

ANTI MONEY LAUNDERING POLICY AND KNOW-YOUR-CLIENT POLICY

JER-TEAM N.V.

22.04.2026
Nr.001/2026

1. INTRODUCTION

In response to increasing global concerns regarding money laundering and the financing of terrorism, jurisdictions worldwide have established comprehensive legal and regulatory frameworks to prevent the misuse of financial systems. International standard-setting bodies have issued recommendations outlining the obligations of companies to identify, mitigate, and report risks associated with money laundering (ML), terrorist financing (TF), and other financial crimes.

JER-TEAM N.V. (hereinafter referred to as the “Company”) adopts a zero-tolerance approach to ML, TF, and any related criminal activity. The Company is committed to ensuring that its products and services are not misused for illicit purposes and operates in full compliance with all applicable legal and regulatory requirements.

The Company operates under a license issued by Antellephone N.V. and is subject to the applicable legal framework of Curaçao, including the National Ordinance on Identification when Rendering Services (NOIS) and the National Ordinance on the Reporting of Unusual Transactions (NORUT), as amended.

In addition, the Company aligns its Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) framework with the supervisory expectations and regulatory guidance issued by the Curaçao Gaming Control Board, which establishes enhanced compliance standards for licensed gambling operators.

The Company further adheres to internationally recognized standards, including those issued by the Financial Action Task Force (FATF), as well as relevant European Union legislation, including Directive (EU) 2015/849 and its subsequent amendments.

This Policy establishes the principles, procedures, and controls implemented by the Company to identify, assess, and mitigate ML/TF risks. The Policy applies to all employees, management, and relevant stakeholders of the Company and is subject to periodic review to ensure ongoing effectiveness and alignment with evolving regulatory requirements.

The Company applies a risk-based approach in the implementation of its AML/CFT framework, enabling the identification and mitigation of risks proportionate to their nature and scale. All employees and members of the Board of Directors are required to adhere to this Policy and contribute to maintaining the integrity and reputation of the Company.

2. OBJECTIVES

The purpose of this Policy is to establish a comprehensive framework for the prevention, detection, and reporting of ML, TF, and other financial crime risks within the Company and its affiliated entities.

The Company is committed to maintaining high standards of AML/CFT compliance and ensures that its management and employees adhere to these standards in order to prevent the misuse of its products and services for illicit purposes.

This Policy defines the principles, procedures, controls, and internal responsibilities required to effectively identify, assess, and mitigate ML/TF risks. It provides a structured approach to customer due diligence, transaction monitoring, reporting obligations, staff training, and internal control mechanisms, all of which are implemented across the Company on a risk-based basis.

The objective of this Policy is to ensure consistent application of AML/CFT measures across all business units, promote a strong compliance culture, and support the Company's ongoing adherence to applicable legal, regulatory, and supervisory requirements.

3. REGULATORY FRAMEWORK

3.1 National regulations

The Company operates in accordance with the applicable AML/CFT legal and regulatory framework of Curaçao. Money laundering and terrorist financing are criminal offences under the applicable laws of Curaçao, including the relevant provisions of the Criminal Code.

The primary legislative instruments governing AML/CFT obligations in Curaçao include, inter alia:

- a) the National Ordinance on the Reporting of Unusual Transactions;
- b) the National Ordinance on the Identification of Clients when Rendering Services;
- c) the Criminal Code of Curaçao;
- d) applicable sanctions legislation and related national decrees;
- e) the National Ordinance on the Obligation to Report Cross-Border Transportation of Money.

These laws and related regulations establish the legal basis for customer due diligence, reporting obligations, sanctions compliance, and other AML/CFT controls applicable to the Company.

The Company shall ensure ongoing compliance with all applicable laws, regulations, and guidance issued by competent authorities in Curaçao, including the relevant supervisory requirements.

3.2 International regulations

The Company's AML/CFT framework is aligned with internationally recognized standards, in particular those issued by the Financial Action Task Force.

Curaçao participates in the global AML/CFT framework through its membership in the Caribbean Financial Action Task Force ("CFATF"), a regional body associated with the FATF, and implements FATF Recommendations through its national legal and regulatory framework.

The FATF Recommendations establish the international standard for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction, including requirements relating to risk-based approaches, customer due diligence, reporting obligations, and sanctions compliance. The Company shall ensure that its AML/CFT policies, procedures, and controls are consistent with both applicable Curaçao legislation and relevant international standards, including the FATF Recommendations.

Where applicable international standards impose higher requirements than local regulations, the Company shall apply the more stringent measures to the extent practicable.

4. DEFINITIONS

Definitions of Money Laundering and Terrorist Financing

For the purposes of this Policy, money laundering shall include the following acts:

- the conversion or transfer of property, knowing that such property is derived from criminal activity or from participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or assisting any person involved in such activity to evade the legal consequences of their actions;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or participation in such activity;
- the acquisition, possession, or use of property, knowing at the time of receipt that such property was derived from criminal activity or participation in such activity;
- participation in, association to commit, attempts to commit, and aiding, abetting, facilitating, or counselling the commission of any of the actions referred to above.

Terrorist financing shall mean the provision or collection of funds or other assets, by any means, directly or indirectly, with the intention or knowledge that such funds or assets will be used, in

whole or in part, by a terrorist organization or by an individual terrorist, regardless of whether there is a link to a specific terrorist act.

5. GOVERNANCE

The Board of Directors has appointed the **Money Laundering Reporting Officer (MLRO)**. To fulfill his tasks, the MLRO has the right to access all necessary data, documentation and information.

The MLRO shall report directly to senior management and shall have access to the Board of Directors to ensure effective oversight of AML/CFT matters. The MLRO shall provide regular reports, including key risk indicators and regulatory updates, to senior management and, where appropriate, to the Board.

The AML/CFT program is directed by the MLRO and it is designed to address also related risks in financial crimes and to provide unobscured guidelines for all employees when it comes to preventing financial crimes such as ML and FT.

Within the Company, responsibilities are assigned to designated teams and employees, which support the MLRO in his duties, in order to secure the implementation and the following of Company's policies and procedures. It is the MLRO's responsibility to ensure that operational procedures are updated on a regular basis, at least once a year, and will be approved by it in cooperation with the responsible team leaders/managers.

To monitor the accordance with legal requirements, the Company established **Compliance department** developing AML/CTF and KYC procedures, obligatory for all employees of the Company and determining the policy of engagement with clients registered on the Company's website <https://royspins.com/>, <https://wazbee.casino/> and <https://welle.casino/> and opened an account.

5.1. AML Governance and Oversight

The Board of Directors retains ultimate responsibility for the Company's AML/CFT governance framework. The Board shall approve this Policy, the Company's AML/CFT risk appetite, the Business Risk Assessment, and any material changes to AML/CFT controls, systems, outsourcing arrangements, or governance structure. The Board shall receive AML/CFT reporting at least quarterly and shall oversee material AML/CFT risks, unusual transaction reporting trends, sanctions/PEP exposures, regulatory interactions, audit results, and remediation of deficiencies.

Senior Management is responsible for implementing the Board-approved AML/CFT framework, allocating adequate and proportionate resources, maintaining effective systems and controls, ensuring employee training, and addressing identified deficiencies without undue delay. Senior Management shall review AML/CFT management information at least monthly and shall escalate material AML/CFT matters to the Board promptly. Senior Management approval shall be required where mandated by law or this Policy, including for PEP relationships and other designated high-risk cases.

The Company shall designate a fit-and-proper MLRO who, for Curaçao AML/CFT purposes, shall act as the AML/CFT Compliance Officer unless another person is formally designated for that statutory role. The MLRO shall be a senior officer at management level, independent from gaming and revenue-generating operations, and shall not be combined with CEO, CFO, COO, internal audit, or other operational functions that create a conflict of interest. The MLRO shall have timely and unrestricted access to customer identification data, CDD/EDD records, transaction records, screening results, and any other information necessary to perform his or her duties, and shall be able to escalate matters directly to Senior Management and, where necessary, to the Board or its Chair. The MLRO shall oversee AML/CFT policy implementation, unusual transaction investigations and reporting, sanctions and PEP oversight, employee training, and periodic AML/CFT reporting to management and the Board.

The Company applies a Three Lines of Defense model. The first line owns operational AML/CFT controls in onboarding, payments, customer support, game operations, fraud operations, and transaction monitoring. The second line, led by the MLRO/Compliance function, establishes policy, oversees adherence, reviews screening and reporting, and challenges the first line. The third line shall perform independent AML/CFT testing. An independent AML/CFT audit shall be conducted at least annually, and also when there is a material regulatory, business, product, payment, geographic, or systems change. Audit findings shall be documented, risk-rated, assigned to accountable owners, and reported to Senior Management and the Board together with target remediation deadlines.

Any suspected unusual transaction, sanctions-related freeze or match, FIU information request, or material AML/CFT control failure shall be escalated to the MLRO immediately. Any reportable incident shall be escalated internally without delay so that external reporting deadlines can be met, including the requirement to report unusual transactions to the FIU without delay and reportable incidents to the regulator within 24 hours where applicable. AML/CFT governance records, including Board papers, approvals, decisions, investigations, internal reports, audit reports, and remediation records, shall be retained for at least five years, or longer where required by law or instruction of the FIU.

