

GRRR TECH B.V.

Anti-Money Laundering and Counter- Terrorism Financing Policy

Version 1.0

Table of Contents

1. Policy Statement.....	4
2. Purpose.....	5
3. Audience.....	6
4. Definitions.....	7
5. Policy Implementation	9
5.1. Risk-based approach (RBA)	9
5.2. Business Risk Assessment (BRA).....	9
5.3. Data processing system.....	10
5.4. Partner Risk Assessment (PRA)	10
5.5. Acceptance Criteria and Exclusion Rules for B2B Partners.....	11
5.6. Partner Due Diligence (PDD).....	12
5.5.1. Standard DD Procedure for B2B Partners.....	12
5.5.2. Enhanced Due Diligence (EDD).....	12
5.5.3. Prohibited Business Relationships	13
5.7. Ongoing Monitoring	13
5.8. Reliance on Third Parties for PDD (Outsource)	14
5.9. Anti-Money Laundering Compliance Program.....	15
5.8.1. Employee Training.....	16
5.8.2. Employee Background Checks:	18
5.8.3. Risk Assessment of New Products, Services, and Technologies	18
5.8.4. Internal and external audit and staying up-to-date	19
5.10. Individual Status.....	20
5.9.1. Document acceptance	22
6. Compliance and Consequences of Non-Compliance.....	23
6.1. Termination of Business Relations.....	25
6.2. External report to FIU.....	26
6.3. Reporting Indicators	26
Note: The Cg. 5,000 threshold resets per calendar gaming day.....	27
6.4. Reporting Procedure.....	27
6.4.1. Internal and External Reporting Timelines.....	27
6.5. Tipping-off	28

6.5.1. Internal Whistleblower Protection.....	28
7. Internal Control.....	28
7.1. Introduction.....	28
7.2. Recordkeeping.....	28
7.3. Money Laundering Reporting Officer	29
7.4. Regulatory Oversight.....	31
8. Contact Information.....	32
9. Policy History.....	33
10. Policy URL	34

Key Information

Approving Official(s):

- Director.
- e-Management N.V.

Responsible Office:

- Compliance Department.

Effective Date:

- 1 June 2025.

Next Review Date:

- 1 June, 2026 (initial review within one-year, subsequent reviews every three years).

1. Policy Statement

Grrr Tech B.V. ("the Company"), a Curaçao-incorporated (Registration No. 166739; Registration address: Emancipatie Boulevard, Dominico F. "Don" Martina 31, Willemstad, Curaçao; has a valid license issued by the Curaçao Gaming Authority), is committed to preventing its services, products, and facilities from being used for money laundering (ML), terrorist financing (TF), or the financing of proliferation of weapons of mass destruction (FP). The Company's Policy and Procedures have been developed in accordance with the relevant applicable legislation, including but not limited to the following:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025;
- The FATF Recommendations.

2. Purpose

This AML/CTF Policy ensures compliance with Curaçao's legal framework and international standards, including the "Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction" (effective January 9, 2025), FATF Recommendations, and EU Directives. The policy aims to:

- Protect the Company's reputation and operations from financial crime risks;
- Implement a risk-based approach to identify, assess, and mitigate ML/TF/FP risks;
- Ensure robust partner due diligence (PDD), know-your-business (KYB), transaction monitoring, and reporting of unusual activities;
- Establish procedures for screening and monitoring B2B partners to comply with the Company's requirements;
- Foster a culture of compliance through employee training, background checks, and internal controls;
- Prevent predicate offenses to ML/TF, such as fraud, as defined in EU Directive 2018/1673 and other legislative acts.

3. Audience

This policy applies to:

- All employees and outsourced staff involved in anti-money laundering, responsible remote gaming activity, and anti-fraud procedures as they relate to their respective duties, including senior management and the Compliance Officer of Grrr Tech B.V.
- Third-party service providers, agents, affiliates, and subcontractors involved in the Company's operations;
- B2B partners (business partners, such as platform providers or operators using the Company's services or the Company's platform);
- Collectively referred to as partners.

4. Definitions

- **Financial Transactions:** Deposits, withdrawals, wire transfers, and currency exchanges (excluding remote gaming transactions like wagers or winnings);
- **Financing of proliferation (FP):** the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials;
- **FIU:** Financial Intelligence Unit Curaçao, responsible for receiving unusual transaction reports (UTRs);
- **Politically Exposed Person (PEP):** Person who is or has been entrusted with a prominent public function at the international, national, regional, or local level. This includes, but is not limited to, heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned enterprises, and important political party officials. This includes but is not limited to individuals or entities associated with the restricted list of countries as per the Company's Terms and Conditions;
- **Ultimate Beneficial Owner (UBO):** Natural person(s) who own or control a partner or entity, holding $\geq 25\%$ shares/voting rights or exercising ultimate control;
- **Money laundering (ML):** Is the process of concealing the origins of illegally obtained money so it appears to come from a legitimate source;
- **Terrorist financing (TF):** Refers to the collection or provision of funds with the intention that they will be used, in whole or in part, to carry out terrorist acts. This includes:
 - Direct funding of terrorist operations (e.g., buying weapons, logistics);
 - Supporting terrorist organizations indirectly (e.g., through charities or legitimate businesses).

