



Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy

Company: Nuxgen B.V. (the "Company")
Effective Date: May 14, 2025

1. Policy Statement

Nuxgen B.V. is fully committed to conducting its business in an honest and ethical manner, in compliance with all applicable laws and regulations aimed at combating Money Laundering (ML) and Terrorism Financing (TF). This AML/CTF Policy (the "Policy") outlines the Company's framework to prevent its products and services from being used to facilitate ML/TF or other illicit activities. The Policy applies to all operations of Nuxgen B.V. and to all employees, officers, contractors, and third parties acting on the Company's behalf.

2. Purpose

The purpose of this Policy is to set forth the Company's internal standards and procedures for compliance with anti-money laundering and counter-terrorism financing requirements. It is designed to ensure Nuxgen B.V. meets the obligations under the Financial Action Task Force (FATF) Recommendations and Curaçao's AML/CFT laws and regulations. By implementing this Policy, the Company seeks to prevent, detect, and mitigate the risk of ML/TF, protect the Company's reputation, and avoid legal and regulatory penalties.

3. Audience

This Policy is mandatory for all Nuxgen B.V. personnel, including contractors, management, directors, and any third-party agents or service providers who have responsibilities that involve the Company's clients or financial transactions. All such persons must understand and comply with the Policy in their daily activities. The Policy is also relevant to the Company's business partners and suppliers to the extent they are involved in processes governed by this Policy.

4. Definitions

Money Laundering (ML): The process by which criminals conceal or disguise the origins of illegally obtained money ("dirty money") by making it appear legitimate. This often involves multiple transactions or layers (placement, layering, integration) to distance the funds from their illicit source. ML also includes the use of legal funds to support terrorism or other criminal acts.

Terrorism Financing (TF): Providing, collecting, or using funds, whether from legal or illegal sources, to support acts of terrorism. TF may involve smaller sums and can use similar concealment techniques as money laundering to hide the terrorist purpose of funds.

Know Your Client (KYC): The process of identifying and verifying the identity of the Company's clients and understanding relevant information about them. KYC entails Customer Identification Program (CIP), Customer Due Diligence (CDD), and ongoing monitoring to ensure the Company knows who its clients are and the nature of their business.

Customer Due Diligence (CDD): A set of procedures to collect and evaluate information about a client to assess the risk of ML/TF. CDD includes verifying a client's identity, understanding the purpose of the business relationship, identifying beneficial owners, and screening for risk factors such as Politically Exposed Persons or sanctions.

Enhanced Due Diligence (EDD): Additional investigative measures performed for higher-risk clients or situations. EDD may include obtaining extra information about the client's business activities, source of funds, financial statements, and closer scrutiny of ownership structures. EDD is required, for example, when a client is classified as high risk, such as a client with complex corporate structures, from a high-risk jurisdiction, or with Politically Exposed Persons involved.

Employee (or employees): all Contractors or other stuff of the Company.

Beneficial Owner: The natural person(s) who ultimately own or control a client entity. Typically, this includes any individual who owns 25% or more of the company's shares or voting rights, or otherwise exercises control over the company's management. If no individual meets the 25% threshold, the beneficial owner is the person(s) who otherwise control the entity (e.g. senior managing official). All such persons are subject to identification and verification under this Policy.

Politically Exposed Person (PEP): An individual who is or has been entrusted with prominent public functions, such as a government official, senior politician, senior executive of state-owned corporations, judicial or military official, or important political party official. The definition of PEP includes their immediate family members and close associates. PEP status in a client's ownership or management structure is a risk factor requiring enhanced due diligence due to the higher risk of corruption associated with PEPs.

Financial Intelligence Unit (FIU): The authority in Curaçao responsible for receiving, analyzing, and investigating reports of unusual or suspicious transactions (also known in Curaçao as the Meldpunt Ongebruikelijke Transacties). FIU Curaçao is the competent authority to which Nuxgen must report any transactions or activities that are identified as suspicious or unusual under the law.

Suspicious Activity/Unusual Transaction: A transaction or attempted transaction that is inconsistent with a client's known legitimate business, or that has no apparent economic or lawful purpose, or which is indicative of potential criminal activity. Within this Policy, any sign of potential ML/TF is considered suspicious and will trigger internal review and possible reporting.

