

BALKAN INTERNATIONAL N.V.

ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND COUNTER-PROLIFERATION FINANCING POLICY

B2B SUPPLIER / CRITICAL SERVICES PROVIDER

CGA licence number: OGL/2024/2354/1208

Company Registration Number: 165051

Effective date: 02.02.2026

Version: 1.0

Approved by: Board of Directors

CONFIDENTIAL

Document Control

Field	Details
Policy owner	Board of Directors / AML Responsible Officer
Responsible office	Compliance Function
Policy audience	Directors, officers, employees, contractors, outsourced service providers and relevant B2B counterparties
CGA licence type	B2B supplier licence / licence for the supply of critical services and goods
Licensed services	[INSERT THE SERVICES LISTED IN THE CGA LICENCE]
Effective date	[INSERT]
Next scheduled review	No later than 12 months after the effective date
Event-driven review	Before new products, services, payment methods, technologies, markets, delivery channels or material outsourcing; and following material legal, regulatory, ownership or risk changes
Classification	Confidential - Internal Use
Supersedes	The former TC Entertainment N.V. Anti-Money Laundering Procedure dated 29 September 2020, only to the extent formally adopted by Balkan International N.V.

Table of Contents

Section	Page	Section	Page
1. Policy Statement	4	17. Confidentiality and Tipping Off	13
2. Purpose	4	18. Holds, Restrictions and Termination	13
3. Scope and Audience	4	19. Record Keeping	13
4. Legal and Regulatory Framework	5	20. Employee Screening, Conduct and Training	14
5. Definitions	5	21. Independent Testing and Quality Assurance	14
6. Governance and Responsibilities	6	22. Management Information and Cooperation	15
7. Risk-Based Approach and BRA	7	23. Breaches, Enforcement and Consequences	15
8. B2B Counterparty Risk Assessment	8	24. Review, Change Control and Availability	15
9. B2B Customer Acceptance Policy	8	Appendix A - B2B Risk Rating Matrix	16
10. Customer Due Diligence and KYB	9	Appendix B - B2B KYB / CDD Checklist	16
11. Enhanced Due Diligence	10	Appendix C - B2B Red Flags	17
12. Targeted Financial Sanctions and PF	10	Appendix D - Internal Unusual Transaction Report	17
13. Ongoing Monitoring	11	Appendix E - Minimum Contractual AML Clauses	17
14. Payment, Settlement and Funds Controls	11	Appendix F - Regulatory Reference List	18
15. Reliance, Outsourcing and Third-Party Controls	12	Appendix G - Source Policy Adaptation Record	18
16. Internal Escalation and Unusual Transactions	12	Board Adoption	19

Page references are based on this approved-format version and may change if substantive content is added. Word users may update the contents manually after amendments.

1. Policy Statement

Balkan International N.V. (the “Company”) is committed to conducting its B2B gaming-supply business in a manner that prevents its corporate structure, personnel, technology, products, services, systems, settlement arrangements and commercial relationships from being used for money laundering, terrorist financing or proliferation financing (“ML/TF/PF”).

The Company applies a documented, risk-based AML/CFT/CPF framework. It will identify and verify B2B clients and relevant natural persons, understand ownership and control, assess the purpose and intended nature of each relationship, monitor activity, screen for sanctions and politically exposed persons, report unusual transactions where legally required, maintain records, train personnel and test the effectiveness of its controls.

The Company will not knowingly provide licensed goods or services to an illegal, unlicensed, sanctioned, anonymously owned or otherwise unacceptable business. Commercial pressure, revenue targets or seniority do not override this Policy.

2. Purpose

This Policy establishes the minimum AML/CFT/CPF standards for the Company as a Curaçao B2B supplier. It is designed to:

- implement the Company's obligations under its CGA supplier licence and applicable Curaçao law;
- adapt the useful control principles contained in the former TC Entertainment N.V. Anti-Money Laundering Procedure to a B2B corporate-counterparty model;
- protect the integrity and reputation of the Company and the Curaçao gaming sector;
- define responsibilities for governance, risk assessment, due diligence, monitoring, investigation, reporting, record keeping, training and assurance;
- provide staff with clear escalation rules, including strict controls against tipping off; and
- ensure that the Company can provide the CGA, FIU Curaçao and other competent authorities with complete and reliable information when lawfully required.

3. Scope and Audience

This Policy applies to the Company, its directors, officers, employees, temporary staff, consultants, contractors, branches and controlled subsidiaries. It also applies, through contractual obligations and oversight, to outsourced service providers performing onboarding, screening, transaction monitoring, payment, hosting, customer support, compliance, data processing or other relevant functions.

The Policy applies to the following relationships and activities:

- B2B clients receiving the Company's licensed goods or services;
- prospective B2B clients and introducers;
- distributors, resellers, white-label partners, aggregators and platform partners;
- payment service providers, banks, e-money institutions, crypto-asset service providers and settlement counterparties;
- game studios, software suppliers, hosting providers, data centres, test laboratories and other critical vendors;
- beneficial owners, qualifying interest holders, directors, key persons, authorised signatories and other persons acting for or controlling a counterparty;
- material commercial payments, revenue-share settlements, royalties, jackpot or prize-pool administration and other financial flows connected to the licensed services; and
- any access the Company has to player information, player funds, wallets, payment functionality or end-user transaction data, even where the B2C operator remains primarily responsible for player CDD.

