



Date	Version	Author	Summary Changes
26.05.2025	1.0	Trust & Safety Corp B.V.	New version of ANTI-MONEY LAUNDERING POLICY

Table of Content

STATEMENT.....	2
PURPOSE.....	2
AUDIENCE	3
REFERENCE DOCUMENTS	3
DEFINITIONS	4
POLICY IMPLEMENTATION	6
RISK BASED APPROACH	7
BUSINESS RISK ASSESSMENT	7
CUSTOMER RISK ASSESSMENT	8
CUSTOMER ACCEPTANCE POLICY	9
10.1 RESTRICTED JURISDICTIONS	11
10.2 ACCOUNT ESCALATION AND REVIEW	11
10.3 SANCTIONS SCREENING	12
10.4 DOCUMENT RETENTION.....	12
CUSTOMER DUE DILIGENCE	12
ONGOING MONITORING.....	13
REPORTING OF UNUSUAL TRANSACTIONS	14
ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	15
COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	16



Statement

Trust & Safety Corp B.V., a limited liability company incorporated under the laws of Curaçao, with the company number 146616, having registered office at Korporaalweg 10. The management of Trust & Safety Corp B.V. is committed to combat the abuse of the Company's services for the purpose of Money Laundering, Terrorist Financing, Financing Proliferation.

This AML Policy outlines the framework adopted by Trust & Safety Corp B.V. to prevent its operations from being used for money laundering or financing of terrorism. The policy applies to all business units, employees, agents, and third-party partners involved in customer-facing and back-office operations. To facilitate compliance the Company has implemented a risk-based compliance program consisting of the following pillars:

Establishing policies, procedures and internal controls designed to prevent the business from being used to facilitate ML or other criminal activities and to ensure compliance with applicable reporting requirements.

Appointment of a senior CO/MLRO having sufficient knowledge, authority and resources to oversee the Company's AML program.

Employee screening program and ongoing employee training program.

A system of independent testing of the AML/CFT/CFP policies and procedures in place to ensure their effectiveness.

Purpose

The Company developed internal security measures to prevent money laundering and terrorist financing. The key features of these measures aim to stay aware of high-risk customers and detect suspicious activity, including the predicate offenses to money laundering and terrorist financing.

The purpose of this document is to establish the policies, measures and controls designed to reasonably ensure that money laundering and terrorist financing transactions are prevented from occurring or are detected on a timely basis by the company.



Audience

Trust & Safety Corp B.V. is a licensed and regulated gaming operator offering gambling services to end customers. The Company recognizes the money laundering risks that are inherent to gaming and has therefore enacted this policy. This policy has been approved by the Management of the Company.

This policy applies to all activities, products and employees of the Company, including the Company's officers, directors, full-time employees, part-time employees, temporary employees, or contractors employed by the Company or affiliates of the Company, as well as the Company's third-party service providers as relevant. Such individuals will be provided with regular training to ensure awareness of this policy and their obligations under it, at least on an annual basis or more frequently as required.

Reference Documents

The Company's Policy were created subject to the relevant applicable legislation, in particular (but not limited to):

- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Money Laundering (P.B. 1993, no. 52);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92),
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99),
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);



- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015, no. 30);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees (N.G. 2018, no. 34);
- National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);
- National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);

Definitions

Adverse Media

Negative information found in publicly available sources, such as news reports, regulatory filings, and investigative publications, that may indicate a customer's involvement in financial crime, corruption, or other illicit activities.

Compliance Officer/Money Laundering Reporting Officer (MLRO)

A senior employee responsible for overseeing the implementation and ongoing maintenance of the bank's AML/CFT compliance program, ensuring strict adherence to regulatory requirements, and acting as the primary liaison with regulatory bodies. The MLRO is also responsible for managing the bank's AML compliance, including filing reports with FINTRAC and ensuring the institution's full compliance with AML/CFT regulations.

Customer Due Diligence (CDD)

The process of identifying and verifying a customer's identity, assessing their risk profile, and conducting ongoing monitoring to detect suspicious activity.