(Any other relevant terms used in this Policy can be found in the context of their usage)

5. Policy Implementation

This section details how the Policy is put into practice through specific measures and procedures. Nuxgen employs a risk-based approach to AML/CTF, meaning resources and scrutiny are directed in proportion to the level of risk presented. Key implementation areas include risk assessments, client due diligence, monitoring, and reporting, as outlined below.

5.1. Business Risk Assessment

Nuxgen conducts a comprehensive Business Risk Assessment to identify and evaluate the money laundering and terrorist financing risks inherent in its business model. This assessment considers factors such as the nature of the Company's products and services, the methods of delivery, the types of clients, the geographies of operation, and any use of new technologies.

- **Risk Identification:** The Company identifies how its IT products and gaming services might be potentially misused for ML/TF.
- **Risk Evaluation** Each identified risk scenario is analyzed for likelihood and potential impact. Factors such as transaction volume, payment methods (e.g., bank transfers, digital currencies), client industry and jurisdiction, and the regulatory environment are examined.
- **Risk Mitigation:** Based on the assessment, the Company ensures that its policies, procedures, and controls (such as client due diligence protocols, transaction monitoring, and staff training) are adequate to mitigate the identified risks. If certain risks are deemed insufficiently mitigated, the Company will enhance its controls or refrain from engaging in higher-risk activities.

Revisions to the risk assessment occur when there are material changes to the business (e.g., expansion to new markets, offering new types of services, or changes in applicable laws) to ensure emerging risks are promptly addressed.

5.2. Customer (Client) Risk Assessment

For each prospective client, Nuxgen B. V. performs a Customer Risk Assessment as part of its onboarding due diligence. The risk assessment evaluates the particular ML/TF risks associated with that client relationship. This assessment is done when establishing a business relationship and updated if the client's profile changes significantly or new risk factors emerge.

Key factors considered in a Client Risk Assessment include:

- **Jurisdiction Risk:** The country or countries where the client is incorporated, licensed, or operating. Clients from jurisdictions known for high levels of corruption, subject to sanctions or embargoes, identified by FATF as high-risk or non-cooperative, or lacking effective AML/CFT controls are considered higher risk.
- **Industry/Business Risk:** The nature of the client's business. All clients are in the gaming sector by the nature of Nuxgen's services, but their specific business model and the extent to which they themselves are regulated for AML can affect risk. The Company will verify that each client has a valid operating license from a recognized authority if applicable. Operating without a required license if its applicable is a serious red flag.
- **Ownership and Management Risk:** The transparency and background of the client's ownership structure. The Company examines the shareholding structure to identify all beneficial owners. If a client has complex or opaque ownership (e.g., multiple layers of shell companies or trusts, especially in secrecy jurisdictions), or if beneficial owners are not easily identifiable, the risk is higher.
- **Product/Service Usage Risk:** The expected use of Nuxgen's products by the client. The Company will consider the scope and scale of services the client intends to use.
- **Transaction and Payment Risk:** How the client will pay for the Company's services and from what sources. The Company also examines the client's source of funds – e.g., whether the funds used to pay fees are from the client's legitimate gaming revenue,

capital investment, or other verifiable sources. Clients unable or unwilling to disclose their funding sources will not be accepted.

Based on these factors, the Company assigns a risk rating to each client (e.g., Low, Medium, or High). This risk rating forms the client's risk profile and determines the level of due diligence and ongoing monitoring applied. A higher-risk client will undergo Enhanced Due Diligence (see Section 5.4) and more frequent review.

5.3. Customer Acceptance Policy (CAP)

The Customer Acceptance Policy defines the criteria and process for approving new clients and continuing relationships with existing clients, based on the risk assessment findings. Nuxgen B. V. will only conduct business with clients that meet its standards of integrity and transparency. Key principles of the CAP include:

