

Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy for Black Hawk Technology B.V.

Key Information

Approving Official(s): Black Hawk Technology B.V. Senior Management

Responsible Office: Black Hawk Technology B.V. Compliance Department

Effective Date: 31st March 2025

Next Review Date: 31st March 2026

1. Policy Statement

Black Hawk Technology B.V. is unequivocally committed to upholding the most stringent standards in its Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) endeavours. The company acknowledges its critical role in safeguarding the integrity of the global financial system and is dedicated to preventing its services, products, and facilities from being exploited for illicit activities. This commitment extends to conducting all business operations with the utmost ethical integrity, transparency, and strict adherence to all applicable laws and regulations governing AML and CTF. This policy outlines Black Hawk Technology B.V.'s comprehensive framework designed to mitigate the risks associated with financial crime, ensuring full compliance with the legal and regulatory obligations established by the Curaçao Gaming Authority (CGA) and other relevant authorities.

2. Purpose

The primary objective of this AML/CTF Policy is to establish a robust and comprehensive framework that prevents Black Hawk Technology B.V. from being utilized as a conduit for money laundering or terrorist financing. This policy is fundamental to ensuring that Black Hawk Technology B.V. consistently meets its obligations under all applicable anti-money laundering and counter-terrorist financing laws and regulations, particularly those mandated by the Curaçao Gaming Authority. It serves as a foundational document, outlining the specific standards and procedures that Black Hawk Technology B.V. adopts to identify, assess, and effectively mitigate identified money laundering and terrorist financing risks.

This policy must be interpreted and applied in conjunction with all other pertinent internal policies and procedures of Black Hawk Technology B.V. These include, but are not limited to, customer onboarding protocols, comprehensive risk assessment methodologies, escalation procedures for suspicious activities, and detailed suspicious activity reporting processes. Adherence to the provisions of this policy is mandatory for all personnel and entities subject to its scope. Non-compliance carries severe implications, potentially leading to disciplinary actions, and where applicable, may result in significant criminal or civil penalties under relevant laws.

3. Audience

This policy applies to all employees, contractors, consultants, agents, and third-party suppliers of Black Hawk Technology B.V. It also extends to any foreign branches and subsidiaries of Black Hawk Technology B.V., which are required to implement AML/CTF measures consistent with the requirements outlined herein and those of Curaçao.

4. Definitions

For the purpose of this policy, the following terms shall have the meanings ascribed to them below, as defined by the Curaçao Gaming Authority regulations:

- **Casino:** In the context of these regulations, this term encompasses both land-based and online casinos.
- **CFATF:** The Caribbean Financial Action Taskforce, an organization of twenty-four states in the Caribbean Basin, Central, and South America, committed to implementing common countermeasures against money laundering.
- **Compliance Officer:** A senior officer at management level, operating independently from gaming operations, who is responsible for the detection and deterrence of money laundering and terrorist financing.
- **FATF:** The Financial Action Task Force, an independent intergovernmental body established in 1989, tasked with developing and promoting policies to protect the global financial system from money laundering and terrorist financing.
- **FATF Recommendations:** A framework of recommendations on policies and measures issued by the FATF to combat money laundering and terrorist financing.
- **Financial Transactions:** In land-based casinos, these include the purchase or cashing in of casino chips or tokens, account opening, wire transfers, and currency exchanges. They do not refer to gambling transactions involving only casino chips or tokens. In online casinos, financial transactions are deposits and withdrawals (excluding bonuses). Wagered amounts and winnings are considered gambling transactions and are not financial transactions.
- **FIU:** The Financial Intelligence Unit Curaçao, as referred to in Article 2 of the NORUT.
- **Kingdom Sanctions Act:** The National Ordinance published under N.G. 2016 no. 54.
- **Money Laundering (ML):** All acts performed with money of illegal origin to change its identity so that it appears to have originated from a legitimate source. This process typically involves three phases: Placement, Layering, and Integration.
- **NOIS:** National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).
- **NORUT:** National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).
- **Other online games:** Includes sports betting, esports-betting, fantasy sports, lottery and bingo, skill-based games, and virtual sports.
- **Politically Exposed Persons (PEPs):**
 - **Foreign PEPs:** Individuals who are or have been entrusted with prominent public functions by a foreign country, and their direct family members or close associates (e.g., Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials).
 - **Domestic PEPs:** Individuals who are or have been entrusted domestically with prominent public functions (e.g., Heads of State or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials).
 - **International Organization PEPs:** Persons who are or have been entrusted with a prominent function by an international organization, such as members of senior management (directors, deputy directors, board members, or equivalent functions).
- **Sanctions National Ordinance:** The National Ordinance published under N.G. 2014 no. 55.

