

CORPORATE AML/CFT/CPF POLICY

NETGAME ENTERTAINMENT N.V.

TABLE OF CONTENTS

1. INTRODUCTION.....	2
1.1. Purpose.....	3
1.2. Scope	3
1.3. History	4
1.4. Responsibilities	4
1.5. Regulatory Framework	4
2. RISK-BASED APPROACH	5
3. OPERATOR DUE DILIGENCE (ODD)	5
3.1. General Principles.....	5
3.2. ODD Risk Categories	6
3.3. Identification and Verification	6
3.4. Ongoing Monitoring and Refresh	7
4. TRANSACTION MONITORING	7
5. SUSPICIOUS ACTIVITY REPORTING.....	8
6. SANCTIONS SCREENING	9
7. RECORD-KEEPING	11
8. TRAINING	12
9. TIPPING-OFF PROHIBITION	13
10. POLICY REVIEW AND EXCEPTIONS.....	13
10.1. Policy Review	13
10.2. Exceptions.....	14

1. INTRODUCTION

1.1. Purpose

This Anti-Money Laundering and Counter-Terrorist Financing Policy (the "Policy") sets out the framework adopted by NetGame Entertainment N.V. (the "Company") to prevent, detect, and report money laundering, terrorist financing, proliferation financing, and related financial crime.

The Company operates as a Business-to-Business (B2B) gaming technology and software provider licensed by the Curaçao Gaming Authority (CGA) under the National Ordinance on Games of Chance (Landsverordening op de Kansspelen, "LOK"). The Company provides gaming platform software, game content, and related technology services to licensed online gaming operators. The Company does not operate end-player-facing gaming services directly; however, by providing enabling technology to operators, it recognises its exposure to financial crime risk and its obligation to implement appropriate controls.

The Policy is intended to:

2. define the Company's obligations under applicable AML/CFT/CPF law and CGA licensing conditions;
3. establish the risk-based approach applied to identify, assess, and manage AML/CFT risk;
4. set out the procedures for operator due diligence, transaction monitoring, suspicious activity reporting, sanctions screening, and record-keeping;
5. assign responsibilities to the Compliance Officer and all relevant personnel;
6. ensure that the Company meets the standards expected by the CGA and acts consistently with international AML/CFT/CPF best practice, including the FATF Recommendations on counter-proliferation financing.

1.2. Scope

This Policy applies to:

- all employees, directors, officers, and contractors of NetGame Entertainment N.V.;
- all B2B client relationships with gaming operators and other business partners;
- all jurisdictions in which the Company provides services or has business relationships.

This Policy does not govern end-player due diligence. That obligation rests with the licensed gaming operators to whom the Company provides its technology. However, the Company recognises that its technology facilitates operator activity and maintains appropriate controls at the B2B level.

1.3. History

Version	Description	From	Author
1.0	Initial version	9 th November 2025	CCO

1.4. Responsibilities

Role	Responsibilities
Board of Directors / Senior Management	Ultimate accountability for AML/CFT compliance. Approves this Policy. Ensures adequate resources for compliance. Reviews periodic AML reports.
Compliance Officer	Day-to-day responsibility for AML/CFT compliance. Receives and evaluates internal Suspicious Activity Reports (SARs). Decides on external reporting to the FIU. Maintains AML records and registers. Ensures training delivery. Liaison with the CGA and authorities.
Legal Team	Advises on emerging regulatory obligations. Reviews complex cases with potential legal exposure. Supports regulatory correspondence.
Finance Team	Implements payment controls. Flags unusual financial transactions for compliance review. Supports transaction monitoring.
All Employees	Complete mandatory AML training. Report suspicions to the Compliance Officer. Comply with this Policy at all times.

1.5. Regulatory Framework

This Policy is adopted in accordance with:

- National Ordinance on Games of Chance (LOK 2024)
- National Ordinance on the Reporting of Unusual Transactions (NORUT)
- National Ordinance on the Identification of Clients when Rendering Services (NOIS)
- Sanctions National Ordinance and Kingdom Sanctions Act
- CGA AML/CFT Regulations (2025)
- Ministerial Decree on Indicators of Unusual Transactions (N.G. 2015, no. 73)
- FATF Recommendations

2. RISK-BASED APPROACH

The Company applies a risk-based approach to AML/CFT compliance in accordance with FATF Recommendations and CGA requirements. The risk-based approach means that resources and controls are allocated in proportion to the level of AML/CFT risk identified.

The Company's AML/CFT risk assessment considers:

- the nature and scale of the Company's business as a B2B technology provider;
- the jurisdictions in which the Company operates and in which its operator clients are licensed;
- the characteristics and risk profiles of its B2B client base;
- the channels through which services are delivered and payments are received;
- emerging money laundering, terrorist financing, and proliferation financing typologies and intelligence relevant to the online gaming sector.