Feature	Terrorist Financing	Money Laundering
Source of Funds	Legal or illegal	Always illegal
Purpose	Support terrorism	Conceal the criminal origins of money
Legality of Funds	May be legal (e.g., charity donations)	Always illegal
End Goal	Political/ideological objectives	Financial gain

Feature	Terrorist Financing	Money Laundering
Amount Involved	Often, a small but significant impact	Often, large sums of money
Detection Challenge	Difficult due to legitimate funding sources	Complex transactions to obscure origins

There are three stages of money laundering:

- **Placement** – The introduction of illicit funds into the financial system, either directly or through indirect means such as blending with legitimate funds, committing invoice fraud, or using smurfing techniques;
- **Layering** – This phase focuses on distancing illegal proceeds from their origins by conducting a series of complex financial transactions. These layers are meant to obscure the audit trail and provide anonymity, often through multiple bank transfers or investing in cash-heavy businesses;
- **Integration** – The final stage is when criminally derived money is reintroduced into the economy, appearing legitimate. After successful layering, the funds are integrated into the financial system, for instance, through property purchases, making the illicit money seem legally earned.

The company strictly prohibits any activity that facilitates money laundering or the financing of terrorism, in accordance with applicable laws and regulations.

5. Policy Implementation

The Company adopts a risk-based approach to AML/CTF compliance, as mandated by the Curaçao Gaming Authority (CGA, formerly Curaçao Gaming Control Board) and FATF Recommendations. The following sections outline the implementation framework.

5.1. Risk-based approach (RBA)

The Company is committed to preventing and combating money laundering and terrorist financing by employing a risk-based approach. This approach is outlined in the following key areas:

- Risk identification and assessment – Identifying the money laundering risks the Company faces, considering its partner base, products, and services, as well as relevant available information, and evaluating the potential scale and impact of these risks;
- Risk mitigation – Implementing appropriate measures to reduce the significant risks that the Company may encounter;
- Risk monitoring – Establishing management information systems to continuously track changes in the risk profile, whether from business developments or evolving threats;
- Documentation – Recording the risk assessment and strategy, ensuring policies and procedures cover these areas, and securing effective accountability from the board and senior management.

The Company adopts an RBA to AML and CFT, in line with international best practices and regulatory expectations. This approach ensures that resources are focused where the risk of ML and TF is highest, thereby enhancing the overall effectiveness and efficiency of the compliance program.

5.2. Business Risk Assessment (BRA)

The BRA identifies and evaluates risks associated with the Company's overall operations, taking into account:

- The nature and complexity of products and services offered;
- The partners' base and target markets;
- Delivery channels (e.g., face-to-face, online, intermediaries);
- Geographical Risk: Geographic exposure, including countries of operation and counterparties (e.g., FATF High-Risk Jurisdictions <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>, EU Directive 2018/843 Annex II countries);

- Industry sectors involved;
- Partners Risk: PEPs, or partners with irregular income;
- Distribution Channel Risk: Risks from non-face-to-face interactions or third-party intermediaries.

BRA is conducted annually and updated upon significant changes (e.g., new products, markets, or regulations). The BRA is documented, approved by the Board of Directors, and submitted to the CGA upon request. Outcomes inform the Company's risk appetite and AML/CTF controls, ensuring alignment with FATF Recommendation 1 (risk-based approach).

For detailed information, the Company has a separate document dedicated to BRA for the purposes of the AML Compliance Program. It is a process whereby the Company identifies the threats and vulnerabilities to which it is exposed and assesses the likelihood and impact of ML/FT/FP risks.

5.3. Data processing system

The Company utilizes an internal data processing system to identify high-risk situations, detect money laundering, and monitor terrorist financing in its daily operations.

The data processing system includes the following components:

- Identification of all partners before entering into a business relationship requires them to complete a registration form to confirm their details;
- Politically Exposed Person (PEP) and sanction list checks, performed using specialized software;
- Reporting of all suspected money laundering cases to the Compliance Officer and the Financial Intelligence Unit (FIU).

The Company will continue to monitor trends and developments related to ML/TF and will introduce additional internal procedures as necessary to stay current.

5.4. Partner Risk Assessment (PRA)

The Company conducts a Partner Risk Assessment (PRA) for every B2B relationship established. The PRA evaluates the inherent risk posed by the partner based on factors such as:

- Jurisdiction of incorporation and operation;
- Ownership and control structure (including UBO thresholds $\geq 25\%$);
- Exposure to PEPs, sanctions, or adverse media;

- Business activity sector (including whether the partner offers player-facing gambling services);
- Prior regulatory history or enforcement actions.

PRA results inform the level of CDD/EDD required. The PRA is documented, retained for five years, and updated annually or when trigger events occur (e.g., changes in ownership or law).

5.5. Acceptance Criteria and Exclusion Rules for B2B Partners

Objective: To define the criteria for accepting or rejecting B2B partners in accordance with the Company's RBA to AML and CFT, and to ensure that all relationships align with the Company's compliance standards and risk appetite.

Acceptance and Classification Procedure:

- The Partner Acceptance Policy (PAP) sets out criteria for onboarding B2B partners based on their risk profile and jurisdiction.
- Partners are classified as:
 - High-Risk: Entities owned or controlled by PEPs, sanctioned individuals or entities, or those based in FATF-listed high-risk jurisdictions;
 - Standard or Enhanced CDD Measures: Applied based on the assessed risk level. SDD is used for low-risk partners, while EDD is mandatory for high-risk partners.