The MLRO shall have sufficient authority, independence, and access to all relevant information and systems to perform their duties effectively and without undue influence.

5.2. AML/CFT Risk Appetite Statement

The Company adopts a conservative risk appetite in relation to money laundering, terrorist financing, sanctions evasion, and other financial crime risks. The Company shall not enter into or maintain business relationships where the ML/TF risk cannot be effectively identified, mitigated, and controlled in accordance with applicable laws and this Policy.

1. Prohibited Relationships and Activities

The Company shall not establish or continue a business relationship in the following circumstances:

- Where the identity of the customer, beneficial owner, or controlling person cannot be verified in accordance with Customer Due Diligence requirements;
- Where the customer, beneficial owner, or any associated party is subject to applicable sanctions or restrictive measures;
- Where the customer is resident in, incorporated in, or otherwise connected to jurisdictions subject to comprehensive international sanctions, unless permitted by law and approved by the MLRO and Senior Management;
- Where the source of funds or source of wealth cannot be reasonably established or is inconsistent with the customer's known profile;
- Where there is suspicion or knowledge of involvement in money laundering, terrorist financing, fraud, or other criminal activity;
- Where the customer uses anonymity-enhancing mechanisms (including proxies, VPNs, mixers, or third-party payment arrangements) in a manner that prevents effective risk mitigation;
- Where the customer refuses or fails to provide required information or documentation within the prescribed timeframe.

2. High-Risk Customer Acceptance

The Company may accept high-risk customers only where:

- Enhanced Due Diligence measures have been fully completed;
- The source of wealth and source of funds have been satisfactorily established and verified;
- Senior Management approval has been obtained prior to establishing or continuing the relationship;
- Enhanced ongoing monitoring controls are in place.

Foreign Politically Exposed Persons (PEPs) shall always be classified as high risk and subject to these requirements.

3. Jurisdictional Risk

The Company applies strict controls in relation to geographic risk:

- Customers from jurisdictions identified as high-risk by the Financial Action Task Force shall be subject to Enhanced Due Diligence and may only be accepted with Senior Management approval;
- Customers from sanctioned or embargoed jurisdictions shall not be accepted unless explicitly permitted by applicable law;
- The Company shall implement controls to detect and prevent circumvention of geographic restrictions, including the use of VPNs or proxy services.

4. Transactional Risk Limits and Controls

The Company establishes thresholds and controls to manage transactional risk, including:

- Mandatory Enhanced Due Diligence for customers engaging in high-value or unusual transactions inconsistent with their profile;
- Escalation and review of transactions exceeding predefined internal thresholds or exhibiting unusual patterns;
- Prohibition of transactions where the origin or destination of funds cannot be verified or linked to the customer.

Specific thresholds and monitoring scenarios shall be defined in internal procedures and reviewed periodically.

5. Risk Acceptance Limits

The Company shall maintain a balanced risk profile and shall:

- Limit exposure to high-risk customers to a level that can be effectively managed through available controls and resources;
- Regularly review the composition of its customer base to ensure alignment with its risk appetite;
- Terminate relationships where risk exceeds the Company's tolerance or where mitigation measures are no longer effective.

6. Ongoing Review

This Risk Appetite Statement shall be reviewed at least annually, and whenever there are significant changes in the Company's business model, regulatory environment, or risk profile. Any material changes shall be approved by the Board of Directors.

5.3. AML/CFT Key Risk Indicators

The Company shall establish and maintain a set of measurable AML/CFT Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) to assess the effectiveness of its AML/CFT framework.

Such indicators shall be reviewed by Senior Management on at least a monthly basis and reported to the Board on a quarterly basis.

The indicators shall include, at a minimum:

- Number of alerts generated, reviewed, and escalated;
- Volume of Internal SARs and external reports submitted to FIU Curaçao;
- Average time taken to review alerts and escalate suspicious activity;
- Number and proportion of high-risk customers;
- Number of overdue CDD/EDD cases;
- Sanctions screening matches and resolution time;
- False positive rates in transaction monitoring and screening systems.

Where thresholds are exceeded or deficiencies are identified, corrective actions shall be implemented without delay and tracked until resolution.

6. RISK ASSESSMENT

The Company is required to assess on a yearly basis the risks of money laundering and terrorism financing, taking into account risk factors relating to Clients, countries or geographic areas, products, services, transactions. The Company will collect certain minimum Clients identification information from each Client who opens an account; utilize risk-based measures to verify the identity of each Client who opens an account; record Client identification information and the verification methods and results; and compare Client identification information with government-provided lists of suspected terrorists, once such lists have been issued by the government.

By following the risk-based approach, all possible risk areas and risks can be identified, and mitigating measures are applied according to the grade of risks that have been assessed. These measures will then be implemented to reflect the day-to-day responsibilities under applicable AML regulations.

A business risk assessment and customer risk assessment are performed. The Company implements an ongoing corporate AML/CFT risk assessment to analyse the level of risk that its

customers, services, channels, products or geographic locations of its legal entities are posing. The results of the risk assessment lead to appropriate risk mitigating actions.

The Company has set out its comprehensive set of risk mitigating measures in its IT-based AML/CFT Framework of risk assessment, policies, procedures, trainings and controls.

Constant safeguarding of AML/CFT compliance is achieved by designing and installing also controls to manage and reduce the impact of identified risks and to assess the effectiveness and functionality of taken measures.

On an ongoing basis, the MLRO is monitoring the AML/CFT controls to improve their efficiency, proper records of taken actions and the reasoning behind such actions are kept and documented.

Risk Classification

The Company maintains a risk-based approach in relation to its clients in order to effectively detect and deter any risks it may be exposed to such as money laundering, the financing of terrorism or any prohibited transaction such as fraud.

The Company maintains the following risk classification:

- Low risk
- Medium risk
- High risk

Low risk

Customers assessed as Low Risk present a lower likelihood of involvement in money laundering or terrorist financing activities. Such customers typically demonstrate straightforward ownership structures, low-risk geographic exposure, and expected transactional behavior.

Standard Customer Due Diligence (CDD) measures shall be applied, and ongoing monitoring shall be conducted on a routine basis.

Medium risk

Customers assessed as Medium Risk present an increased level of risk due to certain risk factors, such as geographic exposure, transaction patterns, or business characteristics.

In addition to standard CDD, enhanced monitoring measures shall be applied, and additional information may be obtained to better understand the customer's profile and activities.

Customer relationships classified as Medium Risk shall be subject to periodic review at least annually.

High Risk

Customers assessed as High Risk present a significant risk of money laundering or terrorist financing. This category includes, but is not limited to, Politically Exposed Persons, customers connected to high-risk jurisdictions, complex ownership structures, or those exhibiting unusual or high-risk transactional behavior.

Enhanced Due Diligence (EDD) measures shall be applied in accordance with Section 7.2 of this Policy. This shall include, at a minimum:

- obtaining senior management approval prior to establishing or continuing the relationship;
- establishing and verifying the source of wealth and, where applicable, source of funds;
- applying enhanced and ongoing monitoring of the business relationship.

High-risk customers shall be subject to more frequent review, at least annually and more frequently where warranted by risk.

Some customers present higher inherent risk to our organization because of who they are, what they do, the industry they are in, the business they run, or their source of funds or wealth. When assessing the risk posed by a customer, we are checking their status and what they do.

Any customer who will not cooperate, or who refuses to provide satisfactory proof of how the source of funds or source of wealth was obtained, raises a further red flag and become a high risk.

Not all red flags are permanent. We might discover, that our customer has the same name as someone who is listed on an official register for crimes or sanctions. After further investigation, we confirm that our customer is not on that register, we can clear the red flag and high risk status.

Some jurisdictions are higher risk because their own laws, regulations, and enforcement controls to prevent financial crime are weak, or nonexistent. Higher risk jurisdictions, as defined by the FATF, are countries that have been identified as having strategic deficiencies in their national anti-money laundering and counter-financing of terrorism regimes.

6.1. Business Risk Assessment

6.1.1. Executive Summary

This Business Risk Assessment (BRA) primarily addresses money laundering and terrorist financing risks. Broader operational, fraud, cybersecurity, and business risks are managed under separate internal risk management frameworks.

The BRA aims not only to comply with statutory expectations but to exceed them by establishing a best-in-class internal governance and risk management posture. It provides a systemic view into the most probable and impactful threats facing the business, ranging from external cyberattacks and affiliate fraud to high-risk customer behavior, data protection vulnerabilities, and geopolitical exposure. Over 35 high-risk vectors are mapped across operational, financial, IT, human resources, and customer interaction domains. These threats are evaluated using a dual-impact model of Likelihood and Severity, delivering a risk score that drives mitigation prioritization and resource allocation.

Key focus areas include:

- Real-time fraud detection failures and system downtime due to DDoS
- Use of synthetic identities and deepfake documents for KYC evasion
- Exploitation of marketing bonus systems via affiliate laundering schemes
- Improper onboarding of third-party game and payment providers
- Crypto-based anonymized transactions using mixers and tumblers
- Insider collusion risks in handling customer balances and payouts

Jer-Team N.V. has developed this BRA as a living document: subject to continuous review and amendment in accordance with emerging risk trends, enforcement precedents, and evolving global standards such as those established by FATF and EU AML directives. The Company recognizes that regulators will demand not just compliance “on paper,” but dynamic operational integrity validated through documentation, audit trails, independent testing, and data-driven oversight.