4. Legal and Regulatory Framework

The Company shall keep this Policy aligned with the current version of all applicable laws, decrees, licence conditions, CGA instructions and portal checklist requirements. The principal framework includes:

- the National Ordinance on Games of Chance (Landsverordening op de kansspelen, “LOK” or “NOGC”);
- the National Ordinance on Identification in Service Provision (NOIS / LID), PB 2017, no. 92, as amended;
- the National Ordinance on the Reporting of Unusual Transactions (NORUT / LMOT), PB 2017, no. 99, as amended;
- the Sanctions National Ordinance, PB 2014, no. 55, and the Kingdom Sanctions Act and implementing measures;
- the applicable Regulation Indicators Unusual Transactions, including amendments;
- the CGA Regulations for combating Money Laundering, Terrorist Financing and Proliferation Financing, effective January 2025, to the extent applicable and adaptable to the Company’s B2B activity;
- the CGA supplier licence conditions and any conditions or deadlines in the Company’s online gaming portal account; and
- applicable laws of each country in which the Company operates or supplies services.

The CGA supplier licence conditions require the Company to comply with the NOGC, NOIS, NORUT and sanctions framework, take appropriate measures where activities are outsourced, engage only with parties operating lawfully, maintain an AML/CFT/CPF policy, provide information requested by the CGA and submit qualifying incident reports within the applicable regulatory deadline.

Where there is a conflict between this Policy and mandatory law or a written direction of the CGA, the mandatory requirement prevails. The AML Responsible Officer must document the conflict, obtain legal advice where appropriate and arrange prompt amendment of this Policy.

5. Definitions

Term	Meaning
AML Responsible Officer	The senior individual designated by the Board to coordinate the Company’s AML/CFT/CPF framework. This internal designation is used even where the CGA’s specific compliance-officer appointment guidance exempts B2B licensees.
B2B Client	A legal person, legal arrangement or business receiving the Company’s licensed goods or services.
Beneficial Owner / UBO	The natural person who ultimately owns or controls a customer or on whose behalf a transaction is conducted. For legal persons, the Company applies applicable statutory tests and identifies persons holding 25% or more ownership or voting rights, persons exercising control by other means, and, where no such person is identified, the senior managing official.
Business Relationship	A professional or commercial relationship expected to have an element of duration.
CDD / KYB	Customer due diligence / know-your-business measures used to identify and verify a B2B Client and relevant natural persons and understand the relationship.
CFT	Countering the financing of terrorism.
CPF / PF	Countering or financing of proliferation of weapons of mass destruction.
CGA	Curaçao Gaming Authority.
EDD	Enhanced due diligence applied where higher risk is identified.
FIU Curaçao	The Financial Intelligence Unit of Curaçao, including the goAML reporting portal.
PEP	A politically exposed person, including relevant family members and close associates, as defined by applicable law and guidance.
Sanctions	Targeted financial sanctions and other restrictive measures applicable under Curaçao law, UN Security Council measures, EU measures binding through the Kingdom framework, local designations and any other sanctions regime applicable to the Company or a transaction.
Source of Funds	The origin of funds used for a specific transaction or relationship.
Source of Wealth	The origin of the total wealth accumulated by a natural person.
Unusual Transaction	A completed or intended transaction that meets an applicable objective indicator or gives cause to presume a connection to ML/TF/PF.

6. Governance and Responsibilities

6.1 Board of Directors

The Board owns the Company's AML/CFT/CPF risk and is responsible for setting the tone from the top. The Board shall:

- approve this Policy, the Business Risk Assessment ("BRA"), the risk appetite and material amendments;
- ensure sufficient personnel, systems, expertise, authority and budget for effective controls;
- receive at least quarterly management information and promptly review material incidents;
- ensure that high-risk relationships requiring senior approval are decided independently and documented;
- ensure that the compliance function has unrestricted access to records, systems, personnel and the Board;
- approve the annual independent AML audit plan and remediation of findings; and
- ensure the Company does not expand beyond the goods and services authorised by its CGA licence.

6.2 AML Responsible Officer

The Board shall designate an AML Responsible Officer with sufficient seniority, competence, time, resources and independence. The officer must not be placed in a position where commercial or operational duties compromise objective AML decision-making.

The CGA's January 2025 guidance states that B2B licensees are not required to appoint a compliance officer under the specific appointment requirements in that guidance. Nevertheless, the Company voluntarily assigns clear day-to-day ownership through the AML Responsible Officer. The Board must separately verify whether the Company's licence, portal checklist, corporate structure or future CGA directions require a formally approved key person or NOIS/NORUT compliance officer.

- maintain and implement the AML/CFT/CPF programme;
- maintain the BRA, counterparty risk methodology, acceptance rules and monitoring scenarios;
- review and approve high-risk onboarding, EDD and material exceptions;
- review internal unusual transaction reports and determine external reporting obligations;
- coordinate FIU Curaçao and CGA reporting and preserve evidence of decisions;
- oversee sanctions screening, freezing actions and escalation;
- maintain training, internal reporting, case management and record-keeping arrangements;
- prepare quarterly and annual management information;
- track legal and regulatory changes and recommend amendments; and
- coordinate the annual independent review and remediation plan.