- **Source of Funds:** Refers to how the funds for a particular transaction were obtained by the player (e.g., personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings).
- **Source of Wealth:** The origin of all the money a person has accumulated over their lifetime (e.g., employment income, inheritances, investments, business ownership interests).
- **Terrorist Financing (FT):** The financing of terrorist acts, of terrorists, and terrorist organizations.
- **Unusual Transaction:** A transaction considered as such based on specific indicators, pursuant to Article 10 of the NORUT.
- **(Ultimate) Beneficial Ownership (UBO):** Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

5. Policy Implementation

Black Hawk Technology B.V.'s AML/CTF compliance program is built upon a robust risk-based approach, ensuring that measures are proportionate to the identified risks. This approach is systematically applied across all aspects of the company's operations, from initial customer engagement to ongoing transaction monitoring and reporting. The implementation of this policy is a continuous process involving regular assessment, adaptation, and enhancement of controls to address the dynamic nature of financial crime risks.

5.1 Business Risk Assessment (BRA)

Black Hawk Technology B.V. is mandated to conduct a comprehensive Business Risk Assessment (BRA) to identify and understand the inherent money laundering and terrorist financing risks to which its operations are exposed. This assessment is crucial for ensuring that the policies, controls, and procedures adopted by Black Hawk Technology B.V. are adequate and effective in preventing and mitigating these risks.

The BRA process involves a thorough examination of how Black Hawk Technology B.V.'s products and services could potentially be exploited for illicit purposes, along with an evaluation of the likelihood and impact of such exploitation. All factors that may influence ML/TF risks are considered, with particular emphasis on:

- **Type of Customers:** Assessing the risk profiles associated with different customer segments.
- **Products and Services Offered:** Identifying vulnerabilities inherent in specific gaming products or financial services.
- **Delivery Channels:** Evaluating the risks posed by various methods through which services are provided (e.g., online platforms, physical establishments).
- **Geographical Risk Factors:** Analyzing the risks associated with the jurisdictions where customers reside or from which transactions originate.

Black Hawk Technology B.V. also incorporates the outcomes and recommendations from the National Risk Assessment (NRA) of the jurisdictions in which it operates into its BRA. Following the assessment, Black Hawk Technology B.V. establishes a clear risk appetite, defining the level of risk it is prepared to accept. This determination is fundamental to the design and maintenance of its overall anti-money laundering compliance program.

The effectiveness of these risk mitigation measures is continuously monitored and improved as necessary. Black Hawk Technology B.V. commits to revising its BRA whenever there are significant changes to its operating environment or business activities, such as the introduction of new payment methods, expansion into new markets, launch of new games, or changes in regulatory requirements. In the absence of such changes, the BRA is formally assessed at least once annually to determine if any updates are required. The BRA, including its methodology, the rationale for risk factor ratings (low, medium, high), its outcomes, and all information sources used, is meticulously documented and approved by the Senior Management. This documentation is made available to the CGA upon request.

5.2 Customer Risk Assessment (CRA)

In parallel with the Business Risk Assessment, Black Hawk Technology B.V. conducts a Customer Risk Assessment (CRA) for each player. This assessment is undertaken either prior to carrying out an occasional transaction or during the establishment of a business relationship. The CRA is designed to evaluate the specific ML/TF risks that Black Hawk Technology B.V. may encounter when providing its services or products to individual players.

The information gathered during the CRA process is utilized to formulate a comprehensive customer risk profile. This profile enables Black Hawk Technology B.V. to categorize the ML/TF risk posed by a player as low, medium, or high. An initial provisional risk rating is assigned based on the information collected at the outset of the relationship, which may be revised as additional information becomes available or questions are addressed. The CRA is a dynamic process, and a customer's risk rating may be adjusted at any stage of the business relationship in response to new information or changes in behaviour.

The CRA serves as the direct input for applying the appropriate level of Customer Due Diligence (CDD) measures, as stipulated in Black Hawk Technology B.V.'s Customer Acceptance Policy (CAP). This systematic approach ensures that CDD efforts are commensurate with the identified risk, allowing for simplified measures where risks are lower and enhanced measures where risks are higher.

5.3 Customer Acceptance Policy (CAP)

Black Hawk Technology B.V. maintains a comprehensive Customer Acceptance Policy (CAP) that directly stems from the Customer Risk Assessment (CRA). The CAP outlines the specific criteria and procedures for accepting new customers and maintaining existing business relationships, ensuring that the appropriate level of Customer Due Diligence (CDD) is applied based on the assessed risk.

