AML Policy

Last updated: 29.09.2026

This This AML Policy outlines the measures implemented by Continent Gaming N.V. (“Company”, “we”, “us” or “our”), the operator of the CHEXX website (https://chexx.bet), to prevent money laundering, terrorist financing and proliferation financing in connection with our Services.

The Company is committed to complying with applicable anti-money laundering and counter-terrorist financing laws and regulatory requirements of Curacao.

Further information about the Company, including its registered address, registration number and gaming license, is available in our Terms and Conditions.

This AML Policy forms part of our Terms and Conditions.

Applicable framework

The Company shall comply with the laws and binding regulatory requirements applicable to its Curaçao-licensed remote-gaming activities. These include, as applicable, the Landsverordening op de kansspelen (LOK), the Landsverordening identificatie bij dienstverlening (LID, also referred to in English materials as NOIS), the Landsverordening melding ongebruikelijke transacties (LMOT, also referred to in English materials as NORUT), applicable Curaçao and Kingdom sanctions measures, and the requirements, regulations, directions and guidance of the Curaçao Gaming Authority (“CGA”) and FIU Curaçao.
The Company uses the FATF Recommendations and relevant FATF gaming-risk materials as international benchmarks. They do not replace Curaçao law. Where a stricter applicable legal, regulatory or licensing requirement applies, that requirement prevails. The Compliance Officer shall maintain a controlled legal-and-regulatory inventory and escalate material changes to the Company’s management.

Governance, independence and accountability

The Director retains ultimate responsibility for the effectiveness of the Company’s AML/CFT/CPF framework. The Director approves this Policy, the Business Risk Assessment (“BRA”), the risk appetite and material remediation plans; receives periodic compliance reporting; and ensures that the compliance function is adequately resourced, independent and able to challenge commercial decisions.

The Company shall formally appoint a suitably qualified, fit and proper Compliance Officer with day-to-day authority for the AML/CFT/CPF programme and direct access to the Director. The Compliance Officer must have timely access to customer, CDD, payment, transaction, case-management and third-party data; may stop, restrict or escalate activity; and must be able to act independently from gaming and commercial operations. The role must not be combined with an incompatible operational, ownership, executive or internal-audit role.
The Compliance Officer is responsible for maintaining the programme; supervising CDD, sanctions and monitoring controls; investigating internal escalations; making and maintaining UTR filings; arranging training; reporting to senior management and the Director; and keeping the programme current. Where any task is outsourced, the Company remains fully responsible for compliance and retains ownership of customer-acceptance, risk-rating and business-relationship decisions.

Risk-based approach

The Company applies a documented risk-based approach. It maintains a BRA at least annually and whenever there is a material change, including a new product, game, payment method, crypto-asset feature, market, acquisition channel, third party, technology, regulatory requirement or material incident. The BRA considers customer, geographical, product, payment, transaction, delivery-channel, technology, fraud, ML/TF/PF and sanctions risks. The Company also performs and refreshes a Customer Risk Assessment (“CRA”) for each player. The CRA informs customer acceptance, the degree of verification, screening, monitoring, periodic review and the need for enhanced due diligence (“EDD”). Higher risk requires enhanced measures; simplified measures are never used where there is suspicion of ML/TF/PF, a sanctions concern or another higher-risk circumstance.

Customer acceptance, CDD and verification

The Company does not permit anonymous accounts, accounts in obviously fictitious names or accounts used for an undisclosed third party. A player must act in that player’s own name and on that player’s own behalf unless the Company has identified, verified and approved the relevant representative, legal person, arrangement and beneficial owner in accordance with applicable requirements.
At onboarding, the Company collects sufficient reliable information to identify the player and establish an initial risk profile. This includes, at a minimum, the player’s full legal name, permanent residential address, date and place of birth, nationality and identity number, together with contact details and any other information required by the risk profile. The Company verifies identity using reliable, independent sources and valid government-issued identification, supplemented where necessary by proof of address, payment-instrument checks and other risk-based controls.