6.3 Business, Sales and Account Management

- may not promise onboarding, activation, settlement or continued service before required due diligence and approvals are complete;
- must obtain accurate information on ownership, licensing, intended use, target markets and payment flows;
- must promptly escalate changes, red flags, unusual requests, adverse media and regulatory concerns;
- must not coach a client on how to avoid checks or alter facts to fit acceptance criteria; and
- must not disclose internal reports, FIU reports, sanctions investigations or confidential compliance reasoning.

6.4 Finance and Payments

- verify that payer and payee accounts are held in the name of the approved counterparty or are otherwise documented and approved;
- reconcile invoices, contracts, revenue-share calculations, credits, refunds, wallet addresses and settlement records;
- block or refer transactions that fall outside the approved profile;
- preserve a complete audit trail sufficient to reconstruct transactions; and
- apply segregation and safeguarding controls if the Company administers funds intended for player payouts, jackpots or prize pools.

6.5 Technology, Operations and Security

- implement access controls, logging, data integrity and retention necessary for monitoring and investigations;
- ensure rules, alerts and case-management systems cannot be disabled without approved change control;
- preserve relevant logs and evidence following an alert or incident;
- notify the AML Responsible Officer of cyber, fraud, data, payment or integrity incidents with possible ML/TF/PF relevance; and
- support regulatory data-access and reporting obligations.

6.6 All Personnel

All personnel have a personal duty to remain alert, complete training, follow procedures and report concerns immediately. No employee may investigate beyond their authority, confront a suspected person, destroy or alter records, or take action likely to tip off a counterparty.

7. Risk-Based Approach and Business Risk Assessment

The Company shall maintain a documented BRA that identifies, assesses, understands and mitigates the ML/TF/PF risks arising from its B2B business. The BRA shall be approved by the Board, made available to the CGA on request and reviewed at least annually and whenever a material change occurs.

7.1 Mandatory Risk Factors

- Counterparty risk: type of client, licensing status, ownership, governance, reputation, AML maturity, regulatory history and business model;
- Geographic risk: incorporation, operations, ownership, banking, customers, target markets, data hosting and payment flows;
- Product and service risk: platform, aggregation, game content, managed services, payment functionality, wallets, jackpots, affiliate tools, KYC tools, white-label services and any capability that can move or obscure value;
- Delivery-channel risk: non-face-to-face onboarding, intermediaries, agents, resellers, APIs, remote access and cross-border supply;
- Transaction risk: settlement size, frequency, complexity, revenue share, third-party payments, refunds, credits, chargebacks, crypto-assets and unexplained changes;
- Technology risk: anonymity-enhancing technology, digital assets, new payment methods, automated onboarding, artificial intelligence, outsourcing and data gaps;
- Sanctions and proliferation risk: ownership, goods, software, end-use, jurisdictions, designated parties and evasion indicators; and
- Internal risk: staff access, privileged users, conflicts of interest, override capability, vendor dependence and control effectiveness.

7.2 New Products, Markets and Technologies

Before launch or material change, the business owner and AML Responsible Officer shall complete a documented risk assessment for new products, services, markets, payment methods, delivery mechanisms, technologies, outsourcing arrangements and changes in the way value or data moves through the Company's systems. Launch is prohibited until required controls, approvals and licence permissions are in place.

7.3 Risk Appetite

The Board shall define the level and type of risk the Company is prepared to accept. The following are outside risk appetite unless expressly permitted by law and approved following exceptional review: anonymous or nominee ownership without transparent UBOs; unlicensed gaming activity; sanctioned parties; concealment of target markets; payment by unrelated third parties; untraceable or anonymity-enhancing assets; falsified documents; and relationships where CDD cannot be completed.

8. B2B Counterparty Risk Assessment

A counterparty-specific risk assessment shall be completed before establishing a business relationship and refreshed throughout the relationship. The assessment must be based on verified facts, not solely on representations made by sales personnel or the counterparty.

8.1 Risk Categories

Category	General characteristics	Minimum treatment
Low	Transparent ownership; reputable regulated market; simple service; expected payments from own regulated bank account; no material adverse information.	Standard CDD; normal monitoring; refresh normally every 36 months or sooner on trigger.
Medium	Cross-border structure; moderate geographic or product risk; reliance on service providers; higher settlement complexity; limited adverse information resolved by evidence.	Standard CDD plus targeted additional checks; enhanced monitoring; refresh normally every 24 months.
High	PEP/close associate; high-risk geography; complex ownership; crypto or alternative settlement; material regulatory history; white-label/reseller chain; player-fund access; substantial adverse media or unusual payment model.	EDD; source-of-funds/wealth evidence where relevant; senior approval; enhanced monitoring; refresh at least annually.
Prohibited / Unacceptable	Sanctioned; illegal or unlicensed activity; concealed UBO; false information; shell arrangement without legitimate purpose; services intended to evade law or licence conditions; CDD failure.	Reject, suspend or exit; consider FIU/CGA reporting; preserve records and avoid tipping off.

8.2 Risk Scoring and Overrides

The Company may use a numerical model, but judgement and mandatory overrides apply. A sanctions match, illegal activity, inability to identify the UBO, falsified documents or a credible suspicion of ML/TF/PF cannot be reduced to an acceptable rating by scoring. The AML Responsible Officer documents all overrides and the reasons for them.