- **Risk-Based Acceptance Criteria:** Clients assessed as Low or Medium risk may be accepted upon completion of satisfactory CDD. Clients rated as High risk are subject to Enhanced Due Diligence. The Company may set additional conditions for high-risk clients (such as more frequent audits or monitoring) or decide not to onboard them if the risk is deemed too high to manage.
- **Prohibited Clients:** The Company will refuse to onboard or continue business with any client that:
 - Fails or refuses to provide adequate KYC information or documentation as required by the CDD process.
 - Is found to have provided false or misleading identity or business information.
 - Lacks a legitimate business purpose for using Nuxgen's services or where the nature of the client's business cannot be determined.
 - Is an unlicensed operator in a sector where licensing is required (e.g., a gambling operator with no valid gambling license).
 - Has a beneficial owner or key principal who is a known criminal, on an international sanctions list, or who has been convicted of serious financial crimes.
 - Has any connection with jurisdictions, individuals, or activities subject to comprehensive sanctions or embargoes that would prohibit the relationship by law.
 - Presents any other indication of unacceptable risk.
- **PEP and Sanctioned Entity Handling:** If a prospective client or any of its beneficial owners or controlling persons is identified as a PEP or is a sanctioned individual/entity, the Company will apply Enhanced Due Diligence. In the case of a sanctions match (meaning the person or entity is on a relevant sanctions list to which Nuxgen is subject), the Company will **not** onboard the client.
- **Approval:** Every new client must be approved according to an internal process. This process ensures accountability and that no high-risk client is onboarded without proper oversight.
- **Periodic Re-evaluation:** The CAP is not only for initial acceptance but also for continuation of the relationship. If at any time a client's risk profile changes materially (e.g., new negative information, change in ownership to a higher-risk individual, license revocation, etc.), the Company will re-evaluate whether that client remains acceptable under this Policy. The Company reserves the right to terminate any business

relationship that no longer meets the requirements of this Policy or that poses an unacceptable risk.

5.4. Customer Due Diligence (Identification & Verification, PEP/Sanctions Screening)

Nuxgen B.V. implements robust Customer Due Diligence (DD) measures for all clients as required by law and FATF standards. CDD is performed at the start of the business relationship (prior to entering into a contract or providing services) and updated as necessary. The DD process includes:

a. Customer Identification Program (CIP): The Company will identify and verify the identity of every client (corporate customer) through reliable, independent sources. At minimum, the following information and documents must be obtained from a prospective client:

- **Legal Entity Details:** Full legal name, legal form (e.g., LLC, B.V., etc.), registration number, and proof of incorporation/registration (such as a certificate of incorporation or extract from the commercial register).
- **Constitutive Documents:** Key governing documents of the entity, such as the memorandum and articles of association (or equivalent charter documents), and a register of directors or a document listing current directors/executives and their addresses.
- **Business License:** If the client is engaged in a regulated activity, to ensure the client is legally permitted to conduct its business.
- **Registered Address and Contact Information:** The official registered office address of the company and the principal place of business if different. Also obtain main contact details (phone number, email) and the identity of the person(s) acting as the point of contact on behalf of the client.
- **Authorized Representatives:** Identification of individuals who will act on behalf of the. The Company will verify that such persons are authorized by the client (through a power of attorney or corporate resolution) and record their identification information (name, date of birth, position, identification document details).

The Company will verify the provided documents for authenticity. All identification documents and information collected must be current and valid at the time of verification.

b. Beneficial Ownership Identification: In addition to verifying the client entity, Nuxgen will identify any Beneficial Owners of the client. The client is required to disclose all persons who ultimately own or control the entity (as defined in Section 4). For each such Beneficial Owner (and any person owning above a certain threshold, typically 25%, even if they claim not to exercise control), the Company will collect identifying information, including: full name, date of birth, nationality, residential address, and an official photo identification (such as a passport or national ID card). Each Beneficial Owner's identity must be verified.

c. Purpose of Business Relationship: As part of CDD, the Company will gather information on the intended nature and purpose of the business relationship. The client should clarify what services/products they will be using, the expected volume of business.

d. PEP and Sanctions Screening: Once the identifying information is collected, Nuxgen will screen the client and all Beneficial Owners, directors, and controlling persons against relevant PEP lists and sanctions lists.

e. Enhanced Due Diligence (EDD): If the initial CDD measures (a–d above) indicate that the client is high risk (for example, if a PEP is involved, or the client is from a high-risk country, or has an opaque ownership structure, etc.), the Company will conduct Enhanced Due Diligence. Based on EDD findings, the client’s risk profile will update. If the risk is deemed unacceptable, the Company will refuse to onboard the client. These decisions are documented. If the client is onboarded under high risk, the Company will ensure increased monitoring and possibly impose conditions (like periodic review milestones or transaction limits).

f. Approval: No client may be provided access to Nuxgen’s products or services until the CDD (and EDD if applicable) process is completed and the client is formally approved as per the Customer Acceptance Policy. Designated compliance staff must sign off that all required documents have been obtained and verified, and that risk assessment is done. The Company maintains an organized record of all KYC documents, risk assessment forms, and approvals for each client. All such records are retained for at least five (5) years following the end of the client relationship or from the date of the last transaction with the client, whichever is later, in accordance with Curaçao legal requirements. These records include copies of documents, identification data, account files, business correspondence, and results of any analysis undertaken. Records are stored securely (in electronic form).