A formal AML/CFT/CPF Risk Assessment (Business Risk Assessment) is conducted annually by the Compliance Officer, documented, and approved by Senior Management. The Risk Assessment expressly addresses money laundering, terrorist financing, and proliferation financing risk, and is also carried out prior to the launch of any new product, business practice, delivery mechanism, or technology (technological development risk assessment). The Risk Assessment informs the level of due diligence applied to each operator relationship and the intensity of ongoing monitoring.

Risk factors that may increase the assessed risk level include:

- operator licensed in a jurisdiction with weak AML oversight or on the FATF grey/black list;
- complex or opaque ownership structures;
- operating in markets with elevated corruption or financial crime risk;
- prior regulatory sanctions or adverse media coverage;
- unusual commercial terms or payment structures.

3. OPERATOR DUE DILIGENCE (ODD)

3.1. General Principles

Before entering into a business relationship with any gaming operator or other business partner, the Company must conduct Operator Due Diligence (ODD). The extent of ODD applied depends on the risk rating assigned to the operator following a preliminary risk assessment.

No business relationship may be established, and no services may be provided, until satisfactory ODD has been completed and approved by the designated Compliance Officer.

3.2. ODD Risk Categories

Risk Category	Indicators	Required Measures
Standard Risk	Licensed operator in a recognised jurisdiction. Clear and transparent ownership. No adverse media or enforcement history.	Standard ODD: licence verification, UBO identification, T&C review, annual refresh.
Enhanced Risk	Operator licensed in a jurisdiction with weaker AML oversight. Complex ownership structure. Previous regulatory findings. Jurisdiction on FATF grey list.	Enhanced ODD: source of funds, full UBO chain to natural persons, senior management background checks, increased monitoring frequency.
High Risk / Prohibited	Unlicensed operator. Jurisdiction on FATF black list. Operator on sanctions lists. Material deception in onboarding disclosures.	Relationship not permitted. Existing relationship terminated. Compliance Officer notified immediately.

3.3. Identification and Verification

Standard ODD for all B2B operators must include, at a minimum:

- verification of the operator's legal name, registered address, and jurisdiction of incorporation;
- confirmation that the operator holds a valid gaming licence from a recognised regulatory authority;
- identification and verification of Ultimate Beneficial Owners (UBOs) holding 25% or more ownership or control - or 10% where enhanced due diligence applies;
- identification of directors and senior managers;
- assessment of the operator's own AML/CFT framework where available;
- screening of the operator, its UBOs, and senior management against sanctions lists and adverse media sources;
- review and acceptance of the operator's terms and conditions.

Where the operator is itself a regulated entity subject to AML/CFT supervision in a recognised jurisdiction, the Company may apply proportionate reliance on that entity's controls, subject to Compliance Officer approval and documented rationale.

3.4. Ongoing Monitoring and Refresh

Operator relationships are subject to ongoing monitoring to ensure that the risk profile remains consistent with the initial assessment. The refresh cycle is risk-based:

- High-risk operators: annual full review;
- Standard-risk operators: review every two years, or sooner if triggered by a material change;
- Triggered refresh upon: change in ownership, adverse media findings, enforcement action, jurisdiction change, or significant change in commercial activity.

Failure to provide updated documentation within the required timeframe may result in suspension of services pending receipt of the required information.

4. TRANSACTION MONITORING

The Company monitors commercial transactions with its B2B operator clients for indicators of unusual or suspicious activity. Monitoring is applied to:

- settlement payments received from operators;
- payment routing, counterparties, and currency of settlement;
- material changes in commercial volumes or payment patterns.

Red flag indicators that may trigger further review include:

Category	Red Flag Indicators
Onboarding	Resistance to providing KYC/ODD documentation. Unusual urgency to commence the commercial relationship. Inconsistencies between declared ownership and public records. Use of complex legal structures with no apparent commercial rationale.
Transaction Activity	Settlement patterns inconsistent with agreed commercial terms. Payments routed through unexpected or unrelated third parties.

Corporate AML/CFT/CPF Policy – NetGame Entertainment N.V.

	Unusual volumes, frequencies, or transaction sizes with no business explanation. Requests to split or route payments in a manner that obscures their origin.
Jurisdiction and Counterparty	Operator domiciled in a high-risk or non-cooperative jurisdiction. Ultimate beneficial owners located in FATF grey/black-listed countries. Adverse media coverage linking operator or UBOs to financial crime, fraud, or corruption.
Behavioural	Unexplained changes in ownership or business model following onboarding. Failure to respond to refresh or remediation requests. Pressure on staff to approve transactions or bypass controls.