In preparation for both internal resilience and external scrutiny, Jer-Team N.V. applies this BRA not as a static document but as an operational backbone for decision-making and compliance enforcement. The business environment in which the Company operates is volatile and hyper-regulated, with increasing pressure from international watchdogs on offshore gambling jurisdictions. Consequently, risk tolerance levels are set conservatively low, particularly in areas touching customer onboarding, payment flow integrity, and third-party exposure.

A core component of this BRA is its proactive alignment with international regulatory developments, including:

- The full rollout of the Curaçao GCB license and supervisory regime
- Enforcement actions and case studies published by the Financial Action Task Force
- EU-level mandates under AMLD 5 and 6
- Global regulatory signals on virtual asset service providers (VASPs)

To that end, risk governance has been embedded in the Company's structure through the following pillars:

- **Designated MLRO and AML Task Force** reporting to executive management
- **Cross-functional risk committee** meeting monthly to review incidents, STRs, alerts, and process gaps
- **Escalation mechanisms** for emerging threats and regulatory breaches
- **Technical enforcement** of controls through proprietary and third-party RegTech tools

Ultimately, this document formalizes Jer-Team N.V.'s zero-tolerance stance on regulatory breaches, data loss, and financial misconduct. The Company recognizes that failure to identify, assess, and manage these risks does not only endanger its license and client base, but also the broader integrity of the Curaçao gaming sector under global scrutiny.

6.1.2. Risk Scoring Matrix

An essential element of Jer-Team N.V.'s BRA methodology is the standardized scoring of risk events using a dual-dimensional matrix: Likelihood (L) × Impact (I). This approach allows the Company to assign consistent, objective values to various risk types, which are then used to prioritize mitigation strategies, allocate resources, and document audit trails for regulatory review.

Likelihood

Represents the estimated probability that a specific risk event will occur, ranked on a five-point scale:

1. Rare
2. Unlikely
3. Possible
4. Likely
5. Almost Certain

Impact

Describes the severity of consequences if a risk materializes. This too is scored from 1 to 5:

1. Negligence (low financial and operational impact)

2. Minor (localized, reversible impact)
3. Moderate (noticeable operational disruption or financial loss)
4. Severe (major legal, reputational, or customer impact)
5. Catastrophic (business-threatening or regulatory-fatal outcome)

The resulting **Inherent Risk Score (IRS)** is calculated as: **IRS = Likelihood × Impact**

This generates a risk level ranging from 1 to 25. The matrix below demonstrates how these values map onto a heat-based risk prioritization chart:

Likelihood\ Impact	1 (Negligible)	2 (Low)	3 (Moderate)	4 (Severe)	5 (Catastrophic)
1 (Rare)	1	2	3	4	5
2 (Unlikely)	2	4	6	8	10
3 (Possible)	3	6	9	12	15
4 (Likely)	4	8	12	16	20
5 (Almost Certain)	5	10	15	20	25

Risk Rating Scale:

- 1–3: Low – Acceptable risk, routine monitoring
- 4–6: Medium – Requires controls, periodic review
- 7–14: High – Immediate attention and formal mitigation
- 15–25: Critical – Executive oversight, robust controls, and regulatory exposure

Residual Risk Score (RRS)

Once mitigation controls are applied, the residual risk score reflects the remaining exposure.

Controls are evaluated on their Effectiveness (scale 1–4):

1. Non-existent
2. Ineffective
3. Partially effective
4. Fully effective

The RRS is not simply mathematical but incorporates control environment maturity, enforcement records, and audit history.

This risk scoring model is embedded in the Company's governance infrastructure and used across departments—including AML, Compliance, Risk, Operations, and IT Security—to ensure consistent understanding of risk levels and decision thresholds.

6.1.3. Risk Identification and Classification

Risk identification is a foundational element in Jer-Team N.V.'s overall governance and compliance strategy. It is the first step in a multi-layered risk management framework and aims to create an exhaustive map of potential vulnerabilities—both existing and emerging—across all operational domains. The Company employs a hybrid methodology that combines quantitative risk analytics (e.g., transaction monitoring, heat mapping) with qualitative input (e.g., audit reports, staff interviews, incident logs, whistleblower alerts).

Risks are categorized across **seven core domains**, each mapped to specific internal processes and external exposures:

1. **Customer Behavioral Risk:** Unusual play patterns, disproportionate win/loss ratios, bonus abuse, self-exclusion evasion, and high-risk demographic behaviors.
2. **Transactional Risk:** Use of high-risk payment methods (crypto, prepaid cards), third-party transfers, unexplained velocity of deposits/withdrawals, and failure to comply with the closed-loop principle.
3. **Geopolitical/Jurisdictional Risk:** Customers accessing the platform from high-risk or sanctioned jurisdictions using VPN/proxy; regulatory arbitrage between licensing regimes.
4. **Product Integrity & Game Abuse:** Patterned betting suggesting collusion; abuse of RNG outcomes; hedge betting across fixed odds products; risk of non-certified game providers.
5. **Insider & Staff Risk:** Insider fraud, privilege escalation, sabotage, or leakage of confidential data; absence of access control and session logging.
6. **Third-Party & Affiliate Exposure:** Commission laundering via fake traffic, shell affiliate networks, lack of KYC on partners, undisclosed UBOs (Ultimate Beneficial Owners).
7. **Infrastructure and Cybersecurity Threats:** Data breaches, system intrusion attempts, DDoS attacks, and malware/ransomware targeting critical systems.

Each risk category is assessed across two critical metrics:

- **Likelihood (L):** The probability of occurrence, ranging from rare to almost certain.
- **Impact (I):** The potential severity if the risk materializes, from negligible to catastrophic.

This dual-metric scoring produces an **Inherent Risk Score (IRS)** from 1 to 25, prior to any mitigation. Once mitigation controls are factored in, a **Residual Risk Score (RRS)** is assigned.

The BRA also considers risk velocity—how fast a risk can materialize and cause damage—and risk interconnectivity, where failures in one domain can amplify risks in another. For example, a breach in cybersecurity controls may simultaneously impact customer integrity, financial flows, and regulatory exposure.

In total, this assessment identifies **35+ high-sensitivity risk vectors**, many of which are further dissected through scenario analysis and cross-functional workshops to ensure operational relevance and real-time applicability.

6.1.4. Regulatory & Strategic Context

Jer-Team N.V. operates under the evolving regulatory landscape of Curaçao, with its core operations soon to fall fully under the oversight of the newly formed Curaçao Gaming Control Board. This regulatory shift mandates a complete restructuring of licensing standards, AML/CFT obligations, reporting duties, and corporate governance expectations.

The GCB regime is informed by international regulatory best practices and mirrors FATF recommendations, aiming to bring Curaçao into closer alignment with European and global frameworks. In this context, the Company's risk posture must reflect not only local obligations, but global enforcement realities.

Additionally, the Company's risk exposure is influenced by:

- EU 5th and 6th Anti-Money Laundering Directives (AMLD V & VI), especially concerning beneficial ownership transparency and enhanced due diligence for high-risk clients.
- The FATF Methodology for AML/CFT assessments, which drives national expectations for sector-specific risk awareness and documentation.
- Curaçao's commitment to comply with OECD and CFATF (Caribbean Financial Action Task Force) guidance.
- The global rise of cryptocurrency regulation and inclusion of gambling operators in the scope of VASPs (Virtual Asset Service Providers).

This BRA integrates these frameworks into its assessment model to ensure forward-looking compliance and strategic resilience.

6.1.5. Inherent Risk Categories

The assessment of inherent risk represents the baseline exposure faced by Jer-Team N.V. in the absence of mitigating controls. Inherent risk reflects the raw threat posed by a given scenario, process, or actor, considering environmental, technical, procedural, and behavioral factors. It serves as the critical foundation upon which mitigation strategies are prioritized and deployed.

This section outlines the core inherent risk categories, along with representative vectors identified through internal audits, industry benchmarks, regulatory guidance, and data analytics.