5.5. Ongoing Monitoring

The Company engages in continuous and ongoing monitoring of its business relationships and transactions to detect unusual or suspicious activities that might indicate money laundering or terrorist financing. This process ensures that the initial risk assessment of the client remains current and that any changes in the client’s behavior or profile are identified.

a. Transaction Monitoring: The Company monitors the financial transactions and account activity associated with each client. The accounting and finance team, in coordination with compliance, will watch for anomalies such as:

- Payments made from accounts not belonging to the client or from unexpected jurisdictions.
- Payments that materially deviate from the agreed-upon amounts or schedule.
- Requests for refunds or transfers to third parties that were not anticipated in the contract.
- Any use of cash or cash-equivalents in transactions.
- Multiple smaller transactions that are broken up without rationale (potential structuring to avoid detection).

The Company uses a risk-based approach in monitoring: higher-risk clients’ transactions are subject to more frequent and detailed review, whereas low-risk clients are monitored through the normal course of business with periodic spot-checks.

b. Activity Monitoring: Beyond financial transactions, Nuxgen monitors the client’s usage of its products/services for consistency with the stated purpose and known business model of the client. Unusual activities could include, for instance, a client ordering an unusually large number of game integrations in a short time without a clear business rationale, or a client not

utilizing the services as expected (which could indicate they intended the contract for facade purposes).

c. Periodic Review of Client Information: On a periodic basis, the Company will refresh KYC information of existing clients, especially for those rated as medium or high risk. At minimum, high-risk clients should be reviewed annually, and medium risk at least every 1–2 years, to confirm that the information on file (ownership, management, license status, etc.) remains up-to-date. Low-risk clients may be reviewed on a three-year cycle, or more frequently if triggered by any material changes. During such reviews, the Company may request updated documents (such as renewed licenses, notices of any changes in directors or owners, latest financial statements) and rescreen the client and its owners for sanctions/PEP status or new adverse media.

d. Monitoring for Specific Red Flags: Employees (especially those in sales, finance, and compliance) are trained to be vigilant for common red flags of ML/TF relevant to a context, including:

- The client makes unusual requests that do not match their normal business.
- The client shows reluctance or refusal to provide routine information or updates, or becomes evasive when asked for clarification on business activities.
- Sudden changes in the client’s ownership or management without a clear reason, especially if new owners are from high-risk jurisdictions or have concerning backgrounds.
- Public news indicating the client is under investigation, facing legal action, or regulatory sanctions, or rumors of the client being in financial difficulty (which could indicate misuse of funds or fraud).
- Transactions or business patterns that lack a visible economic rationale or are excessively complex and costly without logical justification.

If any such red flags or anomalies are detected, they will be promptly reviewed.

e. Escalation: When staff observes any activity that is inconsistent with the client’s profile or otherwise suspicious, they must escalate it to the MLRO (or compliance team). The ongoing monitoring process ensures that even clients initially rated low risk are not exempt from scrutiny – any emerging risk factor will be captured, and the client’s risk rating can be adjusted accordingly.

f. Technology and Tools: The Company may use software tools or automated systems to assist in monitoring transactions and client data against risk indicators.

Through ongoing monitoring, Nuxgen aims to detect any misuse of its services early and take appropriate action before significant issues occur.

5.6. Reliance on Third Parties for CDD (Third-Party Due Diligence)

As a general rule, Nuxgen B.V. prefers to perform its own due diligence on clients to ensure compliance and thoroughness. However, in certain circumstances the Company may rely on third-party sources or service providers to fulfill some KYC/CDD obligations, in accordance with applicable laws (consistent with FATF Recommendation 17).

- **Use of Third-Party Services:** The Company may engage reputable third-party vendors for specific tasks. These are considered extensions of the Company’s compliance

process. When using such services, the Company ensures the vendors are themselves subject to stringent data security measures and, if applicable, AML regulations.