Grounds for Rejection of B2B Partners:

- B2B partners shall be rejected or offboarded if:
 - They fail to maintain adequate and effective AML/CFT policies, procedures, and internal controls;
 - They are directly or indirectly owned or controlled by any PEP;
 - They are non-compliant with applicable Curaçao regulatory requirements;
 - They are incorporated in, or primarily operate from, jurisdictions subject to FATF blacklisting;
 - They provide anonymous or pseudonymous account services;
 - They are linked to or suspected of involvement in terrorist financing, organized crime, or corruption;
 - They fail or refuse to provide complete and accurate KYB documentation;
 - They rely on third parties or proxy arrangements to conceal true ownership or

control.

5.6. Partner Due Diligence (PDD)

Objective: To verify the identity and legitimacy of B2B partners and to mitigate risks related to ML, TF, and FP, in line with the Company's RBA.

5.5.1. Standard DD Procedure for B2B Partners

The Company applies SDD measures for all business partners entering into legal relations. The SDD process consists of the following:

- Identification – Collecting key corporate information to establish the identity of the business partner, including legal name, registration number, registered office address, ownership structure, and key management personnel.
- Verification – Confirming the authenticity of the provided information through reliable and independent sources, such as official company registers, regulatory filings, or certified corporate documents.

5.5.2. Enhanced Due Diligence (EDD)

The Company shall apply Enhanced Due Diligence (EDD) measures in accordance with the risk-based approach and applicable regulatory requirements where the business relationship or transaction presents a higher risk of money laundering, terrorist financing, or proliferation financing.

EDD is mandatory in the following situations:

- Where the corporate partner is established in or operating from a high-risk third country as designated by the FATF or the CGA;
- Where the ownership structure of the entity is complex or opaque, especially where ultimate beneficial ownership cannot be easily verified or traced;
- Where the corporate partner is associated with politically exposed persons (PEPs), either directly or indirectly through its ownership, control, or management;
- Where the corporate partner provides services that enable anonymity, such as cryptocurrency mixing or unregulated digital asset services;
- Where the partner has been subject to adverse media, enforcement actions, or regulatory sanctions;
- Where red flags are raised during ongoing monitoring or transaction reviews.

The Company may also apply EDD where otherwise deemed necessary based on the results of its Partner Risk Assessment (PRA) or at the discretion of the Compliance Officer.

EDD measures may include, but are not limited to:

- Obtaining additional information on the partner's business activities, financial statements, and source of funds or wealth;
- Conducting enhanced verification of the identity and background of beneficial owners and senior management;
- Requiring notarized or independently certified documents;
- Performing independent background checks (e.g., adverse media screening, corporate registry validation);
- Requiring senior management approval before establishing or continuing the business relationship;
- Increasing the frequency and depth of ongoing monitoring and transaction analysis.

The rationale for applying EDD and the steps taken shall be documented and retained for at least five (5) years in accordance with applicable recordkeeping obligations.

5.5.3. Prohibited Business Relationships

The Company will not establish or maintain business relationships with corporate partners or their beneficial owners involved in any of the following activities, regardless of jurisdiction:

- Provision of anonymous or pseudonymous account services, or use of technologies that prevent proper identification of the client;
- Direct or indirect links to known or suspected terrorist organizations, organized crime networks, or individuals/entities involved in corruption or financial crime;
- Failure or refusal to provide adequate KYC and corporate due diligence documentation, including information on ownership and control structure;
- Use of intermediaries, nominees, or proxy arrangements that obscure the identity of the ultimate beneficial owners;
- Inability to independently verify the source of funds or source of wealth used in the business relationship;
- PEPs, sanctioned entities or individuals.

5.7. Ongoing Monitoring

Objective: To ensure that the activities of B2B partners remain consistent with their assessed risk profile and to detect any unusual or non-compliant behavior in a timely manner.

Ongoing Monitoring Procedures:

- **Transaction Monitoring:** The Company continuously monitors the transactions and operational behavior of B2B partners to ensure compliance with applicable AML and CFT obligations;
- **Periodic Audits:** The Company conducts reviews or audits of B2B partners' internal AML/CTF controls, policies, and procedures to assess their effectiveness and identify potential deficiencies;
- **Risk Reassessment:** The Company re-evaluates the risk profile of each B2B partner upon material changes, including contract renewals, significant business changes, or updates to relevant laws or regulations;
- **Document Updates:** Where identification or verification documents have expired or are no longer valid, the Company requests updated documentation. This requirement is applied using a risk-based approach, with higher-risk partners subject to more frequent reviews.

As part of its general due diligence obligations, the Company ensures that information and documentation relating to B2B partners are kept current and accurate. Ongoing Customer Due Diligence (CDD) is performed at least once every 12 months, or more frequently where warranted by the partner's risk classification or at the Company's sole discretion.

5.8. Reliance on Third Parties for PDD (Outsource)

The Company may engage outsourced employees or third-party personnel to perform specific operational or support functions, including but not limited to partner identification, verification, and the collection of data regarding the nature and purpose of the business relationship.

Where such personnel are engaged, the Company shall ensure that all individuals with access to partner data, financial transactions, or AML&CFT-relevant systems are subject to the same compliance standards, obligations, and controls as internal staff.

All outsourced personnel must fully comply with the Company's AML&CFT Policy, internal procedures, and Code of Conduct, and shall be considered an integral part of the Company's AML compliance framework. Under no circumstances shall any outsourcing arrangement compromise the Company's ability to fulfill its legal or regulatory obligations.