9. B2B Customer Acceptance Policy

9.1 Acceptance Conditions

A B2B Client may be accepted only where the Company is satisfied that:

- the entity legally exists and is authorised to enter the relationship;
- its ownership and control are transparent and verified;
- its gaming or related activity is lawful and properly licensed in relevant jurisdictions;
- the intended services, markets, domains and transaction flows are understood and within the Company's CGA licence;
- the source and expected use of funds are legitimate and consistent with the business model;
- sanctions, PEP and adverse-media results have been resolved;
- the risk rating is within the Board-approved appetite; and
- the contract includes audit, information, compliance, suspension, termination and regulatory-cooperation rights appropriate to the risk.

9.2 Mandatory Rejection or Exit

- a confirmed sanctions prohibition or prohibited ownership/control;
- illegal or unlicensed gaming activity, or use of services for unauthorised domains or markets;
- refusal or repeated failure to provide reliable CDD, UBO, licensing, source-of-funds or transaction information;
- false, forged, misleading or materially incomplete information;
- an ownership or control structure designed to conceal the true controlling persons or commercial purpose;
- payment arrangements with no credible economic purpose or involving unrelated third parties without satisfactory evidence;
- a request to misdescribe services, invoices, jurisdictions, counterparties or transaction purpose;

- use of mixers, tumblers, privacy-enhancing mechanisms or unhosted wallets where risk cannot be adequately mitigated; or
- any risk that the Board determines cannot be effectively controlled.

10. Customer Due Diligence and Know-Your-Business

10.1 Timing

CDD must be completed before contract activation, system access, supply of licensed services, acceptance of funds or settlement, unless a documented legal exception applies. Commercial urgency is not an exception. Where suspicion arises, CDD must be applied regardless of value, and the AML Responsible Officer must consider whether further information gathering would create a tipping-off risk.

10.2 Legal Entity Identification and Verification

The onboarding file shall contain reliable, independent evidence appropriate to the jurisdiction and risk, including:

- full legal name, legal form, registration number, incorporation date and registered office;
- recent official registry extract or equivalent;
- constitutional documents and evidence of active status;
- tax identification and principal place of business;
- gaming and other relevant licences, licence status, licensed activities, approved domains and target markets;
- directors, authorised representatives and signing authority;
- ownership chart to natural-person UBO level and details of qualifying interests;
- business model, products, services, customer base, expected relationship purpose and intended use of the Company's services;
- expected transaction volumes, currencies, payment methods, bank accounts and settlement flows;
- source of operating funds and, where appropriate, source of wealth of relevant UBOs;
- regulatory, enforcement, litigation, insolvency and adverse-media history; and
- material outsourcing, resellers, white-labels, agents, sub-licensees and other parties in the supply chain.

10.3 Beneficial Ownership and Control

The Company shall identify and take reasonable measures to verify the natural persons who ultimately own or control the B2B Client. It shall understand the ownership and control structure, not merely collect a declaration. Trusts, foundations, partnerships, nominees and layered holding structures require identification of relevant settlors, trustees, protectors, beneficiaries, partners, controllers and equivalent persons as required by law and risk.

Where ownership or control cannot be reliably established, the relationship must not start or continue. Identification of a senior managing official as a fallback does not remove the obligation to investigate whether another person exercises ultimate effective control.

10.4 Natural Persons

Directors, UBOs, authorised signatories and other relevant natural persons shall be identified and verified using reliable independent documents, data or information. The Company shall verify document validity, authenticity and consistency and may require address evidence, liveness or biometric checks, a verified bank payment, notarisation, certification or additional documents where risk warrants.

10.5 Purpose and Intended Nature

The Company shall document why the B2B Client requires the services, how they will be used, the jurisdictions and domains involved, expected transaction types and volumes, the commercial rationale, the source of funds, and whether the client or its customers can access payment, wallet, jackpot, game, identity or data functionality through the Company's systems.

10.6 PEP, Sanctions and Adverse-Media Screening

Before onboarding, the Company shall screen the B2B Client, UBOs, controllers, directors, key persons, authorised signatories and other risk-relevant parties against applicable sanctions lists, PEP data and credible adverse-media sources. Screening must be repeated on an ongoing basis and when relevant lists or data change.

11. Enhanced Due Diligence

EDD shall be applied where the risk is higher. EDD measures are cumulative and proportionate to the identified risk. They may include:

- additional corporate, ownership, identity and licensing documents;
- independent verification through regulators, registries, banks, auditors, lawyers or reputable databases;
- evidence of source of funds and source of wealth, including audited accounts, bank statements, tax records, contracts, sale documents or investment evidence;
- detailed explanation and evidence of the business model, transaction rationale, target markets, domains, resellers and end users;
- senior-management approval before starting or continuing the relationship;
- shorter review cycles and more frequent sanctions, licence and adverse-media screening;
- lower alert thresholds, transaction pre-approval or manual settlement review;
- site visits, video interviews or direct contact with directors, compliance personnel or regulators;
- contractual restrictions, audit rights, data-access rights and termination triggers;
- testing of the counterparty's AML controls where reliance, funds, player data or material operational dependence exists; and
- limitation or prohibition of specific markets, payment methods, assets, products, domains or subcontractors.

11.1 PEP Relationships

A PEP relationship is not automatically prohibited. Before onboarding or continuation, the Company shall establish the source of wealth and source of funds where relevant, obtain senior-management approval, understand the reason for the relationship and apply enhanced ongoing monitoring. Former PEP status must be treated according to applicable law and continuing risk.