**Enhanced Due Diligence (EDD)**

Additional scrutiny applied to high-risk customers, such as Politically Exposed Persons (PEPs) and businesses operating in high-risk sectors, to ensure comprehensive risk assessment and monitoring.

Geographic Risk

The risk posed by a customer or transaction due to its association with a jurisdiction known for high levels of financial crime, weak regulatory controls, or inclusion on lists published by the Financial Action Task Force (FATF).

Know Your Customer (KYC)

A regulatory requirement that mandates financial institutions to verify the identity of their customers, assess their risk level, and monitor their financial activities.

Politically Exposed Person (PEP)

An individual who holds or has held a prominent public position, such as a government official, senior executive of a state-owned enterprise, or high-ranking military officer, along with their family members and close associates.

Risk-Based Approach (RBA)

A methodology that financial institutions use to allocate resources and apply controls based on the level of money laundering and terrorist financing risks posed by customers, products, services, and jurisdictions.

Sanctions Screening

The process of verifying customers and transactions against international and domestic sanctions lists.

Suspicious Transaction Report (SAR)

A report submitted to FIU when a transaction is deemed suspicious based on unusual patterns, lack of economic justification, or potential links to money laundering or terrorist financing.



Transaction Monitoring

The ongoing process of analyzing customer transactions to detect potentially suspicious activity, such as unusual transaction patterns, large wire transfers, or structuring.

Supervisory Board

Oversees the governance. Approves the risk appetite and compliance framework. Receives periodic compliance and AML/CFT reporting.

Managing Board / CEO

Responsible for day-to-day management. Ensures adequate resources, systems, and personnel are in place for AML/CFT compliance. Signs off on key compliance policies.

Compliance Manager (MLRO)

Reports directly to the Managing Board and Supervisory Board. Owns the AML/CFT compliance framework and risk register. Approves High-Risk customers and ensures compliance with STR submissions. Ensures alignment with regulatory obligations.

Policy Implementation

The Company will follow applicable directives issued in conjunction with the necessary regulatory bodies to prevent ML, TF, FP, sanction violations, and other criminal activity. The Company will not engage in activities related to these activities or involving any person or business who is under US, UN, or EU sanctions or a partner's prohibited countries or watchlists or involving any country or region subject to comprehensive US sanctions.

The Company has a four-stage risk-based approach to combatting ML, TF, FP sanctions violations, and other criminal activity:

A. Identification: Identifying the Company's products and services could be used for money laundering and/or terrorist financing;



B. Documentation: Ensuring that the Company has clear and well documented policies and procedures in place for employees to understand the risks, to know what to look for, and to know how to report any unusual activity;

C. Mitigation: Implementing strong measures and defense mechanisms to prevent money laundering, terrorist financing, and other criminal activity from occurring in the first place or enabling the Company to detect and report such occurrences if they do happen; and

D. Monitoring: Closely monitoring identified risks and mitigating them by using the established measures on an ongoing basis and, where necessary, adjusting to any changes

Risk Based Approach

Based on the FATF Recommendations, igaming companies are required to apply a Risk-based Approach to ensure that measures to prevent or mitigate money laundering, financing of terrorism and proliferation of weapons are commensurate with the risks identified.

Applying Risk-based Approach means that the Company:

- Assess the risks that money laundering or terrorist financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Document their risk assessments, including everything that has been done and the reason for this being done.

Given that risks are dynamic, the Company subscribes to continuously monitor the effectiveness of these policies, procedures, and controls, making necessary adjustments as needed. The risk assessment must also be made available to the CGA upon request

Business Risk Assessment

The Company conducts a comprehensive Business Risk Assessment (BRA) to identify and evaluate its exposure to ML, TF, FP and sanctions risks. The assessment ensures that AML/CFT



controls are commensurate with the risks associated with the Company's operations, products, services, customer base, and geographical footprint.