The CAP explicitly details:

- **Description of High-Risk Players:** It identifies and describes types of players who are likely to present a higher-than-average risk of money laundering or terrorist financing. This includes, but is not limited to, Politically Exposed Persons (PEPs), individuals with multiple or irregular income streams, high spenders, and those with unknown or unverifiable sources of income or assets.
- **Risk Indicators:** The policy specifies clear indicators for classifying customer risk as low, medium, or high, guiding the application of proportionate CDD measures.
- **CDD Measures:** It defines the specific level of CDD measures, including ongoing monitoring, to be applied for each risk category. This ensures that resources are

concentrated on higher-risk relationships while streamlining processes for lower-risk ones.

- **Declining Service:** The CAP clearly articulates the circumstances under which Black Hawk Technology B.V. will decline to establish or continue a business relationship with a prospective or existing customer. This includes situations where CDD obligations cannot be met, where a customer is identified on a sanctions list, or where there is a suspicion of illicit activity.

In developing and implementing its CAP, Black Hawk Technology B.V. strictly adheres to its obligations concerning Politically Exposed Persons (PEP) and conducts thorough Sanctions Screening. This proactive approach ensures that Black Hawk Technology B.V. does not engage in business relationships with individuals or entities subject to international sanctions or those presenting elevated political risk.

5.4 Customer Due Diligence (CDD)

Black Hawk Technology B.V. implements a robust Customer Due Diligence (CDD) program as a cornerstone of its AML/CTF compliance regime. The company strictly prohibits the maintenance of anonymous accounts or accounts opened under fictitious names. Without sufficient knowledge of a customer's identity, beneficial ownership, and the purpose and intended nature of the business relationship, Black Hawk Technology B.V. will not establish or maintain a business relationship or carry out occasional transactions.

CDD measures are mandatory under the following circumstances:

- When players engage in financial transactions equal to or exceeding NAf. 4,000.
- When carrying out occasional transactions above the monetary equivalent of NAf. 4,000.
- When there is any suspicion of money laundering or terrorist financing, regardless of the transaction amount.
- When Black Hawk Technology B.V. has doubts regarding the veracity or adequacy of previously obtained customer identification data.
- When a series of linked transactions, individually below the threshold, cumulatively meet or exceed the NAf. 4,000 threshold.

For online casinos utilizing physical establishments to expand customer reach, Black Hawk Technology B.V. ensures that such establishments apply the same rigorous AML/CTF policies and procedures. Black Hawk Technology B.V. identifies and verifies the operator of the physical establishment, monitors their compliance, and regularly checks the proper implementation of its AML/CTF policies. All measures taken to guarantee compliance are meticulously documented.

The core CDD measures undertaken by Black Hawk Technology B.V. include:

5.4.1 Identification and Verification of the Player

Black Hawk Technology B.V. collects the following minimum personal details to establish a player's identity: full name, permanent residential address, date of birth, place of birth, nationality, and identity number. In lower-risk scenarios, identification may be limited to the full name, permanent residential address, and date of birth. For higher-risk situations, additional personal details may be collected to mitigate the elevated ML/FT risk.

Verification confirms the collected personal details using reliable, independent source documents, data, or information. As a general rule, verification is conducted by referencing an unexpired government-issued document containing a photograph (e.g., passport, identity card). If the primary document does not include the residential address, supplementary documents such as a bank statement, utility bill (fixed line telephone bills only), letter from a public authority, or rental agreement (not more than six months old) are obtained. Verification methods may include various reliable means to confirm identity and address. Documents presented for verification must be clear, legible, and of good quality. Extra scrutiny is applied to foreign documentation to verify authenticity. If Black Hawk Technology B.V. lacks sufficient assurance of a player's identity, additional verification measures will be implemented as deemed necessary.

5.4.2 Identification and Verification of the Beneficial Owner

Black Hawk Technology B.V. identifies and verifies the identity of the beneficial owner(s) in accordance with regulatory requirements. Black Hawk Technology B.V. ensures that players register and transact on their own behalf, with procedures in place to detect third-party activity. In situations involving syndicates, where funds are collected from multiple persons who share in winnings, these individuals are considered beneficial owners and are subject to identification and verification.

For business participants, such as companies hedging matchbook exposure or operators of physical establishments, Black Hawk Technology B.V. obtains satisfactory evidence to identify these entities and takes reasonable steps to verify the identity of their beneficial owners. This includes identifying natural persons holding 25% or more of shares or voting rights, or those exercising ultimate effective control. If no such natural person is identified, the natural person holding the position of senior managing official is identified.

5.4.3 Obtaining Information on the Purpose and Intended Nature of the Business Relationship

While the purpose of opening a gaming account is generally self-evident, Black Hawk Technology B.V. collects sufficient information to develop a comprehensive customer risk profile. This profile enables the detection of unusual activity throughout the business relationship. Information collected includes the customer's anticipated and actual level of activity, as well as their source of wealth (the origin of all accumulated money) and source of funds (how funds for a particular transaction were obtained).

