

Anti-Money Laundering and Countering Financial Crime Manual (AML/CFT)

Sendosa BV

Version 1.0 / March 2025

Document Control

- **Version:** 1.0
- **Effective Date:** March 20, 2025
- **Last Revision:** Initial Version
- **Next Review:** March 20, 2026
- **Approval:** Board of Directors & MLRO

Glossary of Terms

- **AML/CFT:** Anti-Money Laundering and Countering the Financing of Terrorism
- **MLRO:** Money Laundering Reporting Officer
- **B2B:** Business-to-Business
- **CDD:** Customer Due Diligence
- **EDD:** Enhanced Due Diligence
- **FATF:** Financial Action Task Force
- **CGA:** Curaçao Gaming Authority
- **PEP:** Politically Exposed Person
- **SOF:** Source of Funds
- **STR:** Suspicious Transaction Report

1. Purpose of the AML/CFT Manual & Objectives

1.1 Purpose of the AML/CFT Manual

The purpose of this manual is to:

- Deliver guidance and clarity to staff, Directors, and relevant authorities on the obligations Sendosa BV holds as a gaming software distributor, incorporated in Curaçao.
- Provide a high-level overview of the internal policies and procedures implemented to ensure adherence to these obligations.

To ensure Sendosa BV's compliance with these legal requirements, this manual reflects the standards of:

- **Curaçao:** National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (Landsverordening bestrijding witwassen en terrorismefinanciering), overseen by the Curaçao Gaming Authority (CGA).
- **EU:** Directive 2015/849 and Regulation 2015/847, enforcing AML/CFT across member states, as applicable to Curaçao's international obligations.

These manual references internal measures, policies, and procedures designed to meet our licensing and operational duties, ensuring a robust compliance framework.

1.2 Policy Statement and Objectives

It is the firm policy of Sendosa BV that all staff and Directors shall actively engage in efforts to prevent our services from being exploited by criminals or terrorists for money laundering or terrorist financing purposes.

The objectives of this engagement are:

- Ensuring full compliance with all applicable laws, statutory instruments, and requirements set forth by the authorities in Curaçao and the EU.
- Safeguarding Sendosa BV, its staff, and Directors from the risks tied to violations of legal and regulatory standards.
- Minimizing the potential for reputational damage arising from money laundering or terrorist financing by making a meaningful contribution to combating crime.

To achieve these objectives, Sendosa BV's policy requires that:

- Staff and Directors are fully informed of and fulfil their personal obligations as mandated by law or relevant to their roles and responsibilities within the company.
- Commercial interests or decisions shall never override Sendosa BV's dedication to preventing money laundering, terrorist financing, or other financial crimes.
- A Money Laundering Reporting Officer (MLRO) shall be appointed, and all staff are obligated to provide full assistance and cooperation in carrying out the duties associated with this role.
- Sendosa BV shall not knowingly initiate or proceed with establishing a B2B relationship with any entity, corporation, or business suspected of engaging in nefarious activities or unethical practices.

- Sendosa BV shall not knowingly accept payments or funds from a B2B relationship with an entity, corporation, or business suspected of engaging in such activities or practices.

2. Background to Money Laundering and Terrorist Financing

Sendosa BV is dedicated to preventing and deterring the misuse of its B2B gaming software distribution services by criminals and terrorists. Curaçao and the European Union uphold international standards to combat money laundering and terrorist financing, and Sendosa BV has established policies and procedures to identify and address potential abuse of our platform.

2.1 What is Money Laundering?

Money laundering refers to any process or activity used to disguise the origins of property or funds derived from criminal activities, making them appear to come from a lawful source. It occurs in any situation where illicit proceeds are involved. The primary aims of a money launderer are:

- To conceal the criminal source of their proceeds.
- To maintain control over these funds while masking their ownership.
- To avoid detection by law enforcement or regulatory bodies.
- To ultimately benefit from the illicit gains.