The BRA is reviewed annually and upon any material change to business operations or regulatory obligations. The BRA includes the following key areas:

- **Product and Service Risk:** Evaluation of the ML/TF risks inherent in the Company's gaming offerings (e.g., online poker, sports betting, and virtual currency). Particular focus is placed on features allowing for rapid fund movement or cashout without proportional gameplay.
- **Customer Risk:** Classification of customers by risk levels based on geographic origin, payment behavior, funding methods, and whether they are high-net-worth individuals, Politically Exposed Persons (PEPs), or associated with high-risk industries.
- **Geographic Risk:** Analysis of exposure to countries listed by FATF, OFAC, or other relevant authorities as non-cooperative or high-risk, as well as jurisdictions with weak AML/CFT systems or under international sanctions.
- **Transactional Behavior Risk:** Detection of patterns such as minimal gaming activity before large withdrawals, unusual use of bonuses, or frequent account top-ups followed by inactivity. Findings from the BRA are documented and used to inform risk-based procedures and customer due diligence protocols. The effectiveness of controls derived from this assessment is validated through internal audits, transaction monitoring results, and independent testing

Customer Risk Assessment

The Customer Risk Assessment (CRA) is an essential element of the Company's risk-based approach, aimed at evaluating the ML/TF risk posed by individual customers. It informs the level of due diligence, ongoing monitoring, and other controls applied to each customer.

Each customer is assigned a risk rating (Low, Medium, High, or Very High) based on a set of risk indicators:

Identification and Verification Data: Including full name, address, date of birth, and documentary or non-documentary verification.

Behavioral Factors: Transaction volumes, frequency of deposits and withdrawals, and patterns of gameplay versus monetary activity.



Geographic Indicators: Whether the customer is based in or connected to high-risk or sanctioned jurisdictions.

Payment and Funding Sources: Use of crypto-assets, pre-paid cards, or anonymous funding methods increase risk; documented employment income or regulated bank transfers lower risk.

Third-party Data: Alerts or insights from vendors (sanctions and PEP screening, blockchain transaction tracing).

CRA is initiated at account creation and continuously updated based on the customer's activity and external inputs. Triggers for re-evaluation include:

- Cumulative deposits exceeding defined thresholds (e.g., \$2,000 or Cg. 4,000, whichever is less).
- Document KYC Verification.
- Attempted withdrawals or redemptions.
- Alerts from internal or third-party systems.

High-risk customers undergo Enhanced Due Diligence (EDD), including documentation on source of wealth and intended usage of the platform.

The CRA informs decisions on whether to escalate accounts, impose restrictions, or file unusual transactions to the FIU.

Customer Acceptance Policy

The Customer Acceptance Policy (CAP) sets forth the onboarding requirements and thresholds for escalating due diligence procedures based on CRA outcomes.

The Company uses a **three-tiered** Customer Identification and Verification system:



Level 1: Account Creation Required: Email address.

Purpose: Establish account credentials and provide CIP notification.

Limitations: No monetary transactions permitted.

Level 2: Customer Due Diligence (CDD)

Triggered by: First attempted deposit or wager.

Required Information:

- First and Last Name
- Phone Number
- Full Residential Address (no P.O. Boxes; APO/FPO acceptable)
- Date of Birth
- Government-issued ID Verification (subject to specific policies and management's discretion); The user-provided information must be verifiable by third-party vendors (including Sardine A.I. and Chainalysis) prior to transacting above the prescribed limits and can be provided in two ways: either as photos of government issues, unexpired IDs/selfie uploads (documentary), or as text inputs (non-documentary) when made available.

Level 3: Enhanced Due Diligence (EDD) Triggered by:

- Withdrawal attempts or redemptions
- Cumulative deposits exceeding \$2,000 or (Cg. 4,000, whichever is less)
- Behavioral red flags or vendor alerts Additional Requirements:
- Documentary proof of address (e.g., utility bill or bank statement)
- Source of wealth/income documentation for high-risk accounts, if applicable
- Explanation of transactional behavior or relationships, if applicable All KYC information must be verifiable via approved third-party providers before the customer is allowed to transact beyond set limits



10.1 Restricted Jurisdictions

The Company prohibits customers from countries under comprehensive sanctions and on the FATF's High-Risk Jurisdictions subject to a Call for Action list (e.g., Iran, North Korea, Syria, Myanmar) and maintains:

- A Non-Supported Countries List
- A Prohibited Jurisdictions List for monitoring and reference

10.2 Account Escalation and Review

High-risk accounts are subject to Compliance approval.