11.2 High-Risk Countries and Sanctions-Exposure

The Company shall consider FATF and CFATF statements, Curaçao and Kingdom measures, sanctions exposure, corruption, crime, regulatory quality, transparency and the Company's own experience. The Company shall not rely on a country list alone; it shall assess the complete ownership, operational, banking and end-use chain.

12. Targeted Financial Sanctions and Proliferation Financing

The Company must not make funds, assets, software, services or economic resources available, directly or indirectly, to or for the benefit of a designated person or entity. Screening shall cover the UN and EU lists referenced by CGA guidance, local Curaçao designations and any other list applicable to the Company, its banks, payment providers, contracts or markets.

Potential matches must be escalated immediately and handled confidentially. A confirmed match requires the Company to:

- stop onboarding, access, delivery, payment or settlement as legally required;
- freeze relevant funds or assets without delay and without prior notice where the legal test is met;
- prevent direct or indirect circumvention, including through affiliates, nominees, wallets or intermediaries;
- make required reports to FIU Curaçao and other competent authorities;
- consider whether a separate CGA incident report is required;
- preserve all records, logs and decision evidence; and
- avoid any communication that would disclose a confidential report or undermine an investigation.

Proliferation-financing risk shall be considered where software, infrastructure, hosting, payments, technology or services may be used by sanctioned jurisdictions, entities or procurement networks. The Company shall assess end-use, end-user, ownership, routing, intermediaries and evasion indicators.

13. Ongoing Monitoring

Monitoring is continuous and risk-based. It includes monitoring the counterparty's identity, ownership, licensing, reputation, service use and transactions throughout the relationship to ensure that activity remains consistent with the Company's knowledge of the client, its business, risk profile and source of funds.

13.1 Identity, Ownership and Licence Monitoring

- periodic refresh of CDD according to risk;
- event-driven refresh following ownership, director, licence, domain, market, payment, bank, address, corporate or control changes;
- ongoing sanctions, PEP and adverse-media screening;
- verification of continued licensing and lawful operation in relevant jurisdictions;
- review of new domains, resellers, white-labels, sub-contractors and markets before use; and
- review of expired documents and unexplained inconsistencies.

13.2 Transaction and Activity Monitoring

Monitoring shall cover invoices, payments, refunds, credits, chargebacks, revenue-share settlements, royalties, jackpot and prize-pool flows, bank accounts, wallet addresses, currencies, access logs, system activity and other data available to the Company. Monitoring scenarios shall be calibrated to the Company's actual services and risks.

- payments to or from an unapproved or unrelated third party;
- payments routed through a jurisdiction unrelated to the client or service;
- material deviations from expected volume, frequency, currency or value;
- rapid movement, circular settlement, pass-through activity or unexplained refunds;
- split invoices or transactions apparently structured to avoid review;
- frequent changes to bank accounts, wallets, ownership, domains or settlement instructions;
- use of services for unapproved markets, domains, brands or counterparties;
- revenue inconsistent with website traffic, game activity, contracts or the client's scale;
- unusual chargeback, bonus, affiliate, jackpot, wallet or player-fund patterns visible to the Company;
- requests to suppress data, bypass controls, alter logs or disable monitoring;
- links to fraud, cybercrime, account takeover, sanctions evasion, bribery, tax crime or illegal gambling; and
- activity inconsistent with the declared business model or lawful commercial purpose.

14. Payment, Settlement and Funds Controls

The Company shall use traceable and transparent payment methods. Cash is prohibited for B2B client payments and settlements unless expressly permitted by law, approved by the Board and supported by exceptional controls. As a general rule:

- payments are accepted only from accounts held in the approved counterparty's name;
- payments are returned only to the original verified source, unless a documented legal or operational reason is approved;
- third-party payments require documented ownership, purpose, relationship and AML approval before acceptance;
- bank-account and wallet changes require independent callback or equivalent verification;
- invoices and settlement descriptions must accurately reflect the contracted services;
- no employee may use a personal account or wallet for Company or client funds;
- manual overrides, refunds and credits require segregation of duties and an audit trail; and

- where the Company holds or administers funds intended for player payouts, progressive jackpots or prize pools, those funds shall be safeguarded and segregated as required by the CGA.

14.1 Crypto-Assets and Virtual-Asset Settlement

Crypto-asset acceptance is prohibited unless included within the Company's lawful operating model and approved by the Board following a documented risk assessment. Approved arrangements must include wallet ownership verification, blockchain analytics, sanctions screening, source-of-funds evidence, transaction monitoring, control of unhosted wallets, and restrictions on mixers, tumblers, privacy-enhancing assets and high-risk services. The Company shall also comply with any current CGA crypto policy and directions.

15. Reliance, Outsourcing and Third-Party Controls

The Company remains responsible for compliance where it relies on or outsources to a third party. Onboarding and continuation decisions based on risk cannot be outsourced.

15.1 Reliance on Third Parties for CDD

Reliance may occur only where permitted by law and where the Company:

- obtains the core CDD information immediately;
- has a written agreement requiring the third party to provide copies of documents and data without delay;
- is satisfied that the third party is regulated, supervised, reputable and subject to equivalent CDD and record-keeping requirements;
- assesses country and institutional risk;
- has audit and termination rights; and
- retains ultimate responsibility for the adequacy of CDD.