The Company identifies and takes reasonable measures to verify any beneficial owner and understands the ownership and control structure where the customer, payer, beneficiary or account holder is a legal person or arrangement.
For remote gambling, the Company applies the statutory timing rules for CDD. In particular, it completes the required verification and full CDD no later than when the applicable NAf 4,000 threshold is reached through a single or linked financial transaction. Before verification is complete, no new financial transaction may be permitted when the threshold has been reached. Suspicion of ML/TF/PF, a sanctions concern or doubt as to previously obtained data triggers immediate CDD and escalation regardless of amount.
If CDD cannot be completed, information is unreliable or inconsistent, or the identified risk cannot be adequately mitigated, the Company will not establish or continue the relationship or process the transaction. The Compliance Officer shall document the rationale, assess whether a UTR is required and determine any restriction, termination or return-of-funds action in a manner that does not create unlawful tipping-off.

Remote identification

Remote identification and verification shall meet the applicable Curaçao requirements for identification without physical contact. The Company uses risk-assessed controls designed to establish both the genuineness of the identity evidence and the link between the evidence and the person presenting it. Controls include document validation, reliable-source or database checks where available, image-quality controls, liveness detection for unattended onboarding, biometric matching where used, device/IP/geolocation and payment-data checks, and human escalation when confidence is insufficient.
Automated or AI-enabled tools may support screening, verification and monitoring, but they do not replace the Company's legal responsibility or human compliance judgment. The Company documents the basis for the reliability of the technology, monitors performance, provides an escalation route for exceptions and does not proceed where technical deficiencies, uncertainty, suspected manipulation or identity-fraud indicators cannot be resolved.

Enhanced due diligence, PEPs and geographical risk

The Company applies EDD when the ML/TF/PF or sanctions risk is higher. EDD may be triggered by, among other matters, a PEP or relative/close associate relationship, high-risk geography, adverse media, sanctions exposure, non-face-to-face risk, inconsistent or unusually high activity, multiple or third-party payment instruments, anonymous or high-risk payment features, crypto-asset exposure, linked accounts, source-of-funds concerns or unusual player behaviour. EDD is tailored to the risk and may include senior-management approval, additional identity information, corroborated source-of-funds ("SoF") and source-of-wealth ("SoW") evidence, an explanation for the activity, additional payment verification, more frequent reviews and enhanced

ongoing monitoring. A customer declaration alone is not sufficient in a higher-risk situation where independent and reliable corroboration is reasonably available or required.
The Company screens customers, beneficial owners, authorised persons and relevant payers or payees for PEP status at onboarding and on an ongoing basis. For a foreign PEP, and for domestic or international-organisation PEPs where the relationship is higher risk, the Company obtains senior-management approval, establishes SoW and SoF using proportionate measures and applies enhanced ongoing monitoring. The same approach applies to family members and close associates as required by applicable law.
Geographical risk is assessed dynamically using current official information, including applicable FATF public statements, sanctions measures and other credible risk information. FATF increased monitoring alone is not treated as an automatic or permanent customer ban; decisions must be risk-based. The Company applies EDD and any countermeasures where applicable law, sanctions or a FATF call for action requires them.
In accordance with its internal documents, the company restricts access to its services for a number of countries and territories. The list is provided in Appendix 1.

Sanctions and targeted financial sanctions

The Company screens at onboarding, before or during relevant payment activity, on material customer-data changes, periodically during the relationship and promptly after relevant list updates. Screening covers United Nations lists, applicable Curaçao and Kingdom sanctions measures, including applicable EU restrictive measures, and any other lists used by the Company as a risk-management control.
A potential sanctions match is escalated immediately for documented review. On a confirmed match or other case requiring targeted financial sanctions, the Company freezes funds and other relevant economic resources without delay and without prior notice, makes no funds, services or economic resources available directly or indirectly, and follows the applicable reporting, notification and asset-freezing process. The Company does not close, pay out or otherwise take action that could frustrate a freeze or facilitate evasion.

Payments, third parties and crypto-assets

The Company seeks to maintain a clear audit trail between a verified player, the funding source and the withdrawal destination. Deposits and withdrawals should ordinarily use a verified payment instrument, bank account or wallet attributable to the same verified player. Third-party funding, third-party withdrawals, anonymous payment methods, mismatched payment credentials and unexplained changes in payout destination are prohibited or restricted unless specifically permitted by law and approved in advance by Compliance following documented risk-based due diligence.