Customers that are classified as PEP are per default considered high risk customers. PEPs are subject to management approval.

The term "Politically Exposed Persons" is broad and generally includes all persons who fulfill a prominent public function.

This includes:

- Heads of State, Heads of Government, Ministers, Deputy and Assistant Ministers, and Parliamentary Secretaries;
- Members of Parliament;
- Members of the Courts of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors, Audit Committees or of the boards of central banks;
- Ambassadors, charge d'affaires and other high-ranking officers in the armed forces; and
- Members of the administration, management or boards of State-owned corporations.

The term "immediate family members" of PEPs includes:

- The spouse, or any partner recognized by national law as equivalent to the spouse;
- The children and their spouses or partners; and
- The parents.



10.3 Sanctions screening

The Company is committed to complying with all applicable sanctions, including U.S. UN, and EU sanctions

10.4 Document Retention

All customer information and due diligence records are maintained for at least ten years from the date of collection or account closure, whichever is later.

Customer Due Diligence

The Company is prohibited from keeping anonymous accounts or accounts in obviously fictitious names. It must identify the player and ask for the player's name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge, the Company may not establish or maintain a business relationship or carry out occasional transactions. A sound CDD program is the best way to prevent AML, TF & FP.

The customer's risk profile is essential to apply a certain level of CDD commensurate to the identified ML/TF risk. The purpose of collecting information is to assess the risk that may be associated with the player and to build a customer profile to assess how the player is going to act within the framework of the business relationship. Such an assessment is necessary in order to detect deviations from the expected behavior, which are reported to the FIU.

The obligation to undertake CDD measures when:

- When players engage in financial transactions equal to or above Cg 4,000 or equivalent EUR 2,000;
- carrying out occasional transactions above the monetary equivalent of EUR 2,000;
- there is a suspicion of money laundering or terrorist financing; or
- there are doubts about the veracity or adequacy of previously obtained customer identification data.

Note: a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of EUR 2,000.



For transaction above the monetary equivalent of EUR 2,000, CDD measures are applied immediately. Whether the transaction is carried out in a single operation or in several operations which appear to be linked. Transactions are considered as linked if they are carried out by the same customer through the same game or in one gaming session. A transaction consists of the wagering of a stake or the collection of winnings.

The CDD measures to be taken are as follows:

- a. Identifying the player documents, data or information;
- b. Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the player, its business and risk profile, including, where necessary, its source of funds.

Ongoing Monitoring

The Company will continuously monitor customer transactions to detect any suspicious activity and, based on the level of risk, will maintain and update customer information, including details about the beneficial owners of legal entity customers. This monitoring will use the customer's risk profile as a reference point to evaluate activity and determine whether a transaction is potentially concerning.

Monitoring will be conducted through a combination of automated systems and manual review, utilizing internal tools, vendor-generated reports, and referrals from partners such as card networks and financial institutions. By integrating technology with human analysis, the Company aims to ensure comprehensive oversight.

The objectives of the transaction monitoring process are to ensure:

- A methodology aligned with customer risk levels;
- B. An effective and skilled review procedure;
- C. A reliable process for escalating concerns;
- D. The timely identification and reporting of unusual or suspicious activity.



The Compliance Department is responsible for overseeing this process. It will assess all flagged activity, determine whether further investigation or action is required, and ensure proper documentation of the monitoring procedures, findings, and decisions.

Reporting Of Unusual Transactions

The Company will report any unusual transactions to the Curacao FIU if they're believed to be involved in potential money laundering. To protect the Compliance department, the AML Compliance Person ensures The Company personnel can report violations of the Program anonymously. Employees engaging with customers or accessing customer information will receive anti-money laundering (AML) training to recognize unusual or potentially suspicious behaviors. If employees suspect involvement with proceeds of crime, they must submit an Internal Unusual Activity Report (IUAR) to the AML Compliance Person within 24 hours. The AML Compliance Person will investigate and determine if a report to the Financial Intelligence Unit (FIU) of Curaçao is warranted within 48 hours.