1. Interface & Registration Risk

- Use of fabricated IDs, forged documents, and identity fraud (e.g., AI-generated selfies)
- Bypass of KYC procedures via unverified registration funnels
- Use of VPNs and proxies to manipulate jurisdictional onboarding
- Score: 16 (Severe Risk)

2. Geographical Risk

- Player access from sanctioned or FATF-listed jurisdictions (e.g., Iran, North Korea)
- Use of masking tools to spoof location and evade country restrictions
- Absence of geo-IP alerts or enforcement blocks
- Score: 20 (Critical Risk)

3. Transactional Risk

- Cryptocurrency deposits via high-risk exchanges or anonymizing tools (e.g., mixers)
- Lack of closed-loop withdrawals (withdrawals going to different accounts than funding source)
- Excessive transaction frequency or inconsistent patterns
- Score: 20 (Critical Risk)

4. Customer Behavioral Risk

- Low or zero gameplay turnover after large deposits (classic ML typology)
- Disproportionate bonus exploitation or stake anomalies
- Accounts associated with PEPs or sanctioned individuals
- Score: 18 (High Risk)

5. Product Abuse Risk

- Fixed odds betting for hedging and arbitrage schemes
- Collusive behavior in poker, esports or in-play games
- Integration of non-certified or externally manipulated RNG games
- Score: 17 (High Risk)

6. Internal Staff Risk

- Inadequate access control to backend systems
- Undocumented privilege escalations
- Employee betting or interference with customer data
- Score: 16 (Severe Risk)

7. Affiliate & Partner Risk

- Onboarding of affiliates without full UBO verification
- Commission abuse through fake or recycled traffic
- Providers operating without proper licensing or DD
- Score: 19 (High-Critical Risk)

8. Cybersecurity Risk

- Lack of intrusion detection or breach containment protocols
- DDoS exposure without real-time mitigation
- Insider compromise of critical systems (e.g., database dumps)
- Score: 25 (Maximum/Catastrophic Risk)

9. Cross-Platform Account Duplication

- Users registering multiple accounts across different brand domains to exploit bonuses or evade previous restrictions
- Often coordinated via proxy servers and recycled credentials
- Score: 18 (High Risk)

10. Social Engineering of Support Staff

- Use of persuasive tactics or spoofed identities to bypass account security and extract sensitive customer or operational data
- Score: 17 (High Risk)

11. Bonus Abuse via Affiliate Networks

- Systematic exploitation of promotional campaigns through affiliate referrals using fake or duplicate accounts
- Score: 19 (High-Critical Risk)

12. Velocity Abuse of Progressive Jackpot Games

- High-frequency betting to statistically manipulate the payout cycle on progressive RNG games
- Score: 17 (High Risk)

13. Non-Compliant Marketing Practices

- Distribution of marketing materials to jurisdictions where online gambling is prohibited or restricted.
- Score: 16 (Severe Risk)

14. Identity Farm Exploitation

- Use of large-scale identity farms (real or synthetic) to mass-register accounts for fraudulent purposes.
- Score: 20 (Critical Risk)

15. Insider Collusion with Players

- Coordination between internal staff and selected customers to manipulate payouts or override limits.
- Score: 21 (Critical Risk)

16. Use of Dormant Accounts for Laundering

- Dormant accounts reactivated for single high-value transaction with no gaming activity.
- Score: 18 (High Risk)

17. Supplier Data Breach

- Leakage of player data from third-party providers leading to reputational and financial damage.
- Score: 22 (Critical Risk)

18. Lack of Multi-Jurisdictional Risk Classification

- Inadequate mapping of user jurisdictions in relation to evolving geopolitical or sanctions regimes.
- Score: 19 (High-Critical Risk)

6.1.6. Risk Mitigation & Control Measures

Risk mitigation refers to the development and implementation of policies, procedures, technologies, and cultural practices aimed at reducing identified risks to an acceptable level. For Jer-Team N.V., effective mitigation is essential not only to satisfy regulatory obligations under the Curaçao GCB, but also to preserve business continuity, protect user assets, and maintain reputational integrity.

The Company applies a defense-in-depth strategy, ensuring that risks are addressed across multiple control layers. These include preventive, detective, and responsive controls embedded into daily operations, technology platforms, and governance workflows.

Key Mitigation Measures by Risk Domain

1. AML/CFT Compliance

- Daily automated PEP/sanctions screening via updated lists (UN, EU, OFAC)
- EDD triggers for large deposits, geographic anomalies, and behavioral outliers
- KYT analytics deployed to monitor transaction velocity and unusual behavior

2. Customer & Identity Verification

- eKYC onboarding with biometric checks, document OCR validation, and duplicate detection
- Re-verification processes for returning or high-value users
- AI-driven identity similarity analysis to flag synthetic or farmed accounts

3. Transaction & Payment Controls

- Closed-loop withdrawal enforcement to original funding sources
- Flagging and manual approval of third-party name mismatches
- Use of payment velocity thresholds and single-session withdrawal caps

4. Affiliate & Partner Governance

- Full KYC onboarding for affiliates, including UBO validation and sanction screening
- Monthly affiliate traffic audits and incentive abuse detection
- Blacklisting and immediate deactivation of flagged affiliate IDs

5. Cybersecurity

- Endpoint detection and response (EDR) tools for internal networks
- DDoS mitigation via global CDN partners and firewall traffic shaping
- Role-based access controls (RBAC) and centralized logging for system actions

6. Internal Staff Risk

- Background screening and police conduct certificates (where permitted by law)
- Segregation of duties and audit trails for all financial operations
- Mandatory conflict of interest declarations and AML awareness training

7. Geolocation & Jurisdictional Risk

- Real-time IP geolocation blocking and proxy/VPN detection tools
- Dynamic risk mapping system that adjusts exposure scores by jurisdiction
- Sanction list ingestion and auto-flagging for conflicting country data

Future Measures (2025–2026 Roadmap)

- Launch of AI-based behavioral anomaly detection across all active user accounts
- Development of automated transaction flow mapping to support rapid AML investigations
- Dual approval for large payouts and high-risk jurisdiction withdrawals
- Expansion of RegTech stack to include blockchain analytics integrations

Together, these measures provide layered assurance and demonstrate a forward-leaning approach to risk governance. Controls are subject to quarterly testing and continuous improvement, in line with regulatory feedback, audit results, and emerging threat intelligence.

6.1.7. Ongoing Monitoring, Reporting & Governance

A robust risk management framework requires not only initial risk assessment and mitigation but also a sustained, structured approach to **monitoring, escalation, and governance**. Jer-Team N.V. maintains a formal risk oversight infrastructure, combining automated surveillance with human supervision, to ensure that emerging threats, system gaps, and non-compliance indicators are identified, reported, and acted upon in real time.

1. Real-Time Monitoring

- **AML Transaction Monitoring Engine** operates 24/7 and flags suspicious behavior based on velocity, volume, and pattern deviations.
- **Login & Access Logs** are tracked for anomalies such as off-hour access, credential mismatches, and device changes.
- **Geolocation Monitoring** ensures continuous enforcement of restricted jurisdictions and detects use of masking tools.
- **Fraud Alerts** are triaged through a centralized compliance dashboard, escalating high-severity alerts automatically.

2. Internal Governance Structure

- **MLRO (Money Laundering Reporting Officer)** oversees day-to-day AML/CFT activities, STR filings, and control testing.
- **Monthly Risk Committee** includes representatives from Compliance, Legal, Finance, and IT Security to review KPIs, breaches, and mitigation effectiveness.
- **Quarterly Risk Register Review** updates all residual risk entries and control adjustments.
- **Board-Level Oversight** includes quarterly compliance reporting and mandatory notification of regulatory or data breach events.

3. Reporting Protocols

- **Suspicious Transaction Reports (STRs)** are filed to the FIU Curaçao promptly upon internal escalation.
- **Monthly Internal Reports** summarize flagged events, control performance, and mitigation actions.
- **Annual Compliance Statement** prepared for GCB, confirming BRA review, system updates, and employee training.

- **Incident Reports** are logged and tracked until full remediation, with root cause analysis and regulatory disclosures when applicable.

4. External Assurance and Testing

- **Independent AML Audits** conducted semi-annually to assess effectiveness of controls and rule calibration.
- **Penetration Testing & Red Team Exercises** simulate real-world attacks to test IT and fraud resilience.
- **Third-Party Reviews** (KYC vendors, PSPs, affiliates) are required to submit compliance attestations and undergo due diligence refreshes.

5. Culture of Compliance

- **Mandatory AML/CFT training** is required for all employees annually, with targeted refreshers for at-risk roles.
- **Whistleblower Program** allows confidential internal escalation of unethical or suspicious behavior.
- **Continuous Feedback Loops** integrate lessons learned from incidents into control refinement.

Through this framework, Jer-Team N.V. ensures that risk management is not a one-time effort but an embedded part of the company's operational DNA, aligned with regulatory expectations and stakeholder accountability.

The results of the Business Risk Assessment are operationalized across the Company's AML/CFT framework. Specifically, the identified risks and risk scores directly inform:

- customer risk classification and onboarding requirements;
- transaction monitoring rules, alert thresholds, and escalation criteria;
- the scope and application of Enhanced Due Diligence measures;
- sanctions and geographic risk controls.

This ensures that the Company's AML/CFT controls remain proportionate, dynamic, and aligned with its evolving risk profile.

7. KNOW YOUR CLIENT

7.1. Client Identification and Verification

The Company has adopted a Customer Acceptance Policy in conformity with its obligations as a licensed gaming operator to meet all applicable legal requirements, including those relating to responsible gaming, player protection, and the prevention of financial crime. The said policy

is not only used for AML/CFT purposes, but also for player protection and is maintained in a separate document.

The Board of Directors and senior management of the Company have established a strong player protection and AML/CFT culture and are constantly communicating a clear message to all employees that the Company, as a responsible operator, protects minors and its customers. The Company has adopted a zero-tolerance approach to money laundering, terrorist financing, and any other illegal activities, and shall not knowingly conduct business with individuals or entities it believes to be engaged in such activities. No business relationship shall be established or maintained where the ML/TF risk cannot be effectively mitigated.

CDD shall be conducted prior to establishing a business relationship and, in all cases, prior to allowing any transactions or withdrawals. CDD shall also be performed when there is a suspicion of money laundering or terrorist financing, when there are doubts about the accuracy or adequacy of previously obtained customer identification data, or when there is a change in the customer's risk profile or activity. Where CDD cannot be completed, the Company shall not establish the relationship or shall terminate the existing relationship and consider whether reporting to the Financial Intelligence Unit is required.

