

KYC POLICY

Effective date: September 11, 2025

Scope: This KYC Policy applies Esti Technologies N.V. (the “Company”, “we”, “us”, “our”), its subsidiaries and to all customer-facing products and services that accept wagers, bets or stakes, process deposits/withdrawals, or otherwise engage in financial transactions related to the services.

More detailed information about KYC and EDD methods is set out in the AML Policy of Esti Technologies N.V. published on a website.

1. GENERAL PROVISIONS AND POLICY STATEMENT

The Company is committed to preventing money laundering (ML), terrorist financing (TF), fraud, tax evasion and other financial crime by implementing robust customer identification, due diligence, monitoring and reporting procedures consistent with Curaçao law and CGA requirements (including the National Ordinance on Identification when Rendering Services and the National Ordinance on the Reporting of Unusual Transactions). The Company will implement risk-based KYC and customer due diligence (CDD) measures, appoint appropriately qualified compliance personnel, and maintain complete and accurate records in accordance with applicable retention rules.

POLICY OBJECTIVES

- Comply with LOK and other applicable Curaçao AML/CFT rules and any CGA guidance.
- Identify and verify the identity of customers in a timely and reliable manner.
- Assess and mitigate ML/TF risk presented by customers, transactions, geographies and products.
- Detect, escalate and report suspicious activity to competent authorities per statutory obligations.
- Cooperate with the CGA, law enforcement and financial intelligence units as required.

2. AUDIENCE

This policy is intended for:

- All staff involved in customer onboarding, compliance, payments, customer support, fraud/financial investigations, and senior management.
- Third-party service providers performing outsourced KYC or transaction monitoring services.
- Board members and the designated Compliance Officer.

3. DEFINITIONS AND ABBREVIATIONS

- **CDD (Customer Due Diligence):** Measures to identify and verify customers.
- **EDD (Enhanced Due Diligence):** Additional checks for higher-risk customers (e.g. PEPs, high risk jurisdictions, complex ownership).
- **KYC (Know Your Customer):** Procedures to verify customer identity and understand customer activity.
- **LID:** National Ordinance on identification when rendering services (Curaçao statutory instrument).
- **LMOT:** National Ordinance on the reporting of unusual transactions.
- **CGA (or GCA):** Curaçao Gaming Authority / Gaming Control Board (the regulator and AML/CFT supervisor for the gaming sector).
- **PEP:** Politically Exposed Person.
- **FIU:** Financial Intelligence Unit / the entity designated under LMOT (or goAML portal rules referenced by CGA).

4. CUSTOMER RISK ASSESSMENT

We apply a risk-based approach to all customers and relationships.

Risk factors

Assess risk using a combination of:

Customer risk

Customer risk is the risk of ML/FT/FP that arises from maintaining relations with a given customer. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. 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 (money can be derived from illegal activities);
- disproportionate spenders (inconsistent with the Company's information about the customer's known source of income/assets);
- casual customers like locals/tourists, especially when spending pattern changes;
- improper use of third parties, criminals use third parties to gamble and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid CDD

measures;

- customers using multiple casino player rating accounts to hinder the Company to track their gambling activities;
- unknown customers (redeeming large amounts of chips);
- junkets (junket operators monitor customer activity and issues and collect credit)

Geographical risk

The geographical risk is the risk posed to the Company by the geographical location of the Company itself, the customer and the source of wealth of the business relationship. The nationality, residence and place of birth of the customer have to be taken into account as well as these might be indicative of a heightened geographical risk. It is advisable to take into account a variety of sources of information, including:

- countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- countries on the FATF list of Jurisdictions under Increased Monitoring;
- countries on the CFATF Public Statement;
- countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT/CFP regime;
- countries sanctioned by the OFAC;
- countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- countries on the Corruption Perception Index compiled by Transparency International.

Product, service and transaction risk

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by the Company of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include:

- proceeds of crime – the risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from the employer;
- anonymous payment methods such as pre-paid cards and virtual assets;
- use of casino accounts – this should only be done for gambling purposes and not to deposit and withdraw without gambling or after minimal play;

- types of specific games (e.g. roulette, craps → even bets); peer-to-peer gaming;
- the use by customer of accounts held or cards issued in the name of third parties;
- the transfer of funds from one gaming account to another;
- types of financial services (credit/marker, currency exchange, check cashing); multiple casino accounts or wallets (internet operator may own and control multiple websites);
- changes to financial institution accounts to fund casino account;
- identity fraud - details of stolen financial institution accounts or stolen identities used to successfully open financial institutions accounts and used on websites;
- using cash to fund a pre-paid card poses similar risks as cash;
- games involving multiple operators (poker on platforms shared by multiple operators);
- electronic wallets (e- wallets) - not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the casino. This may be useful for dishonest customers who wish to disguise their gambling.