Where a transaction alert is generated, the relevant employee escalates to the Compliance Officer for review. The Compliance Officer determines whether the alert warrants further investigation or an internal SAR. All alerts and outcomes are logged in the Transaction Monitoring Register.

The Company reviews and updates its monitoring parameters periodically to reflect emerging typologies and any changes to the operator risk profile

5. SUSPICIOUS ACTIVITY REPORTING

All employees have a legal and policy obligation to report knowledge or suspicion of money laundering or terrorist financing to the Compliance Officer without delay. The process for doing so is set out below.

Step	Action	Detail
1	Internal report submitted	Any employee who identifies a suspicion submits an internal SAR to the Compliance Officer using the prescribed form. The report must not be discussed with the subject of the suspicion (tipping-off prohibited).
2	Compliance Officer review	The Compliance Officer reviews the internal SAR within 5 business days. The Compliance Officer may request additional information from the reporting employee or from the Compliance Team.
3	Decision	The Compliance Officer decides whether: (a) to make an external disclosure to the FIU; (b) to file and monitor

Corporate AML/CFT/CPF Policy – NetGame Entertainment N.V.

		without disclosure; or (c) to dismiss the report as not meeting the threshold. All decisions are documented with rationale.
4	External disclosure (if applicable)	Where disclosure is required, the Compliance Officer submits a report of the unusual transaction to the Curaçao Financial Intelligence Unit (FIU / MOT) in accordance with the NORUT and the Ministerial Decree on Indicators of Unusual Transactions, applying both the objective indicators (including the reporting threshold of XCG 5,000, or its equivalent in another currency, where applicable to the transaction concerned) and the subjective indicator (any transaction giving rise to a suspicion of money laundering, terrorist financing, or proliferation financing). A consent request may be made if a transaction is pending.
5	Record-keeping	All internal SARs, Compliance Officer decisions, and external disclosures are recorded in the SAR Register and retained for five years.

Employees must not take any unilateral action in response to a suspicion. In particular, employees must not:

- directly challenge or accuse the counterparty;
- tip off the subject of the suspicion that a report has been or may be made;
- take any action that could compromise an investigation.

No employee will suffer any adverse consequence for making a good-faith internal SAR, even if the report is subsequently dismissed by the Compliance Officer.

6. SANCTIONS SCREENING

The Company screens all operators, their UBOs, directors, and senior management against applicable sanctions lists before and during the business relationship. Sanctions are restrictions used by international communities as part of an attempt to stop financial crime and terrorism. They are designed as attempts to change the behavior of a targeted country, regime or individuals where diplomatic efforts have failed. Sanctions can take form of economic, trade,

financial services, or international movement (travel bans) prohibitions. The Company is obliged to comply with the sanction's regimes announced by the UK, UN and EU. Also, there is a possibility to include persons in the national sanction's regime.

UN

Sanctions

The United Nations Security Council publishes the names of individuals and organisations subject to UN financial sanctions in relation to involvement with ISIL (Da'esh), I-Qaeda, and the Taliban. All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities.

The UN has in place other sanction lists pertaining to other jurisdictions, entities and individuals, including wider terrorist activity under UNSR 1373. The UN consolidated sanctions list is available at the following link: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

EU

Sanctions

The European Union applies sanctions or restrictive measures in pursuit of the specific Common Foreign and Security (CFSP) objectives set out in the Treaty of the European Union. Restrictive measures imposed may incorporate UN Security Council sanctions or EU autonomous sanctions. The latter cannot be imposed against individuals or entities where there is no foreign policy dimension.

Link to the EU sanctions regime: <https://www.sanctionsmap.eu/#/main>

The above-mentioned website also includes information about the UN sanctions regimes.

UK

Sanctions

The Company does not enter into any transaction with individuals, companies and countries that are on UK sanction's list.

Link to the EU sanctions regime: <https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation>

OFAC

Sanctions

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on the US foreign policy and national security goals against targeted foreign countries and regimes; terrorists; international narcotics traffickers; and those engaged in activities related to the proliferation of weapons of mass

destruction; and other threats to national security, foreign policy or the economy of the US. It is important to note that while US sanctions do not directly apply to non-US companies outside the US, the use of the US dollar currency automatically engages OFAC regulations. US prosecutors take the view that if a financial transaction has clear in the US (as do all US dollar payment, in the New York), the US has jurisdiction over the offense. OFAC publishes a list of 'specially designated nationals' or SDNs (known as the SDN List) whose assets are blocked and firms, including US persons, are generally prohibited from doing business with them.

The OFAC Sanctions List Search is available at the following link:
<https://sanctionssearch.ofac.treas.gov/>

Australia

Sanctions

The Company does not enter into any legal relationship with individuals, companies and countries that are on Australia sanctions list. Information about the Australian Sanctions can be accessed via <https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list>.