15.2 Outsourced Functions

Before outsourcing a material AML-related or operational function, the Company shall conduct due diligence on the provider, assess concentration and country risk, define service levels, confidentiality, security, record retention, audit rights, regulatory access, incident reporting, subcontracting and exit arrangements. Performance shall be assessed periodically and deficiencies remediated promptly.

16. Internal Escalation and Reporting of Unusual Transactions

16.1 Internal Reporting

Any director, employee, contractor or service provider who knows, suspects or has reasonable grounds to suspect ML/TF/PF, sanctions evasion, unlawful gaming, fraud or another predicate offence must submit an internal unusual transaction report ("IUTR") to the AML Responsible Officer without delay. The report must include available supporting evidence and must not be filtered through a line manager if that would cause delay or a conflict.

The reporter must not continue investigating beyond their role, disclose the report, contact the counterparty about the suspicion, close the relationship, block funds, alter account access or take another unusual action unless instructed by the AML Responsible Officer or legally required.

16.2 Assessment and Decision

The AML Responsible Officer shall review the facts, applicable objective and subjective indicators, CDD, ownership, licensing, transaction history, related parties and available intelligence. The decision to report or not report, the reasons, supporting evidence, authorisation and subsequent controls shall be recorded.

The Company shall apply all unusual-transaction indicators legally applicable to its service-provider category and actual activity. Numerical indicators drafted for player or casino transactions shall be applied only where their legal scope covers the Company's transaction. Regardless of value, any completed or intended transaction giving cause to presume ML/TF/PF must be considered for reporting.

16.3 External Reporting to FIU Curaçao

Where the Company is a reporting entity and an unusual transaction or intended transaction is reportable under NORUT and applicable indicators, the AML Responsible Officer shall arrange reporting to FIU Curaçao without delay through goAML or the method required by FIU Curaçao. Reports and supporting information shall be complete, accurate, in the required language and securely retained.

The Company shall register with FIU Curaçao and maintain goAML access where required for its B2B licence and activities. If applicability is unclear, the AML Responsible Officer shall obtain written legal or regulatory guidance without delaying protective measures or a clearly required report.

16.4 CGA Incident Reporting

A report to FIU Curaçao does not replace a report to the CGA. Material AML/CFT/CPF, sanctions, fraud, integrity, system or funds incidents shall be assessed against the CGA incident-reporting requirements. Where an incident report is required, it shall be submitted within the deadline in the applicable supplier licence conditions, currently 24 hours after the incident.

17. Confidentiality and Prohibition of Tipping Off

STRICT RULE - NO TIPPING OFF

No person may tell a counterparty, employee without a need to know, vendor or other third party that an internal report or FIU report has been made or is contemplated, that FIU Curaçao has requested information, or that an AML investigation is underway. No unusual account, payment, access or relationship action may be taken in a way that is likely to reveal the report or investigation without approval.

Confidential information shall be restricted to personnel with a genuine need to know and stored separately from ordinary client files where appropriate. Communications must use neutral operational language approved by the AML Responsible Officer.

18. Holds, Restrictions, Rejection and Termination

Where CDD cannot be completed, risk becomes unacceptable, a sanctions issue arises or activity is unusual, the Company may defer activation, restrict services, hold a transaction, require further evidence, reject onboarding, suspend access or terminate the relationship, subject to law, contract, FIU/CGA directions and tipping-off risk.

Exit decisions shall address: protection of evidence; lawful treatment and return of funds; access and system security; data retention; regulator notification; outstanding player, jackpot or prize-pool obligations; continuity and wind-down; contractual rights; and whether enhanced monitoring is safer than immediate termination.

19. Record Keeping

The Company shall retain complete, accurate, secure and retrievable records sufficient to demonstrate compliance and reconstruct transactions. Unless a longer period is required, records shall be kept for at least five years:

- transaction records, domestic and international, from the date of the transaction;
- CDD, UBO, risk assessment, account, contract and business-correspondence records after the relationship ends or the occasional transaction occurs;
- sanctions, PEP and adverse-media screening results and resolution evidence;
- internal and external unusual transaction reports, decisions and supporting documents;
- monitoring alerts, investigations, overrides, approvals, restrictions and exit decisions;
- training content, attendance, testing and employee screening records;
- BRA versions, Board approvals, audit reports and remediation evidence; and
- outsourcing, reliance and vendor oversight records.

Records must be protected against unauthorised access, alteration, deletion or loss and must be available to competent authorities under lawful authority. A legal hold suspends normal deletion where litigation, investigation, reporting or regulatory review is pending.

20. Employee Screening, Conduct and Training

20.1 Screening and Fit-and-Proper Controls

The Company shall apply risk-based pre-employment and ongoing screening, including identity, qualifications, employment history, references, conflicts, sanctions, adverse media and criminal-record checks where lawful. Enhanced screening applies to directors, key persons, compliance staff, finance, payments, privileged-system users and personnel able to override controls.

20.2 Training

Training shall be provided at induction and at least annually, with additional role-specific and event-driven training. Content shall include Curaçao obligations, B2B risks, CDD/KYB, UBOs, PEPs, sanctions, proliferation financing, monitoring, unusual-transaction indicators, internal reporting, tipping off, record keeping, fraud, cyber-enabled crime and practical case studies.