- **Reliance on Regulated Third Parties:** In some cases, a client might be introduced to Nuxgen through an intermediary that has already performed due diligence on the client. The Company may choose to rely on the CDD performed by that third party *only if*:
 1. The third party is a regulated entity subject to equivalent AML/CTF.
 2. The Company has assessed the third party as trustworthy and competent in performing CDD.. If any doubt exists about the adequacy of the third party's due diligence, Nuxgen will conduct its own full CDD despite the referral.
- **Due Diligence on Third-Party Partners:** Separately from client due diligence, the Company also conducts due diligence on significant third-party business partners such as game content providers or other vendors from whom it purchases games or IT services.

5.7. Reporting of Unusual Transactions and Suspicious Activity

Nuxgen B.V. adheres to Curaçao's legal requirements for identifying and reporting unusual or suspicious transactions to the authorities. All employees and relevant personnel must be vigilant and promptly report any suspicions through the proper internal channels.

a. Internal Reporting: If any employee detects or suspects that a transaction, attempted transaction, or any client activity is unusual or potentially indicative of ML/TF, they must immediately report it to their direct manager (or MLRO). This includes situations where:

- A client's behavior or request raises suspicion (e.g., reluctance to provide information, asking staff to bypass normal procedures, or making inconsistent statements about their activities).
- A transaction seems to have no legitimate business purpose, is overly complex or large given the client's profile, or fits a pattern known to be used for money laundering.
- The employee has any reason to suspect that the client or a transaction is linked to criminal activity or a sanctioned party.

The report should include all relevant details (who, what, when, where, and why the activity is suspicious) and any supporting documents or evidence. The identity of the reporting will be kept confidential within the limits of the law. Prompt internal reporting is critical to enable the Company to assess the situation and fulfill its legal duties.

b. Analysis and Decision: Upon receiving an internal suspicious activity report, the manager (or MLRO) will promptly acknowledge receipt and initiate a review. The manager (or MLRO) will gather additional information available to evaluate the suspicion. If the manager (or MLRO) determines that there are reasonable grounds to suspect that the activity is related to ML, TF, or any criminal offense, MLRO will escalate externally by filing a report with FIU Curaçao. This decision will be made without undue delay, in line with Curaçao's reporting requirements. (Under Curaçao law, certain unusual transactions must be reported within a prescribed timeframe once detected). If the manager (or MLRO) decides that the activity, after investigation, does not warrant reporting, this decision will be documented along with the rationale.

c. External Reporting to FIU Curaçao: The MLRO is the designated point of contact to send reports to the FIU. If a decision is made that a transaction or activity should be reported, the

MLRO will file an official Unusual Transaction Report (UTR) (via the channels provided by FIU Curaçao). The report will contain comprehensive details of the client and the transaction(s) in question, and the reasons the activity is considered unusual or suspicious.

d. Tipping-Off Prohibition: It is strictly prohibited for any employee, including the MLRO, to inform the client or any unauthorized person that a suspicious activity report has been or will be made, or that an investigation may be underway. Such disclosure (known as “tipping off”) can compromise investigations and is against the law. Employees should continue business as usual with the client after raising a suspicion, unless instructed otherwise by the MLRO or law enforcement. Any external inquiries (e.g., from law enforcement agencies) received by staff should be referred to the MLRO, to ensure consistent and controlled communication.

e. Post-Reporting Actions: After a report is filed, the MLRO will follow any instructions or guidance from FIU Curaçao or other authorities. In some cases, the FIU may request additional information or ask the Company to monitor the account further. Alternatively, law enforcement might issue an order (such as to freeze assets or provide records). The MLRO will ensure full cooperation with such requests. Separately, even after filing a report, the Company will internally reassess the risk of the client: it may decide to enhance monitoring or even terminate the business relationship if the level of suspicion is high or if instructed by officials.

f. Training and Awareness on Reporting: The Company ensures that all relevant staff are trained on how to recognize signs of ML/TF and the procedure for internal reporting. This includes training on the use of any internal report templates or hotlines.

5.8. Blocking Accounts and Freezing Measures

In circumstances where ML/TF is suspected or confirmed, or when required by law (such as upon identification of a sanctioned person or an official order), Nuxgen will take appropriate action to block or restrict the client’s account and/or freeze relevant transactions to prevent further misuse of its services.