The extent of information collected is proportional to the identified ML/FT risk. For lower-risk situations, a customer declaration with relevant details may be sufficient, supplemented by other available information. For higher-risk situations or when doubts arise, the information obtained is substantiated by independent and reliable documentation. Black Hawk Technology B.V. may utilize various data sources to develop customer behavioral models, ensuring direct source of wealth information is collected in high-risk scenarios.

5.4.4 Sanctions Screening and Politically Exposed Persons (PEP) Status Screening

All players are rigorously screened against sanctions lists published by the United Nations (UN) and the European Union (EU). Black Hawk Technology B.V. also incorporates any local lists of designated persons and organizations published by Curaçao authorities. The company ensures that it does not engage in business with any customer subject to international sanctions. Before

establishing a business relationship or performing an occasional transaction for the first time, Black Hawk Technology B.V. checks published lists of known or suspected terrorists and other sanctioned persons or companies, utilizing reliable and up-to-date resources.

For PEP status screening, Black Hawk Technology B.V. utilizes reliable and appropriate sources. Screening for PEP status is conducted at the onboarding stage and is regularly refreshed throughout the business relationship. If a player is identified as a PEP after onboarding, Black Hawk Technology B.V. implements enhanced measures within thirty days or terminates the relationship if these measures cannot be applied.

5.4.5 Timing of CDD Measures

Black Hawk Technology B.V. treats the opening of a gaming account as indicative of a business relationship with an element of duration. Verification of identity is completed when players engage in financial transactions equal to or exceeding NAf. 4,000. This implies that all CDD measures must be completed by the time this threshold is reached.

However, Black Hawk Technology B.V. applies a minimum level of CDD measures simultaneously with account opening, prior to the threshold being reached. This includes collecting minimum personal details (name, surname, permanent residential address, and date of birth) and conducting initial PEP status and sanctions screening. The NAf. 4,000 threshold is calculated on a daily basis, encompassing all deposits, withdrawals, and peer-to-peer transfers made by the player since the establishment of the business relationship. Once this cumulative threshold is reached, Black Hawk Technology B.V. proceeds with a full customer risk assessment and fulfills all remaining CDD obligations.

While CDD measures are being completed, customers may be allowed to continue using their gaming account. However, if the NAf. 4,000 threshold is reached due to a deposit, the player is prohibited from making further deposits or withdrawals, though they may continue to play with existing funds. If the threshold is reached due to a withdrawal request, a complete freezing of the account occurs, preventing further play.

If the requested information and documentation for CDD are not received within 30 days from the moment the NAf. 4,000 threshold was reached, Black Hawk Technology B.V. terminates the relationship with the player. If a presumption of money laundering or terrorist financing exists, a report is submitted to the FIU. If no such presumption exists, funds are returned to the same bank account or wallet from which they were originally deposited. Internal procedures dictate whether funds are blocked in cases of suspected money laundering, with careful consideration given to the risk of tipping off the customer.

5.4.6 Enhanced Due Diligence (EDD)

Black Hawk Technology B.V. applies Enhanced Due Diligence (EDD) measures for customers identified as presenting a higher risk of money laundering or terrorist financing. These measures are tailored to the specific risks identified and involve a more thorough and intensified level of scrutiny. EDD is particularly applied in situations such as:

- Relationships with residents of higher-risk geographic areas.
- Transactions or products that inherently favor anonymity.
- New products, business practices, delivery mechanisms, or technologies, both new and pre-existing.

Examples of EDD measures implemented by Black Hawk Technology B.V. include obtaining additional information, conducting more intensive monitoring, and requiring specific transactional controls as appropriate for the heightened risk.

In higher ML/TF risk scenarios, Black Hawk Technology B.V. periodically requests source of funds information, even in the absence of a change in the customer's typical transactional patterns or activity.

5.4.7 Simplified Due Diligence (SDD)

Where the Customer Risk Assessment indicates a demonstrably lower risk of money laundering or terrorist financing, Black Hawk Technology B.V. is permitted to apply Simplified Due Diligence (SDD) measures. These measures are proportionate to the reduced risk and are designed to streamline the CDD process without compromising compliance effectiveness. Examples of SDD measures include:

- Limiting the collection of specific personal information. For instance, in low-risk scenarios, identification may be limited to the customer's full name, permanent residential address, and date of birth.
- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship, rather than strictly prior.
- Adapting the extent of verification to the perceived risk, potentially allowing the use of alternative reputable information sources even if they do not contain photographic evidence.
- Limiting the scope of personal details to be verified, focusing on basic identification details while other details are verified at the discretion of Black Hawk Technology B.V., provided sufficient comfort in knowing the customer's identity is maintained.
- Reducing the frequency of customer identification data updates.
- Decreasing the degree of ongoing monitoring and transaction scrutiny, based on a reasonable monetary threshold.