The Company shall record the content, date, trainer, attendees, test results, remedial training and annual plan. Directors and senior management shall receive training appropriate to their oversight responsibilities.

20.3 Internal Misconduct and Whistleblowing

Suspected involvement of staff, directors or contractors in fraud, money laundering, sanctions evasion, control circumvention, unauthorised transactions, destruction of records or deliberate avoidance of due diligence must be reported directly to the AML Responsible Officer or, where conflicted, to an independent director or external legal counsel. The suspected person must not be confronted by unauthorised personnel.

21. Independent Testing and Quality Assurance

The AML/CFT/CPF programme shall be independently evaluated at least annually by an adequately resourced internal audit function or qualified external party that is independent of the activities tested. The review shall cover at least:

- governance, risk assessment and policy design;
- sample testing of CDD, UBO, risk ratings, EDD and approvals;
- sanctions and PEP screening effectiveness and match handling;
- transaction monitoring, alert disposition and unusual-transaction reporting;
- record retention, data integrity and regulatory access;
- training, employee screening and conflicts;
- outsourcing, reliance and vendor oversight;
- systems, rules, access, change control and audit logs;
- management information, escalation and Board oversight; and
- remediation of prior findings.

Findings shall be risk-rated, assigned to accountable owners, subject to deadlines and tracked to verified closure. Material findings shall be reported promptly to the Board and, where required, to the CGA.

22. Management Information and Regulatory Cooperation

The AML Responsible Officer shall provide the Board with regular management information appropriate to the size and risk of the business. It should include onboarding volumes, risk distribution, overdue reviews, screening matches, alerts, IUTRs, FIU reports, sanctions cases, rejected or exited relationships, training completion, audit findings, regulatory requests and emerging risks.

The Company shall cooperate fully and lawfully with the CGA, FIU Curaçao and other competent authorities. Information must be accurate, complete, timely and approved under the Company's regulatory-communications protocol. No person may conceal, falsify or improperly delay information requested by a competent authority.

23. Breaches, Enforcement and Consequences

A breach of this Policy may expose the Company and individuals to regulatory action, administrative fines, licence restrictions or revocation, criminal liability, civil claims, contractual loss and reputational harm. Employees may be subject to disciplinary action up to and including dismissal. Contractors and counterparties may be suspended or terminated.

Breaches and control failures must be reported promptly. The Company shall investigate root causes, preserve evidence, assess regulatory reporting, implement corrective action and verify effectiveness. Retaliation against a person who reports a concern in good faith is prohibited.

24. Review, Change Control and Availability

This Policy shall be reviewed at least annually and sooner following relevant legal, regulatory, licence, portal-checklist, ownership, product, market, technology, payment, outsourcing, incident, audit or risk changes. Material changes require Board approval. Procedures, monitoring rules, forms and training shall be updated consistently.

The current approved version shall be available to relevant personnel. Superseded versions shall be archived. The Company shall provide this Policy to the CGA on request.

Appendix A - B2B Risk Rating Matrix

The matrix below is a minimum template. The AML Responsible Officer may refine weightings following Board approval. Mandatory prohibited-risk overrides always prevail over the numerical result.

Risk factor	0 - Low	1 - Moderate	2 - Elevated	3 - High
Licensing and legality	Strong regulator; verified active licence	Licence verified; minor limitations	Weak/unclear oversight or recent issues	Unlicensed, expired, misleading or illegal
Ownership and control	Simple, transparent, verified	One holding layer; transparent	Complex or nominee elements; resolved	Concealed, unexplained or unverifiable
Geography	Low-risk and coherent	Cross-border but coherent	Higher-risk exposure or weak controls	Sanctioned/prohibited or implausible routing
Service/product	Low-value technical service; no funds	Standard B2B supply	White-label, reseller, wallet or funds exposure	Anonymity, evasion or unlawful end-use
Payments	Own regulated bank account; predictable	Multiple currencies; explained	Third-party/crypto/complex settlement	Untraceable, circular or unrelated flows
Regulatory/adverse history	None	Minor resolved issue	Material issue under remediation	Serious unresolved enforcement or criminal link
Delivery/outsourcing	Direct; controlled	Limited reputable vendors	Multi-tier reseller/outsourcing chain	Unknown sub-clients or uncontrolled onward supply
PEP/sanctions/PF	No exposure	Remote/low relevance	PEP or elevated PF exposure with controls	Confirmed sanctions prohibition or evasion concern

Suggested total: 0-5 Low; 6-11 Medium; 12-18 High; 19+ reject or exceptional Board review. This scoring does not override mandatory rejection criteria.

Appendix B - B2B KYB / CDD Checklist

Requirement	Received	Verified	Notes / expiry
Official registry extract / certificate of good standing	☐	☐	
Articles / constitutional documents	☐	☐	
Registered and operating address	☐	☐	
Gaming and relevant licences; approved domains	☐	☐	
Directors and authorised signatories	☐	☐	
Ownership chart to natural-person UBOs	☐	☐	
UBO identity and address documents	☐	☐	
PEP, sanctions and adverse-media screening	☐	☐	
Business model and intended use of services	☐	☐	
Target markets, domains, brands and resellers	☐	☐	
Expected payments, currencies, volumes and bank accounts	☐	☐	
Source of funds / source of wealth where required	☐	☐	
AML/CFT policy and compliance questionnaire where relevant	☐	☐	
Outsourcing and critical third parties	☐	☐	
Risk assessment and approval	☐	☐	
Contract compliance clauses and audit rights	☐	☐	

Appendix C - B2B Red Flags

- The client is reluctant to identify UBOs, directors, regulators, domains, markets or sub-clients.
- Ownership changes repeatedly or immediately before onboarding or payment.
- Corporate layers, nominees, trusts or offshore entities have no clear commercial purpose.