- **Suspension of Services:** If a client is the subject of a serious suspicion or an active investigation for ML/TF, the Company’s MLRO, in consultation with management and legal counsel, may decide to temporarily suspend the provision of any new services to the client. This may involve disabling the client’s access to the platform or products until the issue is resolved. Such a decision might be warranted if continuing to provide services could facilitate further illicit activity or increase the Company’s exposure. Suspension is typically handled discreetly to avoid alerting the client, unless and until formal termination is decided.
- **Blocking / Freezing Transactions:** The Company will comply with any official orders from authorities to freeze assets or block transactions related to a client. Even absent an external order, if a sanctions match is confirmed (i.e., the client or a related party is listed on a sanctions list requiring asset freeze), the Company will not execute any transaction that would contravene those sanctions and will freeze any assets under its control belonging to that sanctioned party (if applicable).
- **Account Closure/Termination:** If, after review, it is concluded that a client has engaged in ML/TF or has otherwise materially breached this Policy or relevant laws, Nuxgen will terminate the business relationship. The Company will ensure that termination (and the reasons for it) is documented. Any funds or assets of the client that

were frozen will only be released with clearance from the authorities or in accordance with law.

- **Documentation:** Any decision to block an account, freeze a transaction, or terminate a relationship for AML reasons will be carefully documented by the MLRO, including the timing, scope of the block, and the rationale (e.g., “account blocked due to confirmed sanctions match on [date]” or “relationship terminated due to MLRO determining unacceptable ML risk”).
- **Legal Compliance:** All blocking and freezing actions are carried out in compliance with Curaçao law and, if applicable, international sanctions obligations. The Company keeps abreast of its legal authority to freeze transactions. Nuxgen incorporates any official lists of designated persons into its screening process to proactively prevent transactions with such parties. By implementing these blocking and freezing measures when appropriate, Nuxgen ensures that it is not complicit in ongoing illegal activity and that it can swiftly isolate and mitigate risks as they are identified.

6. AML Compliance Program

Nuxgen B.V. maintains a comprehensive **AML/CTF Compliance Program** that supports the effective implementation of this Policy. The program is designed to meet the requirements of Curaçao’s AML/CFT regulations and the international standards set by FATF. Key components of the program include:

- **Management Oversight:** The Directors and senior management of Nuxgen are fully committed to AML/CTF compliance. They endorse this Policy, ensure that a culture of compliance is instilled at all levels of the company, and allocate necessary resources for its execution. Senior management regularly provides direction or support for any enhancements needed.
- **Money Laundering Reporting Officer (MLRO):** The Company has appointed an MLRO who is responsible for the day-to-day oversight of the AML program. The MLRO's duties, as outlined in the Definitions and throughout this Policy, include designing internal procedures, receiving and investigating internal reports, reporting to FIU Curaçao, liaising with regulatory bodies, and advising the organization on compliance matters. The MLRO has the authority to access all necessary information within the Company to perform these tasks and is supported by the Compliance Department staff.
- **Employee Training:** A part of the AML program is ongoing **training** for all relevant employees. Nuxgen conducts mandatory AML/CTF training for all new hires upon joining, and refresher training for all staff. The training content is tailored to the roles of employees:
 - All staff receive general awareness training on what money laundering and terrorist financing are, how they can occur in the industry, and the importance of AML compliance to the Company and personal responsibility.
 - Staff in key positions receive detailed instruction on this Policy, how to perform KYC checks, how to spot red flags, and the internal reporting process. Real-world scenarios or case studies are used to illustrate warning signs.
 - The MLRO may attend external workshops or obtain certifications to stay current with regulatory developments and industry best practices, bringing back knowledge to improve internal training.
- **Record Keeping and Data Protection:** As noted, all records related to due diligence, transactions, and internal/external reports are maintained as required by law. The AML

program includes measures to ensure the confidentiality and security of these records. Access to KYC files and STR filing records is restricted to the MLRO and authorized compliance personnel. Digital records are stored in secure systems with access controls and backups. The Company also complies with applicable data protection regulations when handling personal data obtained for AML purposes, ensuring it's used only for lawful compliance uses.