Depending on the risk arising from a customer, different levels of due diligence shall be applied, distinguishing between standard CDD and EDD, in accordance with the risk classification set out in Section 6 of this Policy.

Any natural person or corporate entity as a business partner shall be adequately identified through full registration of personal or company data, risk-rated, and subject to ongoing monitoring in accordance with documented procedures.

Personal data such as the official full name, place and date of birth, permanent residential address, identification reference number, nationality, and contact details shall be obtained. This information shall be complemented, where required based on risk, with information and documentation relating to the source of funds and source of wealth, as well as any other relevant information necessary to understand the customer's profile and activities.

CDD measures include not only the identification of the customer or business partner, but also the verification of such identity using reliable and independent documentary or electronic sources. This includes, where applicable, the identification and verification of Ultimate Beneficial Owners (UBOs) and legal representatives. UBOs shall be understood as natural persons who ultimately own or control the customer, typically through direct or indirect ownership of 25% or more, or through other means of effective control. Where no such person can be identified, the senior managing official shall be identified and verified.

No business shall be conducted with any natural person or corporate entity that does not meet legal requirements or is prohibited from using the Company's services. Anonymous or fictitious accounts are strictly prohibited, and no more than one active account shall be maintained per customer.

Generally, no business relationship shall be established or maintained where the customer is suspected or known to be involved in money laundering, terrorist financing, fraud, or other criminal activity. In cases of doubt, the MLRO shall be involved to perform a risk assessment and determine appropriate mitigating measures.

The Company has established Know-Your-Client standards requiring due diligence on each prospective client prior to entering into a business relationship, including:

- identification and verification of the customer and, where applicable, any representatives, based on documents, data, or information obtained from reliable and independent sources;
- obtaining information on the purpose and intended nature of the business relationship.

Prior to opening an account, the Company collects preliminary identification information, including:

- the name;
- the client's country of residence or registration;
- the client's IP address and geolocation data.

The Company does not allow its clients to open anonymous accounts and does not permit any transactions or withdrawals until full identification has been completed.

Prior to allowing any transactions or withdrawals, the Company shall collect and verify complete identification information, including:

- the name (confirmation);
- date of birth;
- residential address;
- a valid identification number (e.g., passport or government-issued ID), including country of issuance;
- contact details, including phone number.

The Company has developed a list of documents required for the purpose of complete identification, including:

- a valid passport or government-issued identification document;
- proof of address (e.g., utility bill or equivalent);
- additional documents such as a driver's license, where required.

Verification may be conducted using both documentary and non-documentary methods. In addition to documents, the Company may apply electronic verification, database checks, biometric verification (such as liveness checks), and analysis of device, IP address, and geolocation data.

While the Company may rely on government-issued identification documents, it shall not do so uncritically. Where there are indications of fraud, inconsistency, or elevated risk, additional verification measures shall be applied to ensure the authenticity of the customer's identity.

Non-documentary verification methods may include:

- independent verification through public or private databases;
- cross-checking with financial institutions or other reliable sources;
- obtaining additional financial or supporting information;
- direct communication with the client.

Based on the risk, and to the extent reasonable and practicable, the Company shall ensure that it has a reasonable belief that it knows the true identity of the client. The information obtained shall be analyzed to ensure consistency and to detect any discrepancies.

Customer Due Diligence is an ongoing process. The Company shall monitor customer activity and ensure that customer information remains up to date. Re-verification shall be performed where necessary, including in cases of unusual activity, changes in customer behavior, or identification of new risk factors.

If a potential or existing client refuses to provide the required information, provides misleading information, or cannot be satisfactorily verified, the Company shall not establish the relationship or shall terminate the existing relationship. Such cases shall be escalated to the MLRO, who shall determine whether further action, including reporting obligations, is required.

7.2. Enhanced Due Diligence

Enhanced Due Diligence (EDD) shall be applied where a customer, beneficial owner, transaction, delivery channel, jurisdiction, payment method, technology, or third-party involvement presents a higher risk of money laundering, terrorist financing, sanctions evasion, or other financial crime. EDD supplements the standard customer due diligence measures in Section 7.1 and shall be applied together with the customer risk classification in Section 6.

EDD shall be mandatory, at minimum, where: the customer or beneficial owner is a Politically Exposed Person; the customer or beneficial owner is resident in, incorporated in, funded from, or otherwise materially connected to a high-risk or sanctioned jurisdiction; the ownership or control structure is unusual, opaque, nominee-based, or otherwise excessively complex; the

customer engages in high-value, complex, or unusual transactions or patterns of activity inconsistent with the expected profile; the customer uses anonymity-enhancing products, payment methods, wallets, accounts, or third-party funding arrangements; the customer relationship is conducted remotely or through non-face-to-face onboarding with elevated impersonation risk; or the relationship involves an affiliate, intermediary, agent, PSP, or other third party that materially increases AML/CFT risk.

EDD measures shall be proportionate to the risk identified and shall include, where applicable: obtaining additional identification and verification evidence; obtaining additional information on occupation, business activity, expected account activity, and the intended nature of the relationship; identifying and verifying beneficial owners and persons exercising ultimate effective control; establishing and verifying source of funds and, where relevant, source of wealth; obtaining information on the reasons for intended or performed transactions; requiring that payment methods, accounts, wallets, and withdrawals are satisfactorily linked to the customer or otherwise separately verified; obtaining senior management approval before establishing or continuing the relationship where required; and applying enhanced ongoing monitoring.

For EDD cases, the minimum evidence to be considered shall include, as applicable: valid government-issued identification; proof of address; verified phone and e-mail data; liveness, selfie, device, IP, geolocation, and funding-method checks; public-source and database checks; corporate registry and control documents; beneficial ownership declarations and supporting evidence; and independent supporting evidence for source of funds and source of wealth. Where risk is elevated, declarations alone shall not be sufficient if they are not supported by independent and reliable information.

EDD shall be initiated immediately upon identification of a trigger and escalated to Compliance or the MLRO without delay. Where the applicable statutory CDD threshold has been reached, full CDD and any required EDD shall be completed as required by law. If requested information or documents are not received within 30 days from the threshold date, the Company shall terminate, block, or suspend the relationship in accordance with applicable law and MLRO direction. Where a customer is newly identified as a PEP during the relationship, the Company shall implement the required enhanced measures within 30 days or terminate the relationship.

All EDD cases shall be documented in an EDD case file or equivalent record. The record shall include the trigger, risk rationale, evidence requested and received, beneficial ownership findings, source of funds/wealth analysis, approvals, restrictions applied, monitoring settings, review date, escalation decisions, and reporting outcome. All CDD/EDD records, transaction records, account files, business correspondence, and related analyses shall be retained for at

least five years after the relationship ends or after the date of the occasional transaction, in accordance with applicable law.

The MLRO or Compliance Officer shall oversee EDD design, case assessment, escalation, and reporting. Senior Management shall approve the commencement or continuation of relationships where required under this Policy, including PEP relationships and any other EDD cases designated by internal procedures. The Board shall approve this Policy and receive periodic management information on the EDD population, overdue files, material breaches, and external reporting.

Where EDD identifies an unusual or suspicious transaction, or a transaction meeting an objective reporting indicator, the matter shall be escalated internally without delay and reported externally in accordance with the Company's reporting procedures. No employee may disclose to the customer or to any third party that a report has been made or is being considered.

For the avoidance of doubt, Section 6 sets out the Company's customer risk-classification methodology. A customer classified as High Risk under Section 6 shall be subject to EDD under this Section. Conversely, an EDD trigger identified under this Section may require the customer's risk classification in Section 6 to be upgraded and the relationship to be reassessed.

8. CUSTOMER RISK ASSESSMENT FACTORS

The Company shall apply a risk-based approach when assessing and classifying customers and shall consider a range of risk factors in determining whether a customer is classified as Low, Medium, or High Risk, in accordance with Section 6 of this Policy.

Customer risk assessment shall take into account, at a minimum, the following categories:

- product, service, and transaction risk;
- customer-specific risk;
- geographical risk.

In assessing the level of ML/TF risk associated with a customer, the Company shall consider, inter alia, the following factors:

- the customer's country of residence, registration, or operation;
- the customer's country of birth and nationality;
- the customer's occupation, profession, and economic activity;
- whether the customer or any associated party appears on sanctions lists;
- whether the customer or any associated party is identified as a PEP;
- the delivery channel, including whether the relationship is established face-to-face or remotely;

- the source of wealth and source of funds;
- the expected type, volume, and size of transactions;
- any other relevant information obtained through Customer Due Diligence or ongoing monitoring.

Where one or more risk factors indicate an increased level of risk, the customer shall be classified accordingly and EDD measures shall be applied in accordance with Section 7.2 of this Policy.

8.1. Clients Acceptance Policy

The Company shall apply a risk-based approach when establishing or maintaining business relationships and shall not enter into or continue a relationship where the money laundering or terrorist financing risk cannot be effectively mitigated.