Distribution channels risk

The channels through which the Company establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction, including:

- channels that Favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;
- non-face-to-face interactions - while situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes unless the Company adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;
- involvement of a third party in the interactions between the customer and the Company. This is especially the case where these third parties are not themselves subject to any form of AML/CFT/CFP obligations.

Technological developments risk assessment

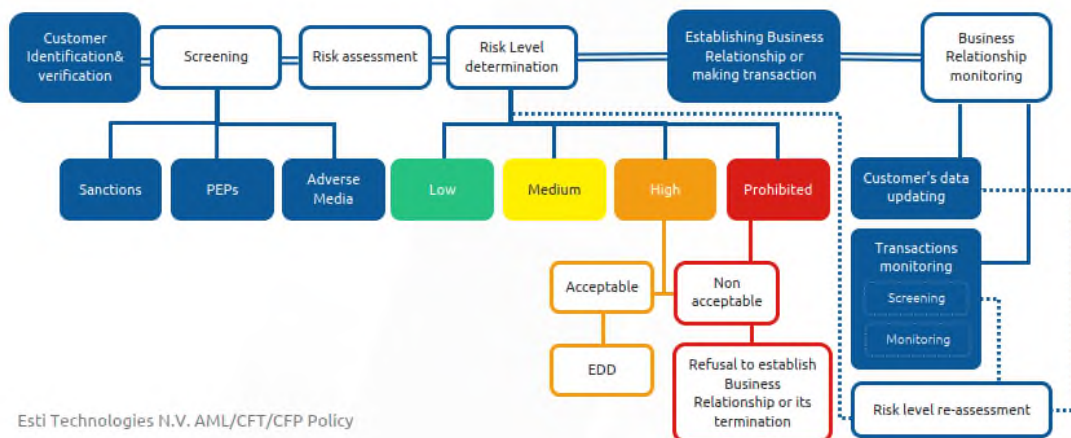
The Company shall also maintain appropriate procedures and controls for preventing the misuse of technological developments for the purpose of ML/FT/FP. The Company shall identify and assess the ML and T risks that may arise whenever:

- a new product is developed;
- a new business practice emerges;
- a new delivery mechanism becomes available;
- a new or developing technology is used for both new and pre-existing products.

In those cases, a risk assessment should take place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism. Such risk assessments must be documented. Where risks are identified, measures must be taken to mitigate these risk

Risk scoring and segmentation

- Each new customer is assigned a risk score (Low / Medium / High) using automated and manual inputs from onboarding and transaction history.
- Low-risk: basic verification; standard monitoring.
- Medium-risk: additional identity and source-of-fund checks; periodic review.
- High-risk: EDD measures, senior compliance approval prior to account activation, ongoing enhanced monitoring and potential refusal or termination.
- Risk scores are reviewed periodically and after trigger events (large deposits, suspicious alerts, sanctions lists updates).



5. CUSTOMER ACCEPTANCE POLICY

The Company will only accept customers who pass the required KYC checks and whose risk profile is acceptable. We will not accept anonymous or fictitious accounts. Before allowing wagering activity or enabling withdrawals the Company will, at minimum, complete identity verification commensurate with the risk level. Recent CGA actions confirm identity verification is required before permitting deposits or bets.

Declining or terminating relationships

- Refuse or close accounts where identity cannot be satisfactorily verified.
- Refuse or terminate relationships with customers from jurisdictions prohibited by Company policy or subject to sanctions.
- Decline high-risk customers whose risk cannot be mitigated by EDD.

6. CUSTOMER KYC (IDENTIFICATION & VERIFICATION)

6.1 Natural persons (clients/players)

Minimum information to collect and verify:

- Full legal name.
- Date of birth (to confirm legal age).
- Nationality.
- Residential address (and proof).
- ID (photo of passport, national ID, driver's license).
- Contact details (email, phone).
- Payment method ownership and source of funds for large deposits/withdrawals.

Verification steps

6.1 Natural Persons (Clients/Players)

Verification is carried out via the Profile → Verification section or during withdrawal requests in the Cashier.

(via third party provider Sum and Substance LTD)

Step 1. Identity Document Upload

- Player selects country and document type (ID card, passport, residence permit, or driver's license).
- Both sides/pages must be uploaded if applicable.
- Document must be valid for at least one more month. Expired documents are automatically rejected.

Step 2. Live Selfie

- Player completes a liveness check by rotating their head in front of the camera.
- The system captures biometric markers to ensure the person matches the ID photo.