A Politically Exposed Person (PEP) is generally considered to present a higher risk to a business with whom they are transacting due to being considered more vulnerable to bribery and corruption.

Therefore, full enhanced due diligence must be conducted upon any identified PEPs. The Company does not distinguish between foreign and domestic PEPs, all are considered high risk. A PEP that no longer holds their prominent public role will also be deemed high risk.

Screening is undertaken by the Company internally with the help of automated back end tools as well as using third party KYC service providers to identify PEP and Sanctioned individuals upon customer registration/deposit. This will also pick up on any adverse media relating to the customer.

A PEP is defined as a natural person who is or has been entrusted with prominent public functions, including:

- A head of state, head of government, minister or deputy or assistant minister;
- A senior government official;
- A Member of Parliament (MP);
- A senior politician;
- An important political party official;
- A senior judicial official;
- A member of a court of auditors or the board of a central bank;

- An ambassador, chargé d'affaires or other high-ranking officer in a diplomatic service;
- A high-ranking officer in an armed force;
- A senior member of an administrative, management or supervisory body of a State-owned enterprise;
- A senior official of an international entity or organization.

7. RECORD-KEEPING

The Company retains all AML/CFT records for a minimum of five (5) years from the date of the relevant transaction, the termination of the business relationship, or the submission of a report - whichever is the later. Longer retention periods apply where required by applicable law or regulatory direction.

Records retained include:

- operator identification and verification documents (ODD files);
- UBO and director identification documents;
- risk assessment records for each operator relationship;
- transaction monitoring alerts and outcomes;
- internal SARs and Compliance Officer decisions;
- external STR disclosures to the FIU;
- sanctions screening results;
- training attendance records and materials;
- AML/CFT Risk Assessment (annual).

Records are stored securely in electronic form with access restricted to authorised personnel. Records are made available to the CGA or other competent authorities upon request.

8. TRAINING

The Company is committed to ensuring that all relevant personnel receive appropriate AML/CFT training commensurate with their role and exposure to financial crime risk.

Audience	Training Content	Frequency
----------	------------------	-----------

Corporate AML/CFT/CPF Policy – NetGame Entertainment N.V.

All new employees	AML/CFT fundamentals, the Policy, tipping-off prohibition, how to raise a SAR.	Within 30 days of joining.
All employees	AML/CFT refresher: regulatory updates, case studies, emerging typologies.	Annual.
Compliance, Legal, Finance	Advanced AML: operator due diligence, risk assessment, transaction monitoring, SAR process.	Annual plus as needed.
Compliance Officer	Specialist AML training: FIU reporting obligations, regulatory developments, sector typologies.	Annual – external course preferred.

Training completion is recorded and maintained by the designated Compliance Officer. Failure to complete mandatory training may result in disciplinary action.

Training content is reviewed and updated annually, or sooner where there are material changes to the regulatory framework, CGA guidance, or emerging typologies in the B2B gaming sector.

9. TIPPING-OFF PROHIBITION

It is strictly prohibited for any employee to disclose to any person, including the subject of a suspicion, that:

- a suspicion has been formed;
- an internal SAR has been submitted to the Compliance Officer;
- an external STR has been submitted to the FIU;
- an investigation is underway or contemplated.

This prohibition exists under applicable AML legislation and its breach may constitute a criminal offence. Employees who are uncertain whether a particular disclosure would constitute tipping-off must consult the Compliance Officer before making any communication.

Employees are not prohibited from seeking legal advice in relation to a suspicion or from complying with a court order or formal regulatory requirement to disclose information.

10. POLICY REVIEW AND EXCEPTIONS

10.1. Policy Review

This Policy takes effect on the date of approval recorded in the Acceptance section below and, unless revised earlier, has a next scheduled review date twelve (12) months thereafter. This Policy is reviewed by the CCO (Compliance Officer) and approved by Senior Management on an annual basis, or earlier if:

- there is a material change in CGA requirements or applicable law;
- the Company's business model or client base changes materially;
- a significant AML/CFT incident or near-miss occurs;
- the annual Risk Assessment identifies a material change in the Company's risk profile.

All revisions are documented in the History table and communicated to relevant personnel.

10.2. Exceptions

Exceptions to any provision of this Policy may only be authorised by the CCO with the approval of Senior Management. Every exception must be documented, including:

- the date and nature of the exception;
- the rationale and risk assessment;
- any compensating controls applied;
- the individual who approved the exception.

Exceptions are recorded in the Policy Exceptions Register, which is reviewed by the CCO quarterly.

ACCEPTANCE

This Policy has been formally adopted by the Management of NetGame Entertainment N.V. and is binding on all operational units and employees.

Approved by

CCO Signature:  Date: 09.11.2025