- **Audit and Review:** The AML Compliance Program is subject to review on a periodic basis. This may be conducted by an internal audit function (if available) or by an external employee.
- **Continuous Improvement:** The AML/CTF Program is not static. Nuxgen is committed to continuously improving its controls in light of new risks, technological changes, and evolving regulatory standards.
- **Regulatory Compliance:** The program ensures compliance with specific Curaçao AML laws and any directives from regulators. The Company stays informed of updates from FIU Curaçao or other relevant bodies and integrates these into its internal processes. The MLRO or other employee may also participate in industry forums or consultations to keep current with regulatory expectations.

In summary, Nuxgen's AML Compliance Program provides a structured and proactive approach to managing financial crime risk. It is embedded into the Company's operations, with clear accountability, adequate resources, and regular oversight to ensure that the Company not only meets its legal obligations but also upholds the highest standards of integrity in its business.

7. Compliance and Consequences of Non-Compliance

Compliance with this Policy is mandatory. All employees and associated persons of Nuxgen B.V. must adhere to the procedures and controls set out above. The Company considers AML/CTF compliance to be a collective responsibility and part of the ethical conduct expected in the organization.

- **Individual Responsibility:** Every staff member is responsible for carrying out the specific duties assigned to them under this Policy. Ignorance of the Policy is not an excuse; training and resources are provided to ensure everyone understands their obligations. Employees are encouraged to seek guidance from the MLRO if they are unsure about any aspect of the Policy or its application.
- **Internal Disciplinary Actions:** Failure to comply with the provisions of this Policy or related procedures by any employee will result in disciplinary action. The severity of the action will depend on the nature and gravity of the breach. Minor or unintentional violations may be addressed through additional training and a formal warning. Serious or willful non-compliance – for instance, deliberately circumventing KYC procedures, facilitating a transaction without required approval, or ignoring clear signs of suspicious activity – is considered gross misconduct and may result in immediate termination of contract.
- **Ongoing Compliance Monitoring:** The Company, through the MLRO and management, will monitor adherence to this Policy. Regular audits and quality control checks will be used to detect any non-compliance or areas for improvement. If gaps are found, the Company will take timely corrective action (which may include further training, revising procedures, or disciplinary measures as mentioned).

- **Reporting Misconduct:** If any employee becomes aware of violations of this Policy or other misconduct related to financial crime compliance, they are expected to report this to the MLRO or to senior management. The Company will treat such reports with confidentiality and protect good-faith reporters from retaliation (consistent with any whistleblower policy in place).

8. Related Information

This Policy is part of Nuxgen's wider compliance framework and should be read in conjunction with any other related internal policies or guidelines. The following laws, regulations, and standards are relevant to the content of this Policy:

- **Financial Action Task Force (FATF) Recommendations:** International standards for combating money laundering and terrorist financing which form the basis for national AML/CFT regimes. Nuxgen's Policy and procedures are designed to meet these standards, including requirements for customer due diligence, record-keeping, PEP handling, and suspicious activity reporting, among others.
- **Curaçao National AML/CFT Legislation:** The laws and regulations of Curaçao aimed at preventing and combating money laundering and terrorism financing. This includes legislation on customer identification and verification when establishing business relationships, and the National Ordinance on the Reporting of Unusual Transactions (which mandates the reporting of certain transactions to FIU Curaçao). These laws provide the legal foundation for many of the requirements outlined in this Policy (such as KYC obligations, record retention periods, and the definition of unusual transactions).
- **FIU Curaçao Guidelines and Indicators:** Guidance documents, red flag indicators, and feedback issued by FIU Curaçao or other regulatory authorities. These may include typologies of how money laundering can occur in the gambling/gaming sector, lists of high-risk jurisdictions or persons, and clarifications on how to apply the law. The Company's procedures incorporate this guidance (for example, by using FIU-provided indicators to help identify suspicious activities).
- **International Sanctions Regimes:** The UN Security Council Resolutions on sanctions, as well as European Union and other relevant sanctions regimes. Compliance with these sanctions (such as asset freezes and restrictions on dealing with designated persons or entities) is reflected in the Policy's screening and blocking account sections.
- **Industry Regulations and Licensing Conditions:** If Nuxgen B.V. holds any license or certification, any AML/CTF requirements from those licenses are also considered part of the regulatory context.

9. Contact Information

For any questions, clarifications, or guidance regarding this AML/CTF Policy or any related compliance matter, employees and associated persons should contact:

Email: compliance@nuxgame.com