It is imperative to note that Simplified Due Diligence measures are never applied when there is any suspicion of money laundering or terrorist financing, or when specific higher-risk scenarios are present.

5.4.8 Application of CDD Measures to Existing Customers

Black Hawk Technology B.V. applies CDD measures to its existing customer base on a risk-sensitive and materiality basis, conducting due diligence reviews at appropriate intervals. Black Hawk Technology B.V. continuously assesses whether its current procedures are sufficient to meet the CDD obligations outlined in this policy. If existing procedures are deemed adequate, they continue to be applied, with particular attention paid to ongoing monitoring obligations. If, however, Black Hawk Technology B.V. previously lacked procedures to meet current CDD requirements, these are implemented on a risk-sensitive basis, and due diligence is conducted on existing relationships at appropriate times to ensure full compliance.

5.4.9 Termination of the Business Relationship

If Black Hawk Technology B.V. is unable to fulfill the obligations arising from its Customer Due Diligence process, it will not establish a business relationship or perform the requested transaction. In such circumstances, Black Hawk Technology B.V. is obliged to terminate the

business relationship with the customer. A meticulous record is maintained of all attempts made to obtain the necessary information and documentation. Black Hawk Technology B.V. may decide to either close the account entirely or keep it blocked and suspended.

Should the customer subsequently provide the requested information and/or documentation after the account has been closed or suspended, Black Hawk Technology B.V. assesses whether the delay in providing the CDD documentation affects the ML/FT risk associated with the business relationship. The mere reluctance of a customer to provide CDD information is not automatically equated to a suspicion of ML/FT. Black Hawk Technology B.V. considers all available factors and information to determine if there are grounds for suspicion. If a presumption of ML/FT exists, Black Hawk Technology B.V. submits an unusual transaction report to the FIU concerning the player.

Where there is no reason for the retention of funds, the funds are remitted back to the player, strictly through the same channels used to receive the funds. If a presumption of money laundering or terrorist financing exists, Black Hawk Technology B.V.'s internal procedures dictate whether the funds are blocked, always considering the risk of tipping off the customer.

5.5 Ongoing Monitoring

Black Hawk Technology B.V. conducts continuous ongoing due diligence on all business relationships and meticulously scrutinizes transactions undertaken throughout the course of those relationships. This critical measure ensures that all transactions are consistent with the casino player's known business and risk profile, including, where necessary, the source of funds.

5.5.1 Ongoing Monitoring of Identity

Black Hawk Technology B.V. is committed to maintaining accurate and up-to-date identification data for all its customers. Recognizing that identity information may change over time, Black Hawk Technology B.V. has established procedures to detect and re-evidence such changes. This involves implementing procedures to periodically review and update identification data, and refresh information upon key events or expiry. Black Hawk Technology B.V. determines, on a risk-sensitive basis, whether changes are substantial enough to necessitate a re-assessment of the customer's risk profile within the business relationship.

5.5.2 Ongoing Monitoring of Transactions

Transaction monitoring is a core component of Black Hawk Technology B.V.'s AML/CTF framework, designed to prevent the company's involvement in illicit activities and to safeguard its reputation. Through ongoing scrutiny of transactions, Black Hawk Technology B.V. identifies any activity that deviates from what is known or expected of the customer based on their established profile. When inconsistencies are detected (e.g., deviations from the declared source of funds, average profile, or historical account activity), Black Hawk Technology B.V. investigates the reason for such deviations and obtains sufficient information and documentation regarding the transaction.

This investigative process may lead to a revision of the customer's risk profile. Following the collection of additional information, Black Hawk Technology B.V. determines whether the transaction constitutes an unusual transaction and requires reporting to the FIU. The intensity and frequency of ongoing monitoring are directly correlated with the customer's risk profile;

even in low-risk situations, a degree of oversight is maintained to ensure the business relationship continues to be classified as low risk.

5.6 Reliance on Third Parties to Perform Customer Due Diligence

Black Hawk Technology B.V. may rely on qualified third parties to perform certain elements of its Customer Due Diligence (CDD) measures, specifically the identification of the player, identification of the beneficial owner, and obtaining information on the purpose and intended nature of the business relationship. This reliance is strictly conditional upon meeting specific criteria to ensure regulatory compliance and maintain the integrity of the CDD process.