Pre-Onboarding Requirements:

All outsourced personnel must undergo appropriate screening, including background checks and qualification verification, in line with the Company's HR protocols and AML risk assessment criteria.

Training & Competency:

Outsourced personnel must complete initial and periodic AML&CFT training tailored to their role, covering:

- PDD and KYC obligations.
- Identification and escalation of unusual transactions;
- Recordkeeping, confidentiality, and data protection requirements;
- Internal supervision and monitoring processes.

Access Control & Confidentiality:

- Outsourced personnel shall be granted access only to those systems and data strictly necessary for the performance of their duties;
- All outsourced individuals must sign confidentiality and data protection agreements and adhere to applicable AML&CFT data handling and retention policies.

Oversight & Enforcement:

- The Company shall ensure effective supervision and ongoing monitoring of outsourced personnel. Designated managers are responsible for ensuring that such individuals adhere to relevant internal controls and escalation protocols;
- Any breach of AML&CFT obligations by outsourced staff shall be addressed without delay and may result in:
 - Termination of the outsourcing arrangement;
 - Disciplinary action, and/or;
 - Reporting to the relevant regulatory or enforcement authority.

Additional Controls:

- The effectiveness of outsourcing arrangements shall be tested periodically as part of the Company's internal compliance review;
- The Company retains full responsibility for conducting Critical Risk Assessments (CRA), PEP screening, and ongoing monitoring of all B2B relationships;
- Third-party CDD may only be accepted for B2B partners incorporated in jurisdictions with equivalent AML&CFT standards;
- Where agents are used, the Company's AML&CFT policies must be fully applied, including the conduct of regular compliance audits of outsourced operations.

5.9. Anti-Money Laundering Compliance Program

Objective: Establish a robust framework to mitigate ML/TF/FP risks.

Procedure:

- **Internal Policies and Controls:**

- Policies express senior management's commitment to AML/CTF compliance;
- Procedure's detail KYB, reporting, and monitoring processes;
- Internal controls detect deviations (e.g., automated transaction monitoring);

- **Compliance Officer:**

- A senior officer, independent from gaming operations, oversees the AML program;
- Responsibilities include risk analysis, policy development, training, UTR submission, and FIU liaison;
- The officer has the authority to issue instructions and conduct random checks.

5.8.1. Employee Training

The Company will ensure that all relevant employees receive training on AML and CTF policies and procedures, emphasizing awareness of these risks. All applicable employees must pass competency assessments on these topics.

Upon joining the Company, and subsequently, on an annual basis, all staff (including outsourced teams) will receive training on AML/CFT procedures and related policies. This training will be delivered either through online and in-person training providers or by the Company's designated specialist. Employees selected for training will be determined based on individual risk assessments.

The Company provides training to all staff, either directly or through a service provider, upon joining the Company and annually thereafter.

Training materials will be specifically prepared for each team, aligned with the Company's policies, which are developed according to applicable legislation and guidelines.

Training will be conducted as follows:

- Training materials will be based on the finalized and approved Company policies and presented as documents and presentations;
- Training will be provided to current management and staff, either in a classroom setting or online;
- Training will also be included as part of the onboarding process for all new staff;

- After training, employees will complete a questionnaire to assess their understanding;
- If any issues remain unclear, the Company will repeat the training, focusing on areas that need further clarification;
- Regular refresher training will be provided, covering updates and addressing any shortfalls identified during the previous period;
- Any updates in policy will be communicated via group email and ad-hoc training, and included in periodic training updates and materials;
- Staff training will focus on raising awareness of the following:
 - All applicable legislation;
 - Provisions related to money laundering and terrorist financing requirements;
 - Staff's personal obligations under money laundering and terrorist financing laws;
 - Applicable internal reporting procedures;
 - The Company's policies and procedures for preventing money laundering and the financing of terrorism;
 - Identification and verification procedures, record-keeping, and other relevant processes;
 - Recognition and handling of unusual transactions;
 - Staff's liability for failing to report information or suspicions in accordance with money laundering and terrorist financing requirements and internal procedures;
 - New developments, including current techniques, methods, and trends in money laundering and terrorist financing;
 - Money laundering and terrorist financing risks faced by the Company;
 - The risks and controls related to any new or developing technologies or products.
 - Data protection regulations;

Induction training will be provided for all employees and will include training on fraud prevention, detection, and other relevant areas as required for their role. Refresher training will be regularly conducted, as well as when needed, to keep staff informed of the Company's policies, procedures, and any updates or improvements.

The Money Laundering Officer is responsible for keeping records of all training sessions, documenting what training was provided, when, by whom, and when the next training is scheduled. Should any changes to the Company's policies, procedures, or

relevant legislation occur, all staff will receive updated training.

5.8.2. Employee Background Checks:

Before engaging employees, the Company will conduct relevant integrity checks based on the employee's position, responsibilities, and access levels. The Company will not employ individuals who are not considered fit and proper for their role.

For this purpose, the Company may request the following documents (while ensuring compliance with data protection regulations):

- A valid original identity document;
- CV (Curriculum Vitae);
- Any other documents the Company deems necessary.

Once employed, employees will be screened on an ongoing basis as needed. All employees must adhere to applicable legislation, fulfil due diligence obligations, report any information relevant to money laundering, and ensure they do not engage in or facilitate unusual transactions, either actively or passively.

