the results of the investigation that must be recorded in writing.

Compliance Officer (MLRO) must report to the Financial Intelligence Unit Curaçao any suspicious or unusual monetary operations or transactions. The Company and its employees and/or representatives and/or the person who acted on their behalf are not liable for damage caused to a person or customer participating in a transaction made in economic or professional activities, in performing a professional act on the provision of a professional service:

- upon performance of duties and obligations arising from AML and TF regulations in good faith, from failing to make the transaction or from failing to make the transaction within the prescribed time limit.
- in connection with the performance of the duty to report in good faith.

The following transactions or intended transactions are deemed unusual:

- cases where it is aware of, obtains information concerning, has suspicions or has substantial grounds to suspect that money laundering and/or terrorist financing was, is, or will be performed, or it has been attempted.
- cases where they have suspicion or sufficient grounds to suspect that the customer's funds have been obtained from criminal activity.
- cases where they have a suspicion or sufficient grounds to suspect that the transactions or activities are related to terrorist financing.
- transactions by or on behalf of a person who is named on a list adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55).

- transactions in the amount of XCG 5,000 or more (such a transaction may be a single transaction or a series, combination or pattern of transactions involving a total amount of the monetary equivalent of XCG 5,000 or more and is considered per gaming day).

There are indicators helping to identify unusual transactions. Indicators describe when a transaction (executed or intended) is to be labeled as unusual and thus must be reported to the Financial Intelligence Unit Curaçao without delay. The term "without delay" is interpreted as follows:

The Compliance Officer (MLRO) should send unusual transaction reports within 48 hours after the transaction has been executed, or after there has been an intention of a transaction.

In individual cases, the reporting to the Financial Intelligence Unit Curaçao might be extended to a maximum of 5 working days. A request for extended reporting should be directed in writing to the Financial Intelligence Unit Curaçao, stating the reasons for the extension.

The Financial Intelligence Unit Curaçao will inform the respective reporting entity in writing of its decision within 24 hours.

The time period between the execution of the transaction (or the intention to execute a transaction) and the moment the Compliance Officer (MLRO) receives the report should not exceed 24 hours.

As of the moment that the Compliance Officer (MLRO) receives the transaction report, he has to complete the relevant research with regard to a possible Money Laundering/Terrorism Financing within 10 working days.

If, after the research period (maximum of 10 working days), there is a suspicion of Money Laundering/Terrorism Financing, the Compliance Officer (MLRO) must report the transaction within 48 hours to the Financial Intelligence Unit.

In the case it is not possible to comply with the above-mentioned time periods, the Compliance Officer (MLRO) shall send a request for reporting extension in writing to the Financial Intelligence Unit Curaçao, stating the reasons for this extension.

The Financial Intelligence Unit Curaçao will evaluate objective grounds and inform the reporting entity of its decision in writing within 48 hours upon receiving the request.

There are two kinds of indicators: objective and subjective.

In case of an objective indicator, it describes the mandatory conditions under which circumstances a transaction is to be considered unusual.

In case of a subjective indicator, the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, and any

other circumstance that may be relevant) has reasonable indications to presume that a transaction is related to money laundering or terrorism financing. For subjective indicators, red flags can be suggested by the supervisors and/or the FIU Curaçao that indicate such possible presumptions.

A report to the FIU is submitted via GoAML reporting portal (link to register in GoAML - https://portal.fiucuracao.cw/goAMLWeb_PRD/Home)

The structural unit of the Company, a member of a management body and an employee are prohibited to inform a person about a report submitted on them to the Financial Intelligence Unit, a plan to submit such a report or the occurrence of reporting as well as about any precept made by the Financial Intelligence Unit or about the commencement of criminal proceedings.

The Company shall establish a system of measures ensuring that the employees and representatives of the entity reporting of a suspicion of money laundering or terrorist financing to the Financial Intelligence Unit are protected from being exposed to threats or hostile action by other employees, management body members or customers of the Company, in particular from adverse or discriminatory employment actions.

5.8 AML Compliance Program

The Company has established a formal, risk-based Anti-Money Laundering (AML) Compliance Program that sets the minimum operational and ethical standards for the prevention of money laundering, terrorist financing, and proliferation financing. The program is designed in line with Curaçao's regulatory requirements and relevant international frameworks and reflects the company's proactive approach to financial crime prevention within the gaming industry.