The Company staff will be trained to identify unusual transactions based on customer profiles and specific indicators. All unusual transactions must be reported to the CO in an approved format, accompanied by supporting documentation.

Unusual transactions include:

- A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- A transaction amounting to Cg. 5,000.00 or more (equivalent EUR 2,450), regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:

1. A cashless transaction in the amount of Cg. 5,000.00 or more.
2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.



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

Please note that indicators (a) to (c) are referred to as “objective indicators”, while (d) is referred to as “subjective indicator”. While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

The AML Compliance Person further ensures that this mechanism is well publicized to all personnel and will take necessary steps to ensure reports of potential violations remain anonymous and confidential. Regardless of whether a report is made anonymously, The Company has zero tolerance for retaliation against an employee for reporting a potential violation up to and including termination. All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

Further, the Company will retain copies of all actions, decisions, and processes outlined in this document for a minimum of seven years. The records will be electronically stored, to be printed as a hard copy when necessary. The records will also be organized in a manner that facilitates easy retrieval to enable reporting to the Curacao FIU without undue delay

Anti-Money Laundering Compliance Program

The compliance program developed by the company includes the following measures:

- A system of internal policies, procedures and controls: The company maintains AML/CTF policies and procedures to prevent its facilities, products, and services from being misused for money laundering, terrorist financing, and weapons of mass destruction proliferation (AML/CTF/PF). These are developed in adherence to current AML/CTF legislation, covering aspects such as due diligence, unusual transaction reporting, and transaction record management, among other established controls.
- A designated compliance officer with day-to-day oversight over the AML program: The Compliance Officer enjoys absolute autonomy and independence in the exercise of their



responsibilities and functions. Their principal duties include:

- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing.
 - To organize training sessions for the staff on various compliance-related issues
 - To keep records of internally and externally reported unusual transactions;
 - To design an internal procedure about when reporting of unusual transactions will lead to blocking/ freezing of user accounts, taking into account the risk of tipping off the customer.
 - To prepare the external report of unusual transactions.
 - To make necessary changes to the AML program.
- An employee screening program and ongoing employee training program: The Compliance Officer will develop a training program for the company's employees. This program aims to raise awareness among senior management, department heads, and all other employees regarding the importance of combating money laundering and the financing of terrorism, as well as the prevention mechanisms established by the company.

These training sessions will be conducted at least twice a year, and attendance is mandatory. Non-attendance will be considered an offense in accordance with the Internal Labor Regulations. Training may be delivered through physical or electronic means, as deemed appropriate. Furthermore, certificates of completed training will be included in the employee's personnel file

- An independent audit function to test the AML program: The compliance program is supervised and evaluated annually by a department independent of the company's AML compliance unit.

The results are documented and brought to the attention of General Management and the shareholders. Corrective measures, including improvements to controls and procedures, may also be established

Compliance and Consequences of Non-Compliance

Failure to comply with AML legislation may result in sanctions being brought against employees such as fines and imprisonment or the Company including criminal prosecutor, and/or fines. These could affect the Company's ability to operate as well as seriously damage the Company's reputation.



Separate and in addition to the foregoing, an employee may also be liable for failure to meet record keeping and client identification responsibilities and requirements, failure to provide assistance or provide information during a compliance examination, or disclosing the fact that a unusual transaction report was made, or disclosing the contents of such a report with the intent to prejudice a criminal investigation.

“Tip Off” shall be defined as revealing to a third party that an internal or FinCEN report has been filed. Similarly, “prejudicing an investigation” involves disclosing to a third party that law enforcement is either investigating or preparing to investigate an individual. Disclosing to a suspected money launderer that a disclosure has been made will almost certainly undermine any subsequent investigation,

“Assist”

An employee commits an offense if he or she: (i) enters an arrangement which he or she knows, or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person; (ii) acquires, uses or has possession of criminal property; and (iii) conceals, disguises, converts, transfers or removes criminal property