Senior management will regularly conduct checks on employees or whenever deemed necessary by the Company. These inspections, particularly when suspicion arises regarding an employee's behaviour, may be carried out through surprise spot checks or other procedures to verify compliance with the Company's policies and procedures.

The frequency and scope of screening will be proportionate to the employee's risk level, which will be determined on a case-by-case basis, depending on factors such as their position (e.g., department head, senior, mid-level), responsibilities, and obligations.

All employees will be checked at least once per year. The Company will use an employee performance sheet for this purpose.

5.8.3. Risk Assessment of New Products, Services, and Technologies

This section of the AML policy ensures that the Company proactively assesses and mitigates ML and TF risks associated with new technologies, products, services, or delivery mechanisms before implementation.

These conditions apply to all departments and personnel involved in the development, approval, or deployment of:

- New products or services;
- New business practices;
- New delivery mechanisms;
- New or developing technologies.

The assessment must:

- Identify potential ML/TF risks associated with the innovation;
- Evaluate existing controls and whether they sufficiently mitigate the identified risks.

Each risk assessment must be reviewed by the Compliance Officer and retained for a minimum of five (5) years.

No new product, practice, delivery mechanism, or technology may be launched without approval of the documented risk assessment by the Compliance Officer.

5.8.3.1. Fraud red flags

The Company has an anti-fraud risk management system designed to prevent various forms of fraud, including bot attacks, fraudulent traffic, synthetic identities, account takeovers, identity theft, credit card and CNP fraud, proxy users, multi-accounting, and collusion. Some fraud red flags may also be linked to potential money laundering.

5.8.4. Internal and external audit and staying up-to-date

The Company has developed its policies and procedures in accordance with applicable legislation and the guidance of the FATF, CGA, and FIU. However, both regulatory requirements and external fraud trends are subject to change. To ensure the ongoing relevance of the Company's internal AML documentation, the following measures have been implemented:

- Key personnel have subscribed to mailing lists from the FIU, CGA, and FATF and have joined relevant forums to stay informed;
- The Company periodically consults Remote gaming industry specialists for legal advice on AML best practices.
- In the event of an update, the Company will take the following actions as necessary:
 - Update internal policy documentation and training materials;
 - Notify relevant staff via email of any updates, meet with team managers, and ensure they inform their teams appropriately;
 - Update email communication templates and chat canned responses.

The Company may also engage a third-party service provider specialising in AML compliance to conduct independent external reviews of its AML policies and procedures. The results of these reviews will be reported to senior management and used to enhance the Company's AML/CTF measures and documentation as needed. The frequency of these external reviews will be determined by senior management. They may occur annually or more frequently, depending on the need for updated assessments of the AML program's effectiveness.

5.10. Individual Status

Politically Exposed Person (PEP)

A PEP is a natural person who is or has been entrusted with a prominent public function at the international, national, regional, or local level. This includes, but is not limited to, heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state-owned enterprises, and important political party officials.

The Company uses the KYC software tool to check all new partners at the registration stage against the PEP and Sanctions databases. The Company also checks the whole partners database every week to ensure existing partners have not changed their status.

Any new or existing partner found on the Sanctions database, or a PEP or relative of such, will have their account rejected or closed.

If a PEP is identified, responsible staff will send a report to the Compliance Officer, who in turn will send a report to senior management.

The Compliance Officer will investigate each case to identify positive or false-positive PEP alerts. The Company has the right to request additional documents from the partner during the investigation.

If the PEP alert is true-positive, the Compliance Officer will reject registration or close the account and inform senior management about the decision.

Politically Exposed Person means any person who has been entrusted with a high-ranking, prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level. In particular, politically exposed persons are:

- Heads of state, heads of government, ministers, members of the European Commission, deputy ministers, and assistant ministers;
- Members of parliament and members of similar legislative organs;
- Members of the governing bodies of political parties;
- Members of supreme courts, constitutional courts, or of other high-level judicial bodies, the decisions of which are usually not subject to further appeal;
- Members of the boards of courts of audit;
- Members of the boards of central banks;
- Ambassadors, chargés d'affaires, and defence attaches;
- Members of the administrative, management, or supervisory bodies of state-

owned enterprises;

- Directors, deputy directors, members of the board, or other managers with a comparable function in an international or European intergovernmental organization.

A family member of PEP means a close relative, in particular:

- The spouse or civil partner;
- A child and the child's spouse or civil partner;
- Both parents.

Any new or existing partner identified as a PEP or as a relative of such a person will have their account either rejected or closed.

Politically exposed persons shall be deemed both domestic and international, and shall be also considered as politically exposed for a period of 12 months after termination from political role.

Dealing with False positives and false negatives:

- Using multiple screening providers or cross-check tools.
- Checking periodic back testing of partner database vs. updated watchlists.
- Ensuring continuous updates to sanctions/PEP/media lists.
- For PEP status screening the Company can rely on an internet search or consult reports and databases on corruption risk (Transparency International Corruption Perceptions Index, or www.knowyourcountry.com, etc.).

Sanctions list

Governments and international organizations release sanctions lists to target individuals, organizations, or governments engaged in unlawful activities. These lists include sanctioned persons, entities, or governments deemed to pose a high risk.

Individuals or entities appearing on these sanction lists are subject to financial restrictions aimed at combating counterterrorism and money laundering efforts globally.