The criteria for reliance on third parties are as follows:

1. **Immediate Information Access:** Black Hawk Technology B.V. must obtain the necessary CDD information (elements a-c) immediately from the third party it is relying upon.
2. **Agreement and Testing:** A formal agreement must be in place with the third party, ensuring that copies of identification data and other relevant CDD documentation will be made available to Black Hawk Technology B.V. upon request. This arrangement is periodically tested to confirm its functional effectiveness. It is crucial to note that Black Hawk Technology B.V. retains ultimate responsibility for conducting the customer-based risk assessment, determining whether a customer is a Politically Exposed Person (PEP), and conducting ongoing monitoring.
3. **Regulatory Oversight of Third Party:** Black Hawk Technology B.V. must satisfy itself that the third party is regulated, supervised, or monitored for compliance with CDD and record-keeping requirements that are consistent with Curaçao regulations. The third party must also have an existing business relationship with the customer that is independent of the relationship to be formed with Black Hawk Technology B.V., and it must apply its own procedures to perform CDD measures.
4. **Country Risk Assessment:** When selecting countries where such third parties can be based, Black Hawk Technology B.V. considers available information on country risk levels, prioritizing jurisdictions with robust AML/CTF regimes.

This reliance differs from outsourcing or agency arrangements, where the outsourced entity acts directly on Black Hawk Technology B.V.'s behalf and procedures. Black Hawk Technology B.V. retains ultimate responsibility for compliance and conducts periodic assessments of service providers. Critical decisions regarding customer onboarding or relationship continuation based on risk are not outsourced.

Any activity performed by an agent or a group company is considered an activity performed by Black Hawk Technology B.V. itself. Consequently, any customer onboarded by an agent or group company must undergo the same rigorous checks and controls as customers onboarded directly by Black Hawk Technology B.V. It is therefore Black Hawk Technology B.V.'s responsibility to ensure that its AML/CTF controls, policies, measures, and procedures are consistently applied by any agent or group company.

5.7 Reporting of Unusual Transactions

Black Hawk Technology B.V. has established robust procedures for the detection, documentation, and reporting of unusual transactions, whether intended or completed, to the Financial Intelligence Unit (FIU) Curaçao. These procedures are critical for fulfilling Black Hawk

Technology B.V.'s obligations under the National Ordinance on the Reporting of Unusual Transactions (NORUT).

5.7.1 Recognition of Unusual Transactions

The ability to recognize an unusual transaction or series of transactions hinges upon having sufficient knowledge of the player and their established customer profile. This profile, built from collected player information, allows Black Hawk Technology B.V. to anticipate expected behavior and readily identify deviations. Black Hawk Technology B.V.'s management provides specific guidance and comprehensive training to all staff members on recognizing and adequately documenting unusual transactions, based on both objective and subjective indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions. All internally identified unusual transactions are reported to the compliance officer in a management-approved format, accompanied by all available supporting documents, such as copies of identification documents, cash-out slips, and other relevant records. If the compliance officer or management decides not to report an internally identified unusual transaction to the FIU, the reasons for this decision are thoroughly documented and formally signed off.

Black Hawk Technology B.V. pays special attention to all complex, unusually large transactions, and any unusual patterns of transactions that lack apparent economic or visible lawful purpose, in line with FATF Recommendation 11.

5.7.2 Indicators of Unusual Transactions

The following transactions or intended transactions are deemed unusual and trigger reporting obligations:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice.
- Transactions by or on behalf of a natural or legal person, a group, or an entity named on a list adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55).
- Transactions in the amount of NAf. 5,000 or more, regardless of whether the transaction is made in cash, by check, other forms of payment, or through electronic or other non-physical means. This includes, but is not limited to:
 - A cashless transaction in the amount of NAf. 5,000 or more. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
 - Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client.
 - Sale to a customer of chips (including tokens and credits) in the amount of NAf. 5,000 or more.
 - A cash out in the amount of NAf. 5,000 or more (this includes credit card and e-wallet transactions).
 - *Note:* A transaction may be a single transaction, or a series, combination, or pattern of transactions involving a total amount equivalent to NAf. 5,000 or more, considered per gaming day.
- Presumed money laundering transactions or terrorist financing: transactions where there is cause to presume, they can be related to money laundering or terrorist financing.

5.7.3 Reporting and Record Keeping

Black Hawk Technology B.V. will register with the FIU and obtain access to the goAML reporting portal. The compliance officer prepares reports of all unusual transactions for external submission to the FIU in accordance with FIU reporting regulations. Black Hawk Technology B.V. liaises with the FIU regarding reporting mechanisms, including potential for bulk reporting services.

Black Hawk Technology B.V., its directors, officers, and employees are legally protected from criminal and civil liability for any breach of information disclosure restrictions when reporting to the FIU. Black Hawk Technology B.V. maintains all necessary records on transactions (both domestic and international) for at least five years to facilitate information requests from competent authorities. These records are sufficient to reconstruct individual transactions and provide evidence for criminal activity prosecution if required. All records obtained through CDD measures (e.g., copies of identification documents), account files, and business correspondence are retained for at least five years after the business relationship terminates or after the date of an occasional transaction. CDD information and transaction records are made available to domestic competent authorities upon appropriate legal authority.