Withdrawals are normally returned through the verified source channel or to a verified account or wallet held by the same customer. Any exception requires a documented legitimate rationale, Compliance approval, appropriate CDD/EDD, sanctions screening and enhanced monitoring. Payment service providers, e-wallet providers and other payment partners are subject to risk-based due diligence, contractual AML/CFT/CPF requirements and ongoing oversight; their controls do not replace the Company's own obligations.

Where the Company accepts or otherwise handles crypto-assets, it shall maintain a documented crypto-asset risk assessment and controls proportionate to the CGA's applicable crypto-policy expectations. These include due diligence on virtual-asset service providers, sanctions and blockchain screening, wallet-risk assessment, ownership or control verification for self-hosted wallets where appropriate, monitoring of deposits and withdrawals, prohibited-source controls and enhanced due diligence for elevated risk. The Company shall not conduct activities requiring a separate payment-service-provider or virtual-asset-service-provider authorisation unless it holds the required authorisation.

Ongoing monitoring and investigations

The Company conducts ongoing monitoring to ensure that customer activity is consistent with its knowledge of the player, expected activity, payment information, source of funds and risk profile. Monitoring is risk-based and combines automated scenarios with trained human review. Relevant alerts and investigations are recorded and may lead to a CRA refresh, EDD, account restriction, UTR consideration or other proportionate action.

Monitoring scenarios address, among other matters:

- deposits followed by withdrawal with minimal or no gameplay, or other activity inconsistent with the stated purpose of the relationship;
- structuring, rapid changes in volume, unusual velocity, dormant-account reactivation or activity inconsistent with the customer profile;
- linked accounts, shared devices, IP addresses, addresses, payment credentials or other indicators of mule activity, account takeover or identity fraud;
- third-party, mismatched, multiple or rapidly changed payment instruments; chargeback patterns; and unexplained changes of withdrawal destination;
- geolocation, VPN/proxy, device or behavioural anomalies; peer-to-peer transfers, collusion or coordinated gameplay where offered; and
- sanctions, PEP, adverse-media, law-enforcement, crypto-wallet or other indicators of ML/TF/PF risk.

Unusual-transaction reporting and confidentiality

All employees and relevant third parties must promptly escalate a completed or attempted transaction, pattern or circumstance that may be unusual to the Compliance Officer through the controlled internal reporting channel. The Company recognises both objective and subjective

indicators under the applicable Curaçao indicators regime. This includes the applicable NAf 5,000 objective reporting threshold for gaming-sector financial transactions, relevant sanctions-related transactions and transactions or patterns that give cause to presume ML/TF/PF.
The Compliance Officer investigates internal escalations, maintains a case record and reports unusual transactions to FIU Curaçao through goAML without delay, in English and with the information and supporting material required by law. The reporting obligation concerns unusual transactions; it does not require proof of a predicate offence. Decisions not to make an external report must be documented with the supporting rationale.
No director, officer, employee, agent, payment partner or other unauthorised person may disclose or suggest to a customer or third party that a UTR has been filed, is being considered, that FIU Curaçao has made a request, or that an AML/CFT/CPF investigation exists. UTR and investigation information is restricted on a need-to-know basis. Customer communications requesting ordinary CDD information must be neutral and must not create tipping-off.

Records, data protection and information security

The Company retains customer identification and verification data, risk assessments, CDD/EDD evidence, account and transaction records, correspondence, screening results, monitoring alerts, investigations, UTR-related information, training records and audit evidence for the periods required by law. As a minimum, transaction and CDD records are retained for five years after the applicable transaction or end of the business relationship, as applicable. The Company maintains an effective legal-hold process and extends retention to ten years where instructed by FIU Curaçao.
Information is maintained in a form that permits timely retrieval and reconstruction of individual transactions. Personal data is processed lawfully, securely and only for legitimate purposes, including compliance with AML/CFT/CPF and sanctions obligations, in accordance with applicable Curaçao data-protection law and any other mandatory regime. Access is controlled using need-to-know, least-privilege and authentication controls. The Company uses appropriate encryption, logging, vendor controls, incident response and safeguards for cross-border transfers and sensitive identity, biometric and case data.