Step 3. Confirmation

- The system provides an immediate notification of submission.
- Verification status is updated once compliance staff review documents.

Fallback Procedure:

- If documents cannot be uploaded via the system, players may send them directly to verification@punch.casino
- For card verification, a separate upload may be requested.
- Support is available 24/7 for troubleshooting.

6.2 Timing and gating

- Deposits/withdrawals are blocked until verification is completed. Low-risk provisional play may be allowed with limited thresholds (to be defined in internal AML/KYC playbook).
- The Company will not permit betting, deposits or withdrawals beyond low-risk thresholds until required identification checks are completed, except where limited provisional play is permitted under a documented risk management procedure.

6.3 Ongoing monitoring

- Transaction monitoring systems will analyze activity for deviations from expected behavior. Alerts will be investigated and escalated to the Compliance Officer.

6.4. Non-acceptable customers

The Company has created a list of prohibited risk factors (indicated AML Policy) in the presence of which the customer will not meet the Company's risk appetite. In case, when such a risk factor has arisen in the course of the customer's onboarding or before making an occasional transaction – the Company refuses to establish a business relationship or perform a transaction with such a customer. If a prohibited risk factor is identified in the course of the business relationship established – such relationship shall be terminated in accordance with this Guideline.

The Company may not establish a business relationship or conduct a transaction and shall terminate the business relationship where the customer does not facilitate compliance with the relevant due diligence measures.

The Company has to make an unusual transaction report to the FIU if the presumption of ML/FT/FP exists.

Anonymous accounts

The Company is prohibited from keeping anonymous accounts or accounts with obviously fictitious names. The Company must identify the customer and ask for the customer'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.

Prohibited countries

Curaçao prohibits its own residents to access Curaçao-based online gaming operators. Additionally, the Company cannot accept customers from territories as determined by the GCB from time to time. There are countries that have treaties in place with Curaçao that include restrictions prohibiting persons from such countries to access to Curaçao-based online gaming operators.

7. AWARE POLICY (AML TRAINING & STAFF AWARENESS)

All staff with AML/KYC responsibilities must receive regular training on:

- KYC procedures, red flags, and reporting obligations.
- Sanctions and embargo lists.
- How to detect and escalate suspicious activity.
- Data protection and confidentiality obligations.

The Company will keep training records and update training annually or more frequently as needed.

The Company shall screen their employees for criminal records before the conclusion of the employment contract.

The Company shall develop training programs and provide training to its employees. Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the Company's AML/CFT/CFP systems and procedures. Most areas of the Company should receive training, and the target audience should include most employees. However, each segment should be trained on topics and issues that are relevant to them. Training must at least address the following topics in regard to different types of employees:

For new KYC Agents (i.e. employees who will handle customers or their transactions), irrespective of their level of seniority:

- the nature and process of ML, FT and FP;
- the Company's existing internal policies, procedures concerning ML, FT and FP;
- regulations concerning ML, FT and FP;
- the reporting requirements;
 - o the need to report any unusual transactions to the appropriate designated officer;
 - o objective and subjective indicators for reporting unusual transactions;
- ML methods and trends in the gambling sector;
- explanation on CDD.

For audit staff:

- the Company's existing internal policies, procedures concerning ML, FT and PF;
- regulations concerning ML, FT and PF;
- ML methods and enforcement, and their impact on the Company.

For Compliance Department staff:

- the Company's existing internal policies, procedures concerning ML, FT and PF;
- regulations concerning ML, FT and PF;
- ML methods and trends in the gambling sector;
- ML methods and enforcement, and their impact on the Company and how the Company manages the arising risks.

This will require attending conferences or AML-specific presentations to go into greater detail.

For supervisors and managers:

- a higher-level instruction of the Company's existing internal policies, procedures concerning ML, FT and PF;
- a higher-level instruction of the regulations concerning ML, FT and PF.

For senior management and the board of directors:

- ML methods and trends in the gambling sector;
- ML methods and enforcement, and their impact on the Company.

8. RELIANCE ON THIRD PARTIES TO PERFORM KYC

Where allowed by law and acceptable under CGA guidance, the Company may rely on third-party agents/verification providers to perform part or all KYC checks, subject to the following conditions:

- A written due-diligence and oversight agreement is in place describing scope, responsibilities, confidentiality, subcontracting, audit rights and data handling.
- The third party is licensed/regulated and demonstrates robust KYC, data security and AML controls.
- The Company retains ultimate responsibility for compliance and must be able to obtain verification records on demand.
- The Company shall periodically audit and monitor third-party performance.