The Company shall refuse to establish or maintain a business relationship in circumstances including, but not limited to, the following:

- where the identity of the customer, beneficial owner, or any person acting on behalf of the customer cannot be adequately verified in accordance with applicable Customer Due Diligence requirements;
- where the source of funds or source of wealth cannot be reasonably established or is inconsistent with the customer's known profile;
- where the customer, beneficial owner, or any associated party is subject to applicable sanctions or restrictive measures;
- where the customer is identified as presenting a level of risk that exceeds the Company's risk appetite and cannot be effectively managed through EDD measures;
- where there is reliable information indicating involvement in criminal activity, including money laundering, terrorist financing, or fraud;
- where the customer has previously been subject to termination of a business relationship for AML/CFT-related reasons;
- where the customer refuses to provide required information or documentation necessary to comply with AML/CFT obligations.

The Company shall not establish or maintain business relationships involving jurisdictions subject to applicable sanctions regimes or identified as high-risk by relevant authorities, including the FATF, unless appropriate mitigating measures are applied and senior management approval is obtained.

Additional restrictions may apply in accordance with the Company's internal policies, including regulatory, legal, or commercial considerations; however, such restrictions are maintained separately from this AML/CFT Policy.

8.2. Ongoing Client Due Diligence

Periodic and risk-based reviews are carried out to ensure that Client-related documents, data or information are kept up-to-date.

8.3. Monitoring of Transactions

Compliance department functions ensure that ongoing transaction monitoring is conducted to detect transactions which are unusual or suspicious compared to the Client's risk profile (expected versus real transactional behavior).

8.4. Record keeping

Records of personal data obtained for the purposes of preventing money laundering and terrorist financing shall be processed and retained in accordance with applicable data protection laws and regulatory requirements. Such data shall be used only for lawful AML/CFT purposes and retained for the required statutory period. Where necessary to comply with AML/CFT obligations, such obligations shall take precedence over confidentiality or data protection restrictions to the extent permitted by law.

9. MONITORING ACCOUNTS FOR SUSPICIOUS ACTIVITY

The Company shall establish and maintain appropriate systems and controls to monitor customer behavior and risk-based activities on an ongoing basis, with the objective of identifying and detecting unusual or suspicious transactions.

In accordance with applicable Anti-Money Laundering and Counter-Terrorist Financing laws and regulations, the Company shall determine whether customers or business partners are PEPs or subject to applicable sanctions measures.

PEP and sanctions screening shall be conducted prior to the establishment of a business relationship and on an ongoing basis throughout the duration of the relationship. Additional screening and verification measures shall be applied where a customer is identified as higher risk, including during EDD procedures.

9.1. Politically Exposed Persons

The requirements relating to PEPs are preventive in nature and form part of the Company's risk-based Anti-Money Laundering and Counter-Terrorist Financing framework.

The Company shall maintain appropriate risk management systems and procedures to determine:

- Whether a customer, beneficial owner, or any person acting on behalf of a customer is a PEP;
- Whether such a customer relationship may be established or continued; and
- What enhanced risk-mitigating measures must be applied.

Definition of a PEP

A Politically Exposed Person is a natural person who is or has been entrusted with a prominent public function. This includes, but is not limited to:

- Heads of State or Government;
- Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries;
- Members of Parliament or similar legislative bodies;
- Members of governing bodies of political parties;
- Members of supreme courts, constitutional courts, or other high-level judicial bodies;
- Members of courts of auditors or central bank boards;
- Ambassadors, chargé d'affaires, and high-ranking military officials;
- Members of administrative, management, or supervisory bodies of state-owned enterprises;
- Persons exercising equivalent functions within international organizations.

Categories of PEPs

In line with Financial Action Task Force standards, the Company distinguishes between:

- **Foreign PEPs:** Individuals entrusted with prominent public functions in a foreign country;
- **Domestic PEPs:** Individuals entrusted with prominent public functions within the Company's jurisdiction;
- **International Organization PEPs:** Individuals entrusted with prominent functions by an international organization.

Family Members and Close Associates

The definition of a PEP extends to:

Immediate family members, including:

- Spouse or equivalent partner;
- Children and their spouses or equivalent partners;
- Parents.

Close associates, meaning:

- Individuals known to have joint beneficial ownership of legal entities or arrangements with a PEP;
- Individuals having close business relations with a PEP;

- Individuals who are the sole beneficial owners of legal entities or arrangements known to have been established for the benefit of a PEP.

Risk-Based Treatment

The Company applies a risk-based approach to PEPs:

- **Foreign PEPs** shall always be treated as high-risk and subject to EDD, including senior management approval, source of wealth and source of funds verification, and enhanced ongoing monitoring.
- **Domestic PEPs and International Organization PEPs** shall be subject to a risk-based assessment and enhanced measures where higher risks are identified.
- **Family members and close associates** shall be subject to the same level of scrutiny as the associated PEP.

PEP status shall not automatically cease after a fixed period. Former PEPs shall continue to be assessed on a risk basis, taking into account the level of influence retained and other relevant risk factors.

The Company shall maintain risk-management systems to identify whether a customer, beneficial owner, family member, or close associate is a PEP. PEP screening shall be performed at onboarding, on material customer changes, and on an ongoing basis during the business relationship. Foreign PEPs shall be treated as High Risk. Domestic PEPs and persons entrusted with a prominent function by an international organization shall be subject to a risk-based assessment and, where the relationship is higher risk, the measures in this Section shall apply. PEP status alone shall not automatically prohibit a business relationship; acceptance or continuation depends on completion of Enhanced Due Diligence, the customer risk classification, and the approval process set out below.

Where a customer or beneficial owner is identified as a PEP, the Company shall: obtain senior management approval before establishing or continuing the relationship; take reasonable measures to establish source of wealth and source of funds; verify relevant public-function and ownership information from independent and reliable sources; and apply enhanced ongoing monitoring. At a minimum, the PEP file shall contain screening results, identification data, beneficial-ownership information where applicable, public-source verification, source-of-funds/source-of-wealth evidence, approval in writing, and the rationale for the customer's risk rating.

If an existing customer is identified as a PEP after onboarding, the required measures shall be completed within 30 calendar days from identification; failing that, the relationship shall be terminated. Active PEP files shall be reviewed at least every 6 months as an internal minimum, and sooner where activity, geography, ownership, or adverse information changes. Any

transaction or behavior giving rise to suspicion shall be escalated to the MLRO/Compliance immediately, documented in an internal SAR/STR case memo, and reported externally to FIU Curaçao without delay where required. No employee may disclose to the customer or any third party that a report has been or may be made.

9.2. Sanctions

The Company shall maintain a documented sanctions and targeted financial sanctions framework designed to prevent the Company from making funds, economic resources, products, or services available, directly or indirectly, to designated persons, entities, or prohibited jurisdictions, and to ensure compliance with applicable Curaçao sanctions law, the Kingdom sanctions framework, and relevant international sanctions obligations.

Screening shall apply, at a minimum, to customers, beneficial owners and UBOs, directors, authorized signatories, representatives, beneficiaries, counterparties to relevant financial transactions, and any affiliates, introducers, payment providers, or other third parties whose relationship with the Company could expose it to sanctions risk. This broader scope is appropriate because Curaçao official guidance on sanctions hits expects institutions to look not only at direct customers, but also at ownership, control, representatives, counterparties, and connected persons and structures.

Screening shall occur before account activation or first material financial activity, on an ongoing basis throughout the business relationship, upon changes to official sanctions or high-risk jurisdiction lists, and on an event-driven basis when customer data, ownership, control, geography, payment details, device or access patterns, or other risk-relevant information changes. Transaction screening shall be applied at least before withdrawals and payouts, and on a risk-sensitive basis to other deposits, transfers, refunds, reversals, and payment instructions.

The Company shall screen against the legally applicable sanctions sources for Curaçao, including measures implemented under the Sanctions National Ordinance and related Curaçao decrees, Kingdom/EU sanctions applicable through the Kingdom sanctions framework, and relevant United Nations Security Council sanctions designations. The Company may also use supplemental external lists and datasets, including those published by Office of Foreign Assets Control, for enhanced risk detection, correspondent banking, PSP, or contractual risk management; however, supplemental lists do not by themselves create a Curaçao legal freezing duty unless otherwise applicable by law or contract.

Automated screening shall be the default for onboarding, periodic rescreening, and transaction screening where technologically feasible. Manual screening may be used only as a

documented fallback for exception handling, system outage, low-volume cases, or enhanced review. All manual reviews, overrides, and close-outs shall be recorded. This is consistent with the Company's own control design in its BRA and with the supervisory expectation that institutions maintain documented sanctions screening procedures and outcomes.

Potential matches shall be reviewed promptly by Compliance using all available identifiers, including name variants, aliases, date of birth, nationality, address, identification numbers, ownership and control information, and transaction context. If the match cannot be confidently cleared, the case shall be escalated to the MLRO without delay. False positives may be closed only on documented grounds. Customer contact during hit review must be strictly controlled to avoid tipping-off.

Where a true match or sufficiently confirmed match exists, the Company shall immediately freeze or block the relevant funds or assets and prevent withdrawals, payouts, transfers, refunds, bonuses, affiliate payments, account changes, or continued service provision, without prior notice to the customer. The Company shall also place a legal and records hold on the account and related files, preserve the balance snapshot, pending transactions, alert evidence, list version, and decision trail, and maintain the freeze until lawful clearance, release, or other competent instruction is received. In doing so, the Company shall take account of the applicable Curaçao process for asset freezing and of the interests of third parties acting in good faith.