Training, screening, testing and assurance

The Company screens employees proportionately to their role and risk exposure. It provides induction and ongoing role-based training to relevant personnel, including customer support, payments, KYC, fraud, gaming operations and management. Training covers ML/TF/PF, sanctions, CDD/EDD, remote identity fraud, red flags, escalation, UTR obligations and no tipping-off. The Company maintains records of content, attendance, assessment and refresher plans.
The AML/CFT/CPF programme is subject to independent testing at least annually by an adequately qualified internal-audit function independent from AML operations or by a qualified

external party. Testing covers policy design, customer files, screening, transaction monitoring, UTR handling, training, records, third parties, technology controls and timely remediation. Findings, owners, deadlines and closure evidence are reported to senior management.

Third parties, reliance and implementation

The Company may rely on a third party for permitted CDD elements only where the legal conditions for reliance are met, the third party is appropriately regulated or supervised, CDD information is available immediately, copies of supporting records can be obtained promptly, country risk is acceptable and the arrangement is tested periodically. The Company remains responsible for its own CRA, PEP assessment, sanctions controls, ongoing monitoring and final onboarding or continuation decision.

The Company applies this Policy to relevant branches, subsidiaries, agents, affiliates and outsourced providers to the extent permitted by applicable law. Material third-party arrangements must be documented, risk-assessed and subject to contractual audit, access, security, information-sharing and remediation rights.

Breaches, review and policy management

Suspected breaches of this Policy must be escalated immediately to the Compliance Officer and, where appropriate, senior management, CGA, FIU Curaçao or another competent authority. The Company may suspend accounts, transactions, products, suppliers or personnel while it investigates. Deliberate or negligent non-compliance may result in disciplinary action, contractual remedies, termination and regulatory or law-enforcement reporting.

The Compliance Officer reviews this Policy at least annually and proposes revisions promptly following legal, regulatory, sanctions, product, payment, technology, geography, control-testing or risk developments. Material changes require Director approval.

Regulatory and standards reference framework

This Policy is drafted by reference to the following sources, as in force or published as at 29 September 2026:

- Landsverordening op de kansspelen (LOK), P.B. 2024, no. 157.
- Landsverordening identificatie bij dienstverlening (LID/NOIS), P.B. 2017, no. 92, as amended, including P.B. 2024, no. 41.
- Landsverordening melding ongebruikelijke transacties (LMOT/NORUT), P.B. 2017, no. 99, as amended, and the applicable Regulation Indicators Unusual Transactions.
- Applicable Curaçao and Kingdom sanctions measures, including the Sanctions National Ordinance, the Kingdom Sanctions Act and implementing sanctions decrees.
- CGA Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, January 2025; CGA Requirements for Compliance

Officer, January 2025; and Provisions for Identification and Verification without Physical Contact, 2026.

- FIU Curaçao reporting and goAML requirements.
- FATF Recommendations, as amended June 2026, and FATF gaming and gambling risk materials, as international standards and good-practice benchmarks.

The Compliance Officer shall maintain the controlled source register, including CGA publications, FIU notices and sanctions notices. In case of conflict, applicable law, individual licence conditions and binding regulator directions prevail over this Policy.

Appendix 1 - List of Restricted Jurisdictions

The following countries and territories are restricted from accessing the Company's Services:

Abkhazia
Afghanistan
American Samoa
Anguilla
Aruba
Belarus
Bermuda
Bonaire, Sint Eustatius and Saba
British Indian Ocean Territory
Canada
Cayman Islands
Comoros
Curaçao
Falkland Islands (Malvinas)
Gibraltar
Greenland
Guam
Guernsey
Iran, Islamic Republic of
Isle of Man
Jersey
Korea, Democratic People's Republic of
Latvia
Montserrat
Myanmar
Netherlands
Northern Mariana Islands
Pitcairn

Puerto Rico
Russian Federation
Saint Helena, Ascension and Tristan da Cunha
Saint Kitts and Nevis
Sint Maarten (Dutch part)
Somalia
South Georgia and the South Sandwich Islands
South Ossetia
Turks and Caicos Islands
Ukraine
United Kingdom
United States Minor Outlying Islands
United States of America
Virgin Islands, British
Virgin Islands, U.S.
Yemen

This list may be updated by the Company from time to time in accordance with applicable legal and regulatory requirements and its internal risk management policies.