5.7.4 Prohibition of Disclosure (Tipping-Off)

Black Hawk Technology B.V., its senior management, and employees are strictly prohibited from disclosing any details or information related to a report filed with the FIU or a request for information made by the FIU. This prohibition extends to the customer and any third parties. The rationale behind this is to prevent jeopardizing any analysis or investigation into money laundering or terrorist financing. Caution is exercised when taking actions such as terminating a relationship or blocking additional transactions following a report to the FIU, as unjustified drastic action may alert the player. In such circumstances, increasing ongoing monitoring and submitting additional reports to the FIU on any other suspected instances of ML/TF is often a more advisable course of action.

5.8 Anti-Money Laundering Compliance Program

Black Hawk Technology B.V. maintains a comprehensive Anti-Money Laundering (AML) Compliance Program, recognized as an essential component of its regulatory compliance regime. The overarching goal of this program is to robustly protect Black Hawk Technology B.V. against money laundering and to ensure full adherence to all relevant laws and regulations. The AML program is inherently risk-based, meticulously designed to identify and mitigate the specific money laundering and terrorist financing risks that Black Hawk Technology B.V. may encounter in its operations. It establishes minimum standards for the organization that are reasonably designed to comply with applicable Curaçao laws and regulations.

The AML program is an organization-wide initiative, supplemented by detailed policies and procedures, developed with a comprehensive understanding of Curaçao's legal and regulatory requirements. The program systematically ensures that all obligations regarding customer due diligence, reporting of unusual transactions, data retention periods, data protection, and employee training are consistently met.

Black Hawk Technology B.V. regularly tests its AML program systematically and adapts it to address current and emerging risks within the company's own operational environment. The

AML program has received formal approval from Black Hawk Technology B.V.'s senior management. Furthermore, Black Hawk Technology B.V. ensures that any foreign branches and subsidiaries implement AML/CTF measures that are fully consistent with the robust requirements established by Curaçao.

The basic elements that Black Hawk Technology B.V.'s AML Compliance Program addresses are:

5.8.1 A System of Internal Policies, Procedures, and Controls

Black Hawk Technology B.V. has established a comprehensive system of internal policies, procedures, and controls. This system includes a clearly articulated policy statement that expresses Black Hawk Technology B.V.'s unwavering commitment to combating the abuse of its facilities, products, and services for money laundering and terrorist financing purposes. These policies explicitly reference current anti-money laundering and combating the financing of terrorism legislation and regulations, particularly the NOIS, NORUT, Sanctions National Ordinance, and Kingdom Sanction Act, thereby setting the tone for the entire organization.

Standard AML operating procedures translate policy principles into practical guidelines for daily operations. Black Hawk Technology B.V. has a robust process in place to continuously monitor and adapt to regulatory changes, ensuring that its AML program remains current and effective. While policies and procedures provide essential guidance, the AML program also relies on a variety of internal controls. These controls are designed to enable the compliance officer to readily recognize any deviations from standard procedures and protocols. All anti-money laundering policies and procedures are documented in writing, formally approved by senior management or the Senior Management, and effectively communicated to all employees.

5.8.2 The Appointment of a Compliance Officer

Black Hawk Technology B.V. has formally designated a senior officer at a management level, operating independently from the games operations, to serve as the AML/CTF compliance officer. This individual is entrusted with the critical responsibility for the detection and deterrence of money laundering and terrorist financing activities within the organization. The AML/CTF compliance officer is granted timely and unfettered access to customer identification data, other CDD information, transaction records, and all other relevant data necessary to perform their duties effectively. The officer's independence is paramount to ensuring objective oversight and decision-making.

The responsibilities assigned to Black Hawk Technology B.V.'s compliance officer include, but are not limited to:

- Designing and implementing the AML program.
- Verifying adherence to local laws and regulations concerning the detection and deterrence of money laundering and terrorist financing.
- Reviewing compliance with established policies and procedures.
- Organizing and overseeing training sessions for staff on various compliance-related issues.
- Analyzing transactions and verifying whether any are subject to reporting based on the indicators outlined in the Ministerial Decree regarding Unusual Transactions.
- Reviewing all internally reported unusual transactions for completeness and accuracy, cross-referencing with other sources.

- Maintaining comprehensive records of both internally and externally reported unusual transactions.
- Designing and implementing an internal procedure for when the reporting of unusual transactions will lead to blocking or freezing user accounts, carefully considering the risk of tipping off the player.
- Executing closer investigations of unusual transactions when deemed necessary.
- Preparing external reports of unusual transactions for submission to the FIU.
- Making necessary adjustments and improvements to the AML program based on identified needs or regulatory changes.
- Staying continuously informed on local and international developments in money laundering and terrorist financing trends and proactively suggesting improvements to management.
- Reporting to senior management on the risks of money laundering and terrorist financing.