- The client claims a licence that cannot be verified, is expired, belongs to another entity or does not cover the activity.
- The client requests supply to hidden, cloned, unapproved or restricted domains or markets.
- Payments come from unrelated parties, personal accounts, high-risk jurisdictions or accounts inconsistent with the contract.
- Settlement instructions change frequently or funds are rapidly moved, refunded or routed onward.
- Invoices are split, misdescribed or disconnected from actual services.
- The client requests the Company to suppress, modify or avoid logs, KYC data, monitoring or regulatory disclosures.
- Revenue, traffic, game use, jackpot activity or settlement volumes are inconsistent or economically implausible.
- The client or its owners are linked to fraud, cybercrime, illegal gambling, corruption, sanctions evasion or other predicate offences.
- A reseller or aggregator refuses to disclose operators, brands, domains or onward customers.
- Crypto-assets are received from mixers, tumblers, privacy services, darknet exposure, stolen-funds clusters or sanctioned wallets.
- A staff member applies pressure to bypass CDD, alter a risk score, release a payment or ignore an alert.
- There is an unexplained mismatch between the contracting entity, licence holder, domain owner, bank account and system user.

Appendix D - Internal Unusual Transaction Report

Field	Information
Report reference	[Assigned by Compliance]
Date and time submitted	
Reporter name / role / contact	
Counterparty / related persons	
Relevant contract, account, domain or system ID	
Transaction(s), amount, currency, date and payment route	
Description of concern and why activity is unusual	
Relevant red flags / indicators	
Documents, screenshots, logs or links attached	
Immediate operational status	
Has anyone been contacted about the concern?	
Compliance assessment and decision	[For Compliance use]
FIU report reference / date	[For Compliance use]
CGA incident report reference / date	[For Compliance use]
Restrictions, monitoring or exit action	[For Compliance use]

Confidential

Submit directly to the AML Responsible Officer. Do not inform the counterparty or unnecessary personnel. Do not place the report in an ordinary client-facing CRM record if the counterparty can access it.

Appendix E - Minimum Contractual AML Clauses

- representation that the counterparty and its operations are lawful and appropriately licensed;
- obligation to disclose ownership, control, licence, domain, market, bank, wallet and material business changes promptly;
- prohibition on use of services for illegal, sanctioned, unauthorised or undisclosed activities;
- obligation to provide CDD, transaction, source-of-funds and compliance information promptly;

- right to screen, monitor, audit and verify information, including through regulators and independent sources;
- right to restrict, suspend, withhold, reject or terminate where compliance concerns arise, subject to law;
- cooperation with regulatory, sanctions, FIU and law-enforcement obligations;
- flow-down requirements for resellers, sub-clients and outsourced providers;
- record retention, data integrity, security and regulatory-access obligations;
- incident notification, subcontracting approval and change-control obligations; and
- indemnity and termination rights for false statements, concealment, unlawful use or compliance breaches.

Appendix F - Regulatory Reference List

- [CGA - Supplier License Conditions \(indefinite-term supplier licence; effective 22 December 2025\)](#)
- [CGA - AML Policy: Document Template for License Applicants and Holders \(30 January 2026\)](#)
- [CGA - Regulations for combating Money Laundering, Terrorist Financing and Proliferation Financing \(January 2025\)](#)
- [CGA - Requirements for Compliance Officer Based on NOIS/NORUT \(January 2025\)](#)
- [CGA - National Ordinance on Identification in Service Provision \(NOIS / LID\), PB 2017 no. 92, as amended](#)
- [CGA - National Ordinance on Reporting Unusual Transactions \(NORUT / LMOT\), PB 2017 no. 99, as amended](#)
- [CGA - Regulation Indicators Unusual Transactions and amendments](#)

Accessed for drafting on 22 July 2026. The Company must use the current official Dutch text where there is any conflict with an English translation and must monitor later amendments, policies, instructions and portal checklist conditions.

Appendix G - Source Policy Adaptation Record

The attached source was the eight-page “TC Entertainment N.V. Anti-Money Laundering Procedure” dated 29 September 2020. The source contained useful principles concerning designated responsibility, annual review, monitoring, KYC, unusual transactions, payment controls, record keeping, internal suspicious-activity escalation, tipping off and internal staff fraud. This document preserves those principles but materially changes the policy to:

- refer to Balkan International N.V.;
- address a B2B supplier rather than a player-facing operator;
- replace Malta/European and FIAU references with the applicable Curaçao framework and FIU Curaçao;
- incorporate the LOK, NOIS, NORUT, sanctions and CGA supplier-licence framework;
- add proliferation financing, sanctions freezing, B2B KYB, UBO, counterparty risk, outsourcing and annual independent audit controls; and
- remove player-deposit, withdrawal and gaming-day procedures that are not automatically relevant to a B2B supplier.