Any intended or executed transaction by or for the benefit of a person or entity designated under the Curaçao sanctions framework must be reported to the FIU without delay through the goAML process, together with supporting information. In addition, confirmed sanctions matches shall be reported immediately to the competent gaming supervisor, with identifying information and freeze details. Where there is evidence of attempted sanctions circumvention, concealment of ownership, use of proxies, or other sanctions-evasion indicators, the Company shall also assess and report under the subjective unusual-transaction indicator without delay, even if the legal designation analysis is still developing.

No director, officer, employee, contractor, or affiliate of the Company may disclose to a customer or third party that sanctions screening has generated a hit, that a report has been or may be filed, or that law-enforcement, security-service, regulatory, or FIU engagement is underway, except where disclosure is legally required and approved by the MLRO and legal counsel. Internal sharing shall be limited to a need-to-know basis.

The Company shall retain sanctions screening records, hit analysis, escalation logs, MLRO decisions, regulator and FIU reports, freeze and unfreeze actions, related communications, and system and list evidence for at least five years, and longer where required by law or instructed

by the FIU or another competent authority. Records must be sufficient to reconstruct the case and demonstrate the timeliness and rationale of every material decision.

Sanctions and TFS controls shall be subject to periodic quality assurance and at least annual independent testing, including review of list currency, sample alert validation, false-positive handling, escalation timeliness, freeze and unfreeze handling, record retention, and staff adherence to confidentiality rules. Relevant staff, managers, and the Board shall receive initial and refresher training appropriate to their roles. This subsection shall be applied consistently with the Company's Business Risk Assessment, including its controls on sanctions screening, affiliate onboarding, and geographic restrictions, and any material BRA change shall trigger a review of this subsection.

9.3. Measures in Case of PEP and Sanctions Matches

The Company shall maintain documented procedures for the identification, assessment, and escalation of PEP and sanctions screening alerts.

All alerts generated through screening systems shall be promptly reviewed by designated operational teams to determine whether they constitute false positives or potential matches. Where an alert cannot be reasonably dismissed, it shall be escalated without delay to the MLRO. The MLRO shall be responsible for assessing escalated alerts and determining appropriate actions in accordance with the Company's AML/CFT framework.

In the case of a confirmed or potential PEP relationship, the Company shall:

- obtain senior management approval prior to establishing or continuing the business relationship;
- apply enhanced due diligence measures, including establishing the source of wealth and, where applicable, source of funds;
- apply enhanced and ongoing monitoring of the relationship.

In the case of a confirmed sanctions match, the Company shall:

- immediately freeze or block all relevant assets or transactions without delay and without prior notice;
- prohibit any further transactions or business activity;
- escalate the matter to the MLRO for further action, including regulatory reporting where required.

All decisions, actions, and supporting documentation relating to PEP and sanctions alerts shall be properly documented and retained in accordance with the Company's record-keeping obligations.

9.4. Transaction Monitoring, Alert Triggers and Escalation Framework

The Company shall maintain a structured, risk-based transaction monitoring and escalation framework designed to detect, assess, and respond to unusual or suspicious activity in a consistent, timely, and auditable manner.

Transaction monitoring shall be conducted on an ongoing basis using automated systems and manual controls, taking into account the customer's risk profile, expected activity, and relevant risk indicators.

1. Monitoring Principles

The Company shall:

- Monitor customer activity against the expected profile established during CDD and EDD;
- Apply both rule-based and risk-based monitoring scenarios;
- Ensure that monitoring controls are aligned with the Company's Business Risk Assessment;
- Review and update monitoring rules and thresholds periodically to reflect emerging risks and regulatory expectations.

2. Alert Triggers

The following non-exhaustive triggers shall generate alerts and require review:

a) Transaction Value and Velocity

- Single or aggregated deposits or withdrawals exceeding predefined internal thresholds;
- Rapid movement of funds (e.g., multiple deposits and withdrawals within a short timeframe);
- Significant increase in transaction volume inconsistent with customer profile.

b) Behavioral Indicators

- Minimal or no gameplay following deposits (indicative of potential money laundering);
- Sudden changes in betting or transactional patterns;
- Repeated use of bonus structures without genuine gameplay activity.

c) Payment and Funding Risks

- Use of third-party payment methods or mismatched account names;
- Use of multiple payment instruments without clear justification;
- Transactions involving high-risk payment methods (e.g., prepaid cards, crypto assets with anonymity features).

d) Geographic Risk

- Access or transactions originating from high-risk or sanctioned jurisdictions;
- Use of VPNs, proxies, or other tools to mask location;
- Inconsistencies between declared residence and actual access location.

e) Customer Risk Factors

- Customers identified as high-risk, including Politically Exposed Persons (PEPs);
- Negative media or adverse information identified post-onboarding;
- Refusal or delay in providing requested CDD/EDD documentation.

3. Escalation and Actions

All alerts shall be subject to a structured review and escalation process:

- **Level 1 – Initial Review:**
Operational teams shall review alerts to determine whether they can be reasonably explained or represent a false positive.
- **Level 2 – Compliance Escalation:**
Alerts that cannot be cleared shall be escalated to Compliance or the MLRO for further assessment.
- **Level 3 – MLRO Decision:**
The MLRO shall determine appropriate actions, which may include:
 - Application of EDD;
 - Request for additional information or documentation;
 - Temporary restriction or suspension of the account;
 - Filing of an Internal SAR;
 - Submission of an external report to FIU Curaçao via goAML.

4. Mandatory Escalation Triggers

The following circumstances shall require immediate escalation to the MLRO without delay:

- Transactions suspected to be linked to money laundering, terrorist financing, or sanctions evasion;
- Transactions involving sanctioned individuals or entities;
- Inability to verify source of funds or source of wealth for significant transactions;
- Patterns clearly inconsistent with the customer's known profile and lacking reasonable explanation.

5. Documentation and Record Keeping

All alerts, reviews, escalation decisions, and actions taken shall be:

- Fully documented with supporting rationale;
- Retained in accordance with the Company's record-keeping requirements;
- Available for internal audit and regulatory review.

6. Review and Calibration

The Company shall:

- Periodically review monitoring thresholds, scenarios, and effectiveness;

- Adjust controls based on findings from the Business Risk Assessment, audit results, and regulatory feedback;
- Ensure that monitoring systems remain proportionate to the Company's risk profile and operational scale.

10. ORGANISATION OF INTERNAL CONTROL

10.1 Suspicious Activity and Unusual Transaction Reporting

Purpose and scope

The Company shall maintain a confidential framework for the identification, internal escalation, documentation, assessment, and external reporting of suspicious activity and unusual transactions. This framework applies to all employees and relevant contractors, all customers and accounts, all deposits, withdrawals, transfers, gameplay-related financial activity, attempted transactions, customer due diligence findings, sanctions alerts, fraud alerts, and any other facts that may indicate money laundering, terrorist financing, proliferation financing, sanctions evasion, or other criminal conduct.

Definitions

For this Policy:

- (i) **Internal SAR** means a confidential internal referral made to the MLRO or duly appointed deputy concerning potentially suspicious activity or a transaction that may meet a Curaçao unusual-transaction indicator;
- (ii) **External report** means the legally required report of an unusual transaction to FIU Curaçao via goAML; and
- (iii) **tipping-off** means disclosing to the customer or any unauthorized third party that an internal SAR has been made, that an external report has been or may be filed, or that FIU Curaçao has requested information. Under Curaçao's reporting model, the Company reports unusual transactions to the FIU, and the FIU analyzes those reports and disseminates suspicious transactions to competent authorities after analysis.

Internal reporting process

Any employee who knows, suspects, or has reasonable grounds to suspect that activity or a transaction is unusual or may relate to money laundering, terrorist financing, proliferation financing, or sanctions evasion, or who identifies an objective reporting indicator, must submit an Internal SAR to the MLRO without delay and attach available supporting records. Internal SARs may not be suppressed, filtered, or closed by business-line management. Internal escalation does not require proof; suspicion, reasonable grounds, or a reportable objective indicator is sufficient.

Escalation and MLRO responsibility

The MLRO shall independently review each Internal SAR for completeness, compare it against customer identification records, CDD/EDD information, transaction data, sanctions screening, monitoring alerts, and other available sources, and decide whether an external report must be filed. The MLRO shall document the assessment, any additional inquiries, any decision to apply enhanced monitoring or account restrictions, the external filing decision, and the rationale for any decision not to file externally. Where the Company has separately appointed an AML/CFT compliance officer, role allocation between that officer and the MLRO shall be documented in writing, but responsibility for timely external reporting shall remain clear at all times.

External reporting triggers and timelines

The Company shall file an external report to FIU Curaçao via goAML without delay when an executed or intended transaction meets a Curaçao reporting trigger, including: a transaction already reported to police or justice; a transaction by or on behalf of a listed person or entity; gaming transactions of NAf 5,000 or more, including linked transactions and patterns considered per gaming day; or circumstances giving reason to presume money laundering or terrorist financing. The Company shall also treat attempted transactions and suspicion-based cases as reportable irrespective of amount, in line with FATF Recommendation 20. The cited Curaçao sources use “without delay” and “timely” language and do not specify a fixed number of hours or days; accordingly, the policy should require filing as soon as sufficient facts exist to complete the report, without waiting for proof or for a full internal investigation to conclude. Reports and supporting documents filed through goAML shall be submitted in English. Any FIU follow-up request for additional information shall be answered within the deadline specified by the FIU.