These responsibilities are explicitly detailed within the compliance officer's job description, which is formally signed and dated by the officer, signifying acceptance of the entrusted duties.

5.8.3 Employee Screening Program and Ongoing Employee Training Program

Black Hawk Technology B.V. is committed to conducting its business with the highest ethical standards and ensuring strict adherence to all laws and regulations pertaining to financial transactions. To this end, Black Hawk Technology B.V. has established and rigorously follows proper policies and procedures for screening its employees for criminal records.

Black Hawk Technology B.V. develops and provides comprehensive training programs to all personnel who handle transactions that may be classified as unusual, based on the indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions. This training encompasses setting out clear rules of conduct governing employee behavior and fostering continuous education to build strong awareness against money laundering and terrorist financing. Training is provided across most areas of the institution, with content tailored to the specific roles and responsibilities of each segment.

Training topics are tailored to specific roles and responsibilities, covering essential aspects for new employees, customer-facing personnel, audit staff, AML compliance staff, supervisors, managers, and senior management.

Refreshment training sessions are conducted at regular intervals to ensure that all staff members remain informed of current and new developments regarding money laundering and terrorist financing techniques, methods, and trends. To demonstrate compliance with these staff training guidelines, Black Hawk Technology B.V. meticulously maintains records that include: details on the content of training programs, names of trained staff members, dates of training, results of any testing to measure staff understanding, and an ongoing training plan.

5.8.4 An Independent Audit Function to Test the AML Program

Black Hawk Technology B.V.'s AML compliance program is subject to rigorous monitoring and evaluation at least annually by an adequately resourced internal audit department or a qualified outside independent party. The audit function is strictly independent, meaning it is performed by individuals who are not involved with the organization's AML compliance staff or daily

operations. Those conducting the audit are sufficiently qualified and possess relevant experience and certifications.

The independent audit includes, at a minimum, the following tests:

- Review of money laundering and counter-terrorist financing manuals.
- Assessment of compliance management effectiveness.
- Performance of transaction testing to identify potential anomalies or non-compliance.
- Assessment of the adequacy and effectiveness of training programs.
- Evaluation of compliance with all applicable laws and regulations.
- Evaluation of the compliance officer's performance.
- Interviews with employees who handle transactions and with their supervisors to gauge understanding and adherence to procedures.
- A sampling of unusual transactions, both at and beyond established thresholds, followed by a review of compliance with internal and external policies and reporting requirements.
- An assessment of the adequacy and integrity of the record retention system.

The audit team also assesses the responsiveness of the Senior Management to previous audit findings. The scope of the testing and the detailed testing results are thoroughly documented. Any identified deficiencies are promptly reported to senior management and/or the Board of Supervisory Directors, as well as to the designated officers, with a clear request for prompt corrective actions to be taken by a specified deadline. These corrective actions may include, but are not limited to, the enhancement of existing controls and procedures.

6. Compliance and Consequences of Non-Compliance

Adherence to this AML/CTF Policy is mandatory for all Black Hawk Technology B.V. personnel and associated entities. Violation of the laws and regulations underpinning this policy, including the NOIS, NORUT, Sanctions National Ordinance, and Kingdom Sanction Act, exposes Black Hawk Technology B.V. to significant administrative and criminal sanctions. Non-compliance may lead to severe penalties, including substantial fines, revocation of licenses, and reputational damage. Individual non-compliance by employees may result in disciplinary action, up to and including termination of employment, and where applicable, criminal or civil penalties under relevant laws. Black Hawk Technology B.V. is committed to fostering a culture of compliance where all stakeholders understand their responsibilities and the critical importance of preventing financial crime.

7. Related Information

This policy should be read in conjunction with, and is supported by, the following internal Black Hawk Technology B.V. documents and external regulatory frameworks:

- Black Hawk Technology B.V. Customer Onboarding Protocols
- Black Hawk Technology B.V. Risk Management Framework
- Black Hawk Technology B.V. Escalation Procedures
- Black Hawk Technology B.V. Suspicious Activity Reporting Processes
- Curaçao Gaming Authority (CGA) Regulations for the combating of Money Laundering and the Financing of Terrorism (January 2025)
- National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 no. 92)
- National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2017 no.99)

- Sanctions National Ordinance (N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- 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)

8. Contact Information

For any questions or clarifications regarding this policy, please contact:

Black Hawk Technology B.V. Compliance Department

Phone: Nil

Email: compliance@bk8.com

9. Policy History

This is a new policy document for Black Hawk Technology B.V., effective as of the date indicated above.

Version	Effective Date	Revisions
1.0	31 March 2025	Initial Policy Document

10. Policy URL (if applicable)

Nil