Program Architecture and Principles:

- **Risk-Based Design:**

The AML program is structured to allocate resources and apply control measures commensurate with the assessed level of risk. Customer, product, geographic, and transactional risks are evaluated continuously to determine the appropriate level of due diligence, oversight, and intervention.

- **Regulatory Alignment:**

The program is specifically built to comply with the following Curaçao legislative instruments:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92)
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)

- The Sanctions National Ordinance (N.G. 2014, no. 55)
- The Kingdom Sanction Act (N.G. 2016, no. 54)
- **Governance and Accountability:**
Oversight of the AML Program is entrusted to the appointed Compliance Officer (MLRO), who reports directly to senior management. The Compliance Officer (MLRO) ensures implementation, conducts internal reviews, maintains communication with regulators, and oversees internal reporting channels.
- **Internal Controls and Independence:**
AML compliance controls are embedded across key operational functions and are supported by independent monitoring. Systematic checks are enforced on transactions, onboarding, and payments to detect anomalies before escalation is required.
- **Escalation and Account Blocking Protocols:**
When there is a reasonable suspicion of money laundering, the Company has a zero-tolerance policy. The Compliance Officer is empowered to:
 - Immediately block the account.
 - Suspend access to funds,
 - Initiate a full internal investigation, and
 - If necessary, report the case to the Financial Intelligence Unit (FIU) as per legal obligation. These steps are taken without notifying the customer, in accordance with anti-tipping off provisions.
- **Program Review and Adaptation:**
The AML Compliance Program undergoes a formal review annually or upon any significant legal, technological, or business model change. Feedback from internal audits, staff training assessments, and regulatory inspections are used to enhance the policy's effectiveness and relevance.

6. Compliance and Consequences of Non-Compliance

The Company enforces a strict culture of compliance to ensure adherence to applicable laws, including Curaçao's AML and sanctions regulations, and to protect its operations from financial crime, legal exposure, and reputational damage. Compliance with this AML/CTF Policy is mandatory for all employees, officers, agents, contractors, and third parties acting on behalf of the Company. Any failure to comply with AML/CTF obligations—whether intentional or due to negligence—may result in serious consequences.

Internally, such breaches can lead to disciplinary action up to and including termination of employment or contract.

From a regulatory standpoint, non-compliance may trigger financial penalties, regulatory sanctions, license revocation, civil litigation, or criminal prosecution against the Company or individuals involved.

Additionally, failure to act upon or report suspicious activity may result in personal liability for the employee or officer responsible. The Company is committed to proactively identifying, investigating, and remedying compliance breaches and will fully cooperate with relevant authorities in any enforcement proceedings.

Employees are therefore required to immediately report any actual or suspected violations of this policy to the Compliance Officer (MLRO) without delay.

7. Related Information

This policy should be read in conjunction with the following legal, regulatory, and operational frameworks, which provide the basis for the Company's AML/CTF obligations and activities:

International and Regional Legal Instruments

- **EU Directive 2015/849:** *Directive of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.*
- **EU Regulation 2015/847:** *Regulation on information accompanying transfers of funds.*
- **EU Sanctions Framework:** *Various regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technologies, including all dual-use goods.*

National Legislation – Curaçao (CW)

- Regulation for the combating of ML/FT and Proliferation of weapons of mass destruction
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92)
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)
- The Sanctions National Ordinance (N.G. 2014, no. 55)

- The Kingdom Sanction Act (N.G. 2016, no. 54)

National Legislation – Belgium (BE)

- **Law of 18 September 2017:** *Law on the prevention of money laundering and the limitation of the use of cash.*

Other Reference Tools and Systems

- **goAML Portal:** <https://portal.fiucuracao.cw>
- **UN Sanctions Overview:** <https://www.un.org/securitycouncil/sanctions/information>
- **OFAC Sanctions Lists:** <https://www.treasury.gov/ofac>
- **EU Sanctions Portal:** <https://www.sanctionsmap.eu>
- **OFSI UK Sanctions Implementation:**
<https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation>

8. Contact Information

For any questions regarding this policy, please contact:

Compliance Department, HERMES CONSULTING COMPANY N.V.

Address: Chuchubiweg 17, Willemstad, Curacao

Email: support-en@sapphirebet.com

9. Version History

Revision No.	Effective dates
4	26.05.2025 (current)
3	10.09.2024
2	14.05.2024
1	12.05.2023