The Company is fully committed to complying with all applicable targeted financial sanctions regimes, including those established by the United Nations Security Council, the European Union, and the Kingdom of the Netherlands as implemented in Curaçao under the Sanctions National Ordinance and related legislation.

If an existing or prospective business partner is identified as a true match to a designated entity or individual listed in relevant sanctions databases, the Company shall take the following steps:

- Immediately suspend any ongoing business activity with the partner;
- Freeze any assets or funds under the Company's control that are owned or controlled—directly or indirectly—by the sanctioned party;
- File a report without delay with the Financial Intelligence Unit (FIU) Curaçao, including all relevant information regarding the match and the actions taken;
- Inform the Central Bank of Curaçao and Sint Maarten (CBCS) or relevant sanctions enforcement authority, if applicable;
- Retain all related records and correspondence for a period of at least five (5) years.

Business relationships will be terminated only upon confirmation from the FIU or designated supervisory authority that the match is verified and sanctionable. Frozen assets will not be released or transferred without prior written instructions from the competent authority.

In cases where the match is inconclusive, the Company will seek guidance from the FIU and take no further action until instructed. All screening and escalation procedures are documented and overseen by the Compliance Officer.

Adverse media

Adverse media refers to any negative or unfavourable information about a partner or business found across various sources, including news outlets, government records, regulatory databases, court filings, and credible online publications. This information could indicate potential involvement in criminal activity, regulatory breaches, association with sanctioned individuals or entities, fraud, money laundering, or reputational risk.

Any new or existing partner mentioned in adverse media will be subject to EDD. Depending on the results of the EDD, the Company may either close the account or reject the registration.

Negative media refers to adverse or unfavourable information published in traditional news outlets, online platforms, or social media that can damage a person's, company's, or organization's reputation. It includes any content that portrays the subject in a controversial, unethical, illegal, or disreputable light.

5.9.1. Document acceptance

For the purpose of verifying the identity and legal existence of B2B partners, the Company requires official and reliable documentation confirming the entity's incorporation, ownership, and operational address. The following documents are accepted:

Corporate Identity Verification:

- Certificate of Incorporation or Registration (issued by the relevant corporate

registry);

- Memorandum and Articles of Association (or equivalent constitutional documents).
- Excerpt from the official business register or Certificate of Good Standing (issued within the last six (6) months);
- Register of Directors and Shareholders (or equivalent documents identifying controlling persons);
- Document confirming the appointment and authority of the individual representing the entity (e.g., Board Resolution or Power of Attorney).

Document Requirements:

- All documents must be valid, clear, and legible;
- Documents must be provided in original format or as certified true copies;
- Documents not in English must be accompanied by a certified translation;
- Mobile phone bills or personal residential documents will not be accepted as a corporate PoA.

6. Compliance and Consequences of Non-Compliance

The Company maintains a zero-tolerance approach to breaches of its AML/CFT obligations and expects full compliance from all internal departments, employees, and external B2B partners. Compliance with this Policy is mandatory and forms an integral part of the Company's regulatory framework.

Internal Responsibility:

- All Company personnel, including management and staff involved in compliance, operations, risk management, and partner relations, are required to adhere strictly to this AML/CFT Policy and related procedures;
- The CO is responsible for overseeing the implementation of AML/CFT controls and procedures across the organization. The CO ensures regulatory alignment, manages internal reporting structures, and advises senior management on risk exposure related to ML, TF, and FP.

Role of the Compliance Officer:

- The CO is responsible for:
 - Designing, maintaining, and enforcing the Company's AML/CFT framework;
 - Ensuring that risk-based due diligence is conducted on all B2B partners prior to and throughout the duration of the business relationship;

- Monitoring all B2B partner activity, including transaction patterns, source of funds, and changes in ownership or control;
- Ensuring ongoing training and awareness within the Company regarding B2B AML/CFT risks and responsibilities;
- Conducting internal audits, sample testing, and remediation of deficiencies in AML controls.

Monitoring and Controls:

- The Company performs ongoing monitoring of its B2B partners, their transactions, business activities, and associated risk profiles.
- All transactions and interactions are reviewed in accordance with the RBA and in compliance with applicable Curaçao regulations, including but not limited to the NOIS, NORUT, NOPML, and the Sanctions National Ordinance.
- The Company does not engage in relationships with individuals. All onboarding and compliance processes are designed strictly for corporate entities.

Consequences of Non-Compliance:

Failure to comply with the Company's AML/CFT Policy—whether by internal staff or B2B partners—may result in serious consequences, both contractual and regulatory.

- **Internal Staff:**

- Employees found in breach of this Policy or found to have failed in their compliance duties may be subject to disciplinary action, up to and including termination of employment.

- **B2B Partners and Third Parties:**

- The Company reserves the right to suspend or terminate business relationships with any B2B partner that fails to meet AML/CFT obligations, refuses to provide required documentation, or is found to be in breach of contractual compliance terms;
- Non-compliant partners may be reported to relevant authorities if their conduct raises suspicion of ML/TF/FP.

- **Legal and Regulatory Risks:**

- Violations may expose the Company to administrative penalties, criminal liability, and regulatory enforcement under NOIS, NORUT, NOPML, or the Sanctions National Ordinance;
- Regulatory breaches may result in loss of license or restrictions imposed by the Curaçao Gaming Authority (CGA).

- **Business and Reputational Risks:**

- Non-compliance may lead to severe reputational harm, loss of business opportunities, and exclusion from financial institutions and strategic markets.