The money laundering process is commonly understood to consist of three distinct stages:

- **2.1.1 Placement:** This initial stage involves introducing proceeds of crime into the financial system. For Sendosa BV, as a B2B gaming software distributor, placement could occur if unscrupulous gaming operators use illicitly obtained funds to pay for our software licenses, inadvertently drawing us into the laundering process as these funds enter legitimate financial channels.
- **2.1.2 Layering:** At this stage, the criminal proceeds are distanced from their initial entry point through a series of transactions designed to obscure their trail and lend an appearance of legitimacy. In our context, layering might involve multiple B2B clients with little or no established trading history contracting with Sendosa BV, or operators reporting unusually high player activity shortly after onboarding, creating layers to confuse any investigation.
- **2.1.3 Integration:** The final stage sees the laundered funds reintroduced into the legitimate economy, appearing as lawful earnings. For Sendosa BV, this could manifest as payments for software services that seem routine but originate from earlier laundering efforts. Points of vulnerability, such as cross-border payments or asset purchases, may offer opportunities for authorities to detect such activities.

It's worth noting that money laundering doesn't always follow a clear three-stage sequence; stages may overlap, and the process can involve various forms of property beyond cash. Due to the high-value nature of contracts in the gaming software industry, Sendosa BV must maintain constant vigilance throughout each B2B relationship to detect and prevent such misuse.

2.2 What is Terrorist Financing?

The United Nations Convention for the Suppression of the Financing of Terrorism describes terrorism as actions intended "to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act." It forbids anyone from directly or indirectly

handling or providing funds with the intent or knowledge that they will support terrorist acts or groups.

- **2.2.1 Terrorism Factors:** Terrorist activities typically involve:
 - Threats or acts designed to influence governments or intimidate the public, often for political, religious, or ideological purposes.
 - Actions that cause serious violence, significant property damage, or endanger lives to further these goals.
 - Criminal enterprises that generate steady income for terrorist organizations.
- **2.2.2 Financial Support of Terrorism:** Funding for terrorism generally arises from two key sources:
 - “State-sponsored terrorism,” where nations, organizations, or wealthy individuals provide resources to terrorist causes, though this has decreased due to international pressure.
 - Revenue-generating activities, both legal and illegal, conducted by terrorist groups, often targeting high-profit ventures to sustain their operations.

Sendosa BV staff and Directors must exercise heightened caution when engaging with new B2B clients located in jurisdictions known to have connections to terrorist organizations, as outlined in Appendix 2.

2.3 Proliferation Financing

- **2.3.1 What is Proliferation?:** Following UN Security Council Resolution 1540, proliferation is defined as “the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of chemical, biological, radiological, or nuclear (CBRN) weapons (weapons of mass destruction or WMD) and their delivery systems or related materials (including technologies and dual-use goods), in violation of national laws or international commitments.” This can range from advanced missile systems to rudimentary devices like “dirty bombs.”
- **2.3.2 Dual-Use Goods:** These are items with legitimate applications that can also be repurposed for proliferation activities, such as WMD development. In Sendosa BV’s case, our gaming software could theoretically fall into this category if misused, despite its primary lawful purpose. Such goods may not appear on control lists, requiring careful evaluation during client assessments. Without proper controls, these materials could end up in the hands of unauthorized parties, profiteers, or terrorists, posing a global security threat.
- **2.3.3 Proliferation Financing:** The Financial Action Task Force (FATF) defines proliferation financing as “the act of providing funds or financial services used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including technologies and dual-use goods for non-legitimate purposes), in contravention of national laws or international obligations.” This can include:
 - Financing terrorism, where funds support groups seeking WMD.

- State-backed efforts to develop or enhance WMD capabilities.

Proliferation financing often mimics legitimate transactions to access foreign currency or the global financial system, making it critical to scrutinize payment chains. Even unintentional involvement risks severe reputational harm, underscoring the need for robust preventive measures.

2.4 Sanctions

Sanctions are punitive actions imposed on countries, individuals, entities, or organizations to maintain or restore international peace and security. These may target specific sectors, industries, or persons and are guided by lists from the United Nations (UN), European Union (EU), and the U.S. Office of Foreign Assets Control (OFAC). Curaçao adheres to international sanctions, and Sendosa BV voluntarily complies with OFAC measures, including:

- Prohibiting business with individuals or entities from OFAC-sanctioned jurisdictions such as Iran, North Korea, and Myanmar (see Appendix 2).
- Monitoring OFAC's "Specially Designated Nationals and Blocked Persons List," "Sectoral Sanctions Identifications List," and other programs like "Counter Terrorism" and "Non-Proliferation."