Tipping-off controls and staff protections

Neither the Company nor its directors, officers, employees, or relevant contractors may disclose to the customer or to any unauthorized third party that an Internal SAR has been made, that an external report has been or may be filed, or that the FIU has requested information. Any customer-facing action after suspicion arises, including suspension, blocking, freezing, rejection, or termination, shall be assessed by the MLRO for tipping-off risk before implementation. Where legally permissible and operationally appropriate, enhanced monitoring and further reporting should be preferred over unnecessary customer-facing action that could alert the customer. Employees who make or support internal or external reports in good faith shall be protected from retaliation by the Company, consistent with the statutory protections against criminal, civil, and damages liability for good-faith reporting under Curaçao law and FATF standards.

Recordkeeping

The Company shall retain Internal SARs, MLRO assessments, external reporting details, supporting evidence, related communications, and correspondence with the FIU for at least five years, and longer where required by law or FIU instruction. Where FIU Curaçao instructs an extended retention period, retention shall be increased up to ten years. Related customer, CDD, and transaction records shall also be retained for at least five years after the business relationship ends or after the date of the occasional transaction, as applicable.

Training and monitoring

The Company shall provide onboarding and periodic refresher training to relevant personnel on unusual-transaction indicators, immediate internal escalation, MLRO reporting lines, no tipping-off obligations, and recordkeeping. The MLRO shall monitor the timeliness and completeness of Internal SAR handling and maintain a register of internally reported cases, externally filed cases, and non-filed cases with documented rationale. Independent testing shall periodically sample unusual transactions, threshold and non-threshold cases, and assess compliance with internal and external reporting requirements and the adequacy of record retention.

10.2. goAML Registration and Reporting Obligations

The Company complies with all applicable laws and regulations relating to the reporting of suspicious activities to the Financial Intelligence Unit Curaçao (FIU Curaçao). The Company is duly registered with and maintains active access to the goAML reporting system, as designated by FIU Curaçao for the submission of Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs).

The Company has appointed a MLRO, who is responsible for the administration and use of the goAML system. Relevant personnel are trained in the identification, escalation, and handling of suspicious activities, and internal procedures are implemented to support the timely and effective reporting process.

Where, in the course of customer due diligence, enhanced due diligence, transaction monitoring, or otherwise, the Company knows, suspects, or has reasonable grounds to suspect that funds or transactions may be linked to money laundering, terrorist financing, or other criminal conduct, such matters are promptly escalated to the MLRO. The MLRO assesses the available information without undue delay and, where appropriate, submits a report to FIU Curaçao via the goAML system in accordance with applicable legal and regulatory requirements.

All reports submitted through goAML, together with supporting documentation and internal analyses, are properly documented, securely retained, and made available to competent authorities in accordance with applicable record-keeping obligations.

The Company and its employees comply with all confidentiality requirements, including the prohibition on tipping-off. No information relating to the submission of a report or the existence of a related investigation is disclosed to any customer or unauthorized third party.

10.3. Procedures

The Company shall ensure that all relevant departments implement and maintain documented operational procedures designed to give effect to the Company's AML/CFT policies and controls. Such procedures shall be proportionate to the nature, scale, and complexity of the Company's activities and shall take into account applicable legal and regulatory requirements, including those issued by the Curaçao Gaming Authority.

The procedures shall, at a minimum, address customer due diligence, ongoing monitoring, transaction processing, suspicious activity reporting, sanctions screening, and record-keeping obligations, and shall ensure consistent application of AML/CFT measures across the organization.

The MLRO shall oversee the adequacy and implementation of such procedures and ensure that they are kept up to date and aligned with the Company's risk profile and regulatory obligations.

10.4. Training

The Company shall establish and maintain an ongoing AML/CFT training program to ensure that all employees are adequately informed of their legal and regulatory obligations and are capable of effectively identifying and reporting suspicious activities. All employees shall receive AML/CFT training upon commencement of employment as part of the onboarding process. In addition, all employees shall complete mandatory AML/CFT refresher training on at least an annual basis.

The Company shall apply a risk-based approach to training, whereby employees with higher exposure to AML/CFT risks, including those involved in customer onboarding, transaction processing, compliance, or management functions, shall receive enhanced and role-specific training tailored to their responsibilities.

The training program shall cover, inter alia, applicable AML/CFT laws and regulations, internal policies and procedures, identification of suspicious activities, reporting obligations, and the prohibition of tipping-off. The Company shall maintain appropriate records of all training delivered, including attendance and completion, and shall ensure that the effectiveness of the training program is periodically reviewed.

The MLRO shall oversee the implementation of the AML/CFT training program and ensure that employees remain adequately trained at all times. Failure to comply with training requirements may result in disciplinary measures in accordance with the Company's internal policies.

10.5. Compliance Monitoring Program

The Company shall establish and maintain a Compliance Monitoring Program to assess the effectiveness and adequacy of its AML/CFT framework, including its policies, procedures, and internal controls.

The Compliance Monitoring Program shall include periodic reviews and testing of key AML/CFT controls, including customer due diligence, transaction monitoring, suspicious activity reporting, sanctions screening, and record-keeping processes. Such monitoring shall be conducted on a risk-based basis, taking into account the nature, scale, and complexity of the Company's activities.

The MLRO shall be responsible for overseeing the implementation of the Compliance Monitoring Program and ensuring that identified deficiencies are documented, reported to senior management, and remediated in a timely manner.

The results of compliance monitoring activities shall be recorded and, where appropriate, reported to senior management and the Board to ensure effective oversight of AML/CFT risks.

In addition, independent AML/CFT testing shall be conducted by an appropriately qualified and independent function, which shall not be involved in the design, implementation, or operation of the Company's AML/CFT controls, in order to ensure objectivity and impartiality of the review.

10.6. Staff Due Diligence

The Company shall ensure that all employees are of appropriate integrity, competence, and reliability, and commensurate with the nature of their roles and responsibilities within the organization. To this end, the Company shall implement and maintain adequate staff due diligence procedures as part of its Anti-Money Laundering and Counter-Terrorist Financing framework.

Prior to employment, all candidates shall be subject to appropriate screening measures, which shall include, at a minimum, verification of identity, review of curriculum vitae, confirmation of relevant qualifications and professional certifications, and the obtaining of references. Such information shall be assessed and verified by the Human Resources Department.

The Company shall adopt a risk-based approach to staff screening, taking into account the level of access to sensitive systems, financial transactions, or AML/CFT controls. Enhanced screening measures may be applied to employees in high-risk or control functions, including senior management, compliance personnel, and those involved in payment processing or customer onboarding.

Ongoing assessment of employee integrity and performance shall be conducted throughout the duration of employment through appropriate supervision, control, and appraisal mechanisms. Where necessary, periodic re-assessment or additional checks may be performed. All employees shall be required to adhere to the Company's AML/CFT policies and procedures and shall receive appropriate training in accordance with their roles. Any concerns relating to employee conduct, integrity, or potential involvement in suspicious activities shall be escalated without delay in accordance with internal reporting procedures.

10.7. Record Retention and Record Keeping

The Company shall create, maintain and retain, in an accessible and readily retrievable form, all records necessary to evidence compliance with the applicable anti-money laundering, counter-terrorist financing and counter-proliferation financing laws and regulations of Curaçao and with lawful requests of the competent authorities, including the Curaçao Gaming Authority and FIU Curaçao. Such records shall include, at a minimum, customer due diligence and know-your-customer records; beneficial ownership and control information; customer risk assessments and account files; records of deposits, withdrawals, transfers, wallets, payment instruments and other transaction data; enhanced due diligence materials, including source of funds and source of wealth information; PEP and sanctions screening results and related decisions; records of unusual or suspicious activity reviews, internal investigations, internal referrals and external UTR/STR/SAR reports and supporting analyses; AML/CFT governance and management information; training records; audit, monitoring and remediation records; and all other documents and information necessary to reconstruct individual transactions and decision-making.

All such records shall be retained for not less than five (5) years after the end of the business relationship or the date of the occasional transaction, as applicable, and for not less than five (5) years after the execution of the relevant transaction where the law so requires. Without

prejudice to any longer retention period required under other applicable laws, including tax, accounting, gaming and data-protection laws, the relevant records shall be retained for the longer period where required by law or where FIU Curaçao lawfully directs an extended period, including up to ten (10) years in relation to a transaction declared suspicious. Records shall be maintained so as to preserve their integrity, accuracy, readability and auditability, protected against unauthorized access, alteration, loss or destruction, and supported by appropriate back-up and recovery measures. They shall be capable of being produced without undue delay to the competent supervisory, investigative, prosecutorial or judicial authorities. Deletion, destruction or anonymization shall take place only after expiry of the applicable retention period and only where no legal, regulatory, investigative or litigation hold applies. The MLRO shall oversee compliance with this Section; provided that detailed technical and operational implementation measures, including system-specific retention schedules, access controls, storage architecture, back-up routines and deletion workflows, shall be governed by separate procedures and the internal handbook of operations.