6.1. Termination of Business Relations

There are several reasons why the Company may terminate the business relations, but not limited to:

- Fraudulent activity, including submission of falsified corporate documents, misrepresentation of the company's legal status, ownership, or licensing credentials;
- Manipulation or tampering with reporting obligations, technical integrations, transaction flows, or platform behaviour that undermines system integrity;
- Unauthorized delegation or subcontracting of contractual responsibilities to third-party entities or individuals without the Company's prior written consent;
- Obstruction of compliance procedures, including refusal to cooperate with audits, delaying information requests, or interfering with AML/CFT monitoring efforts;
- Operational or commercial risk exposure, such as reputational damage, ongoing regulatory scrutiny, or involvement in high-risk sectors misaligned with the Company's risk appetite;
- Failure to meet or maintain PDD standards, including non-submission of corporate KYC documentation, unverifiable UBO structure, or undisclosed changes in control or ownership;
- Material breach of contract, including violations of the Terms and Conditions, AML/CFT covenants, technical integration standards, or data protection and confidentiality clauses.

However, this Company Policy focuses specifically on situations where there is suspicion or knowledge that the partner may be involved in ML or FT.

By law, the Company must end the business relationship with the partners unless the Company has obtained appropriate consent for it to continue, and even then, it is precautionary to close the account.

Due to the laws on Tipping Off, the Company cannot inform the partner that we have concerns regarding ML/FT. Thus, termination must be done sensitively.

Where the Company is unable to complete or apply the required PDD measures in relation to a particular partner at the point the PDD threshold for transactions is reached, it is accordingly required to cease transactions and terminate the business relationship with the partner.

6.2. External report to FIU

Once the Compliance Officer receives an Internal UTR, they will determine whether a UTR should be submitted to the FIU.

In making this decision, the Compliance Officer should consider that AML legislation aims to combat serious crime, typically involving substantial amounts or situations that indicate an attempt to bypass safeguards designed to prevent misuse of the financial system for criminal purposes.

For instance, identity fraud and chargebacks could lead to money laundering, but a licensee is only obligated to report if these activities result in funds being deposited with or held by the licensee.

The Company will not report isolated instances involving small amounts but will assess whether there is a broader pattern or scheme that warrants attention.

When evaluating an internal report for potential money laundering, the Compliance Officer considers all relevant information, such as identifying standard links between repeated unusual behaviours, chargebacks, or identity fraud. This could involve familiar persons, related IP addresses, or other shared factors.

In deciding whether to submit a UTR, the Compliance Officer should answer the following questions:

- Who is involved?
- How are they involved?
- What is the criminal/terrorist property?
- What is the value of the criminal/terrorist property (estimated as necessary)?
- Where is the criminal/terrorist property?
- When did the circumstances arise?
- When are the circumstances planned to happen?
- How did the circumstances arise?
- Why are you suspicious or have knowledge?

6.3. Reporting Indicators

In accordance with Article 10 of the National Ordinance Reporting Unusual Transactions (NORUT) and the Ministerial Decree of 11 November 2015, the Company shall apply the following indicators to determine when a transaction is considered unusual and must be reported to the FIU Curaçao.

- Objective Indicators (must be reported within 48 hours):
 - Any transaction (including attempted transaction) of Cg. 5,000 or more, regardless of whether it is in cash, check, electronic, or other form;
 - Any transaction involving a party listed under a sanction's regime (e.g., UN, EU, OFAC);
 - Any transaction involving a party previously reported to law enforcement or judicial authorities for potential ML/TF.
- Subjective Indicator:
 - Any transaction that, based on the Company's knowledge, experience, or available facts, raises reasonable suspicion of ML, TF, or FP – even if it does not meet the objective threshold.

Note: The Cg. 5,000 threshold resets per calendar gaming day.

6.4. Reporting Procedure

The Company is required to submit a UTR to the FIU, either through the user interfaces on the FIU's website or by mail (if permitted), without undue delay if there are indications that:

- The Company knows, suspects, or has reasonable grounds to believe that money laundering and/or terrorist financing is occurring;
- An asset involved in a business relationship or transaction originates from a criminal offense that could constitute a predicate offense to money laundering;
- A business case, transaction, or asset is linked to terrorist financing.

When deciding whether to submit a UTR, the Company considers several factors, including but not limited to:

- The purpose and nature of the transaction.
- Unusual characteristics or behaviours of the partners.
- The partner's financial and business background.
- The origin of the assets involved or to be contributed.

6.4.1. Internal and External Reporting Timelines

All employees must submit an internal UTR to the Compliance Officer within 24 hours of becoming aware of the suspicious activity.

If the Compliance Officer determines that the report meets the reporting criteria, the external UTR must be submitted to the FIU within 48 hours from the time of the transaction or internal report, whichever comes first.

Reports shall be submitted using the FIU's secure portal at <https://portal.fiucuracao.cw>.

6.5. Tipping-off

It is a criminal offense to inform anyone that a UTR has been submitted or is being considered if doing so could prejudice the investigation. While internal discussions about the partners are permitted, neither the partners nor their associates should be made aware that the partner may be under investigation.

This means that no employee of the Company:

- Can inform a partner that a transaction is being delayed because a report is pending approval (consent) from the FIU.
- Can disclose to the partner that law enforcement is conducting an investigation.