Sanctions may involve:

- Freezing assets and barring resource provision to designated parties.
- Economic restrictions on specific businesses or sectors.
- Controls on dual-use goods, arms embargoes, and import/export bans.
- Travel or visa restrictions for targeted individuals.

If a B2B client or its Ultimate Beneficial Owner (UBO)/Directors is identified as a sanctioned entity or individual (per Appendix 2), staff must immediately compile a full client profile, halt all transactions, and notify the MLRO, who will escalate to the relevant authorities. Sendosa BV maintains a PEP and Sanctions Register to record such cases.

3. Legal and Regulatory Compliance Framework

This section details the legislative and regulatory requirements that Sendosa BV must adhere to as a gaming software distributor, incorporated in Curaçao with registration number 166829. It provides an overview of the laws governing anti-money laundering (AML), countering the financing of terrorism (CFT), and related obligations under Curaçao and European Union (EU) jurisdictions, as applicable. While not exhaustive, this section equips staff and Directors with essential knowledge of the legal landscape, their personal responsibilities, and the consequences of non-compliance. For a full understanding, staff are encouraged to consult the referenced legislation directly or seek clarification from the MLRO.

3.1 Curaçao AML/CFT Legislation

Curaçao's primary legal tool for combating money laundering and terrorist financing is the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (Landsverordening bestrijding witwassen en terrorismefinanciering). It aligns with international standards and applies to Sendosa BV as a Curaçao-registered entity. Key offenses under this legislation include:

- Concealing, transferring, or disguising the proceeds of criminal activities to obscure their illicit origins.
- Aiding another individual or entity in retaining or benefiting from criminal proceeds.
- Acquiring, possessing, or using property known or suspected to be derived from crime.

Penalties:

- Conviction for these offenses can lead to imprisonment for up to 7 years.
- Failing to disclose knowledge or suspicion of money laundering to the MLRO or authorities carries a penalty of up to 4 years in custody.
- Tipping off—revealing information likely to prejudice an investigation—may result in up to 2 years imprisonment.

It is a legal duty for all staff and Directors to report any suspicion or knowledge of money laundering encountered during their work to the MLRO immediately. Criminal conduct includes acts that would be offenses under Curaçao law or, if committed abroad, would constitute crimes if they occurred in Curaçao.

3.2 Curaçao Gaming and AML Legislation

The Curaçao gaming regulations, overseen by the Curaçao Gaming Authority (CGA), mandate AML/CFT compliance for gaming software distributors, requiring robust measures to prevent the misuse of our services. Offenses include:

- Facilitating transactions involving proceeds of crime through gaming-related activities.
- Failing to implement required due diligence or reporting procedures.

Penalties:

- Non-compliance can result in fines, suspension, or revocation of our license, effectively halting operations.
- Criminal involvement in money laundering or terrorist financing may lead to imprisonment under Curaçao penal law, with terms up to 7 years depending on severity.

3.3 EU Directives and Regulations

Sendosa BV operates within the EU framework, where applicable, adhering to:

- **Directive 2015/849 (4th AML Directive):** Establishes a risk-based approach to prevent money laundering and terrorist financing, requiring customer due diligence, record-keeping, and suspicious activity reporting. Non-compliance risks fines or sanctions from relevant authorities.
- **Regulation 2015/847:** Mandates transparency in fund transfers, ensuring traceability of payments linked to our B2B contracts. Violations can lead to penalties imposed by regulators.

These EU laws reinforce our obligations in Curaçao's international compliance framework.

3.4 Terrorist Financing Laws

Terrorist financing is addressed under Curaçao legislation, drawing from the UN Convention for the Suppression of the Financing of Terrorism and, where applicable, EU Directive 2015/849. Offenses include:

- Providing, collecting, or making available funds with intent or knowledge that they will support terrorist acts or organizations.
- Concealing or transferring property known to be linked to terrorism.
- Arranging financial resources suspected to be used for terrorist purposes.

Penalties:

- Conviction carries imprisonment of up to 7 years in Curaçao.
- Failure to report suspicion or knowledge of terrorist financing to the MLRO or authorities is an offense, punishable by up to 4 years in custody.

Staff must escalate any such concerns arising from B2B client activities to the MLRO without delay.

3.5 Sanctions Compliance Obligations

Sendosa BV complies with sanctions imposed by the UN and voluntarily adheres to U.S. OFAC measures, as well as EU sanctions where applicable. These include:

- Prohibitions on dealings with sanctioned individuals, entities, or jurisdictions (e.g., Iran, DPRK).
- Restrictions on financial services or goods transfers that could breach sanctions.

Penalties:

- Breaching sanctions can result in fines, asset freezes, or operational bans, enforced by authorities.
- Non-compliance with OFAC (though voluntary) risks reputational damage and exclusion from U.S.-linked financial systems.

3.6 Staff Responsibilities and Consequences

Every staff member and Director has a personal legal obligation to:

- Understand and comply with the AML/CFT requirements outlined in this manual.
- Report any suspicion or knowledge of money laundering, terrorist financing, or sanctions breaches to the MLRO immediately, using the process in Section 7.
- Avoid actions that could constitute tipping off, such as alerting a client to an investigation.

Failure to meet these duties is a criminal offense, exposing individuals to imprisonment or fines, separate from company-level penalties. Staff with questions about their responsibilities should consult the MLRO for guidance.

3.7 Additional Regulatory Guidance

The FATF Recommendations (2012), incorporated into Curaçao laws, provide international standards that Sendosa BV follows, such as risk-based customer due diligence and enhanced measures for high-

risk scenarios. Compliance with these standards is monitored by the authorities, ensuring our policies align with global best practices.

4. Customer Due Diligence and Risk Assessment

Sendosa BV, as an ethical and responsible B2B gaming software distributor, implements a comprehensive risk-based approach (RBA) to assess and monitor our business clients. This ensures we identify and mitigate risks of money laundering (ML), terrorist financing (TF), proliferation financing (PF), and other financial crimes associated with our services offered. This section outlines the criteria, processes, and controls we apply to safeguard our operations under Curaçao and EU legislation.

4.1 Risk Assessment Criteria

We evaluate B2B clients based on multiple factors to determine their risk level, ensuring a proactive stance against financial crime:

- **Payment Behavior:** Frequent or irregular payment requests deviating from agreed terms may suggest layering attempts. Consistent, predictable payments align with lower risk.
- **Geographic Location:** Clients in high-risk jurisdictions (Appendix A) with weak AML/CFT controls or known links to crime/terrorism elevate risk. Clients in low-risk, FATF-compliant jurisdictions are generally safer, though not exempt from scrutiny.
- **Source of Funds (SOF):** Funds from unclear origins, non-FATF countries, or high-risk jurisdictions (Appendix A) increase suspicion. Verified, legitimate SOF reduces risk.
- **Client Profile and Ownership:** The presence of Politically Exposed Persons (PEPs), sanctioned individuals, or entities with adverse media in the ownership structure heightens risk. Transparent, reputable businesses pose lower risk.

Risk Categories:

- **Standard Risk:** Clients from standard-risk jurisdictions, with clear SOF and stable operations.
- **High Risk:** Clients with PEPs, high-risk jurisdiction ties, or suspicious patterns, triggering enhanced due diligence (EDD).

4.2 Initial Client Onboarding Process

Before establishing a B2B relationship, Sendosa BV conducts thorough due diligence:

- **Documentation:** Clients provide company registration details, beneficial owner (UBO) identification, and initial SOF evidence.
- **Screening:** The Compliance Unit screens UBOs and Directors against PEP and sanctions lists using appropriate tools. Positive hits are escalated to the MLRO for review.
- **Blacklist Check:** Clients are cross-referenced against an internal blacklist of terminated or suspicious entities maintained by the MLRO.
- **Approval:** Contracts are finalized only after clearance by the Compliance Unit, with high-risk cases requiring MLRO sign-off.

4.3 Enhanced Due Diligence (EDD) for High-Risk Clients

EDD is mandatory for clients