9. REPORTING OF SUSPICIONS AND RECORDING

9.1 Suspicious transaction reporting

- All suspicious activity identified by staff or automated systems must be reported immediately to the Company's Compliance Officer. If the Compliance Officer determines there are reasonable grounds for suspicion, a Suspicious Transaction Report (STR) must be filed in accordance with LMOT and CGA reporting procedures (including goAML portal rules and any additional CGA guidance).

9.2 Internal escalation and investigation

- Maintain an internal case file for each suspicion investigation including: source of alert, evidence, customer communications, decisions and reporting timestamps.

9.3 Recordkeeping

The Company shall record the following data in such a way that it is accessible

- the name, address and domicile or place of business of the customer and, if any, the ultimate beneficial owner and of the person in whose name the deposit or account is made, of the person who will have access to the safe deposit box or the person in whose name a payment or transaction is made, as well as their representatives;
- the nature, number, date and place of issue of the document by means of which the identity was established;
- the nature of the service; and
- the nature, origin, destination, extent and other unique characteristics of the values or items concerned in a transaction.

The Company shall maintain, the data referred to above as well as all other relevant data relating to both domestic and international transactions for at least 5 years after the execution of the transactions in question, in such a way that those data are retrievable and the transactions in question can be reconstructed for a period of 5 years to enable them to comply with information requests from the competent authorities.

The Compliance Officer shall adequately document unusual transactions. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

The FIU or staff of the FIU to be designated by the FIU, may, in the case of a transaction that has been reported to the authorities, charged with the investigation and prosecution of criminal offences, issue an instruction to set the retention period at 10 years. Acting contrary to such instruction is prohibited.

The Company shall keep data and documents obtained through the CDD measures application, including the risk profile of the customer, contact information and the copies or registers of official identity documents and passports, identity cards, driving licenses or similar documents, account statements and business correspondence, in an accessible manner for at least 5 years after the termination of the business relationship.

The data and information obtained from the CDD and transaction files shall be made available without delay to the competent authorities and the authorities that are authorized to inspect or obtain this information on the basis of the NOIS.

The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority.

10. COOPERATION WITH AUTHORITIES

- The Company will cooperate fully with the CGA, the FIU, law enforcement and other competent authorities. This includes providing documents, transactional data and access to staff as legally required. The CGA has supervisory and enforcement powers over gaming operators' AML/CFT compliance.

11. NOTIFICATIONS

- Material regulatory matters, enforcement notices or incidents affecting customer identity verification, data breaches, or AML/CFT compliance will be reported to senior management and the Board without undue delay. Where mandated by law or the CGA, the Company will make formal notifications to the CGA and other competent authorities.

12. UPDATING POLICIES AND PROCEDURES. RELATED INFORMATION

- This KYC Policy will be reviewed at least annually and whenever there is a material change in law, regulation, CGA guidance, material enforcement precedent, business model (e.g., introduction of crypto payments), or risk profile. The Compliance Officer is responsible for proposing revisions and the Board for approval.
- Related policies and procedures: AML policy, Transaction Monitoring Policy, Sanctions Policy, Data Protection Policy, Customer Due Diligence Procedures, Customer Acceptance Procedure, Third-Party Oversight Procedure, Incident Response Plan.

13. CONTACT INFORMATION

You can contact the Compliance Officer of Esti technologies N.V.
compliance@punch.casino

Legal address: Schottegatweg Oost 10 Unit 1-9, Bon Bini Business Center, Curaçao
CGA (supervisor): Curaçao Gaming Authority — AML/ CFT supervision pages and contact details available at: Curaçao Gaming Control Board website - gamingcontrolcuracao.org

14. POLICY HISTORY

Version 1.0 dated September 11,2025

ANNEX A — EXAMPLES OF KYC / EDD MEASURES

- Automated ID verification screenshots and audit logs.
- Utility bill / bank statement proof of address (dated within 3 months).
- Source of funds evidence (bank statements, pay slips) for large or unusual deposits.
- Enhanced checks for PEPs: obtain details of office/function, source of wealth and senior management approval to onboard.
- Sanctions screening against UN, EU, OFAC (if applicable), and other relevant lists; nightly re-screening for material customers.

ANNEX B — SUSPICIOUS ACTIVITY RED FLAGS (NON-EXHAUSTIVE)

- Multiple high-value deposits from different payment sources with rapid cash-out.
- Frequent large deposits followed by minimal play and immediate withdrawals.
- Multiple accounts sharing the same IP, device, or payment credentials but different IDs.
- Use of anonymizing tools (VPNs) combined with inconsistent identity documents or addresses.
- Attempts to prevent the Company from obtaining identity documentation or repeated falsified documents.