6.5.1. Internal Whistle-blower Protection

In accordance with Article 20 of NORUT, the Company guarantees that any employee who submits an internal report of unusual activity:

- Shall remain anonymous within the scope of the investigation;
- Shall not suffer retaliation, discrimination, demotion, or dismissal;
- Shall be supported with internal and legal protections if threatened by third parties.

Retaliatory action against whistle-blowers is considered a serious compliance violation and subject to disciplinary measures.

7. Internal Control

7.1. Introduction

The Company has a number of internal controls and general procedures that will be used on a day-to-day basis to manage and run the business's daily operations and prevent money laundering and terrorist financing.

7.2. Recordkeeping

The Company retains all documents and data collected or obtained during the due diligence process, including:

- All data and information used to identify and verify partners (such as document type, number, issuing authority, etc.);
- All documents and records used in preparing the risk analysis, the risk analysis itself, including results of the risk assessment, and documentation on the appropriateness of the measures taken based on these results;
- Results of internal investigations and communications with the FIU and regulators;
- Documents collected as part of due diligence on business partners;
- Documents collected from employees as part of due diligence;
- Documents related to AML training, such as training materials and examination results.

Additionally, the Company retains all documents created and processed in connection with suspected money laundering or terrorist financing, including:

- All related internal and external correspondence;
- File and interview notes;
- Results of internal investigations and the actions taken, explaining the reasoning behind the money laundering officer's decisions and subsequent actions.

The retention period for these documents is five years, starting from the end of the calendar year in which the business relationship ends or, in other cases, the year in which the relevant information was obtained for the completion of a one-off transaction. Applicable legislation may extend this retention period. Records must be kept in a secure and retrievable format and made available to the FIU and CGA upon request.

After the retention period expires, the Company will destroy all collected documents and data unless other recordkeeping or retention obligations apply, but no later than ten years.

7.3. Money Laundering Reporting Officer

The Company has appointed a Compliance Officer whose primary responsibility is to review internal reports of unusual transactions and, when necessary, submit a UTR to the FIU. The Compliance Officer also serves as the main point of contact for the FIU and obtains access to the goAML reporting portal after validation by the FIU.

To ensure the Compliance Officer can effectively fulfil their role, the Company guarantees that:

- The Compliance Officer acts independently, is knowledgeable about the Company's activities, and can independently decide whether to escalate internal reports to the FIU;

- The Compliance Officer has no conflicting responsibilities that could pose a conflict of interest;
- The Compliance Officer is provided with sufficient time, resources, and information to fulfil their duties;
- The Compliance Officer has the authority to assign tasks to relevant employees and make decisions related to ML/TF prevention.
- The Compliance Officer and their deputy are responsible for the following functions, among others:
 - Drafting and continually developing the internal risk analysis, covering the full scope of risks related to money laundering and terrorist financing;
 - Developing and updating internal policies and procedures aimed at preventing money laundering and terrorist financing;
 - Establishing uniform reporting channels;
 - Participating in the creation and further development of internal organizational and operational procedures related to implementing anti-money laundering and counter-terrorist financing regulations;
 - Ensuring compliance with current AML regulations and other relevant legislation;
 - Continuously monitoring the Company's business activities to ensure compliance with money laundering regulations;
 - Ensuring that CDD/EDD is carried out;
 - Submitting UTRs when appropriate;
 - Contributing to the development of staff AML training content;
 - Maintaining records of inquiries from law enforcement agencies and internal/external disclosures;
 - Submit reports to management on the Compliance Officer's activities, the Company's risk situation, and the measures taken or planned to meet AML obligations.
- The Compliance Officer and their deputy are authorized, within the scope of their duties, to:
 - Perform their tasks independently and effectively;
 - Submit legally binding declarations on behalf of the Company and represent it externally in relevant matters;

- Provide Company-specific instructions on all matters relating to the prevention of money laundering and terrorist financing;
- Conduct random checks without restriction.

7.4. Regulatory Oversight

The Company acknowledges the oversight authority of the CGA. The CGA has the right to conduct:

- Periodic reviews or audits of the Company's AML/CFT/CFP framework.
- On-site or remote inspections, including access to policies, risk assessments, and due diligence files.
- Requests for internal reports, training logs, and compliance data.

The Company will fully cooperate with CGA inquiries and provide access to systems and records upon request.

8. Contact Information

For questions, contact:

- Compliance Department:
- Email: Bohdan Snapkovskyi cco@vivatgaming.com

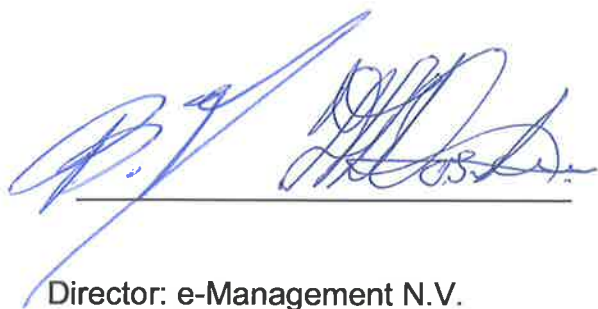
9. Policy History

Version	Date	Approved By
1.0	1 June 2025	Director and Compliance Officer

10. Policy URL

Available at:

Signed This 30th day of July 2025

A handwritten signature in blue ink, consisting of stylized initials and a surname, is written over a horizontal line. The signature is positioned above the text 'Director: e-Management N.V.'.

Director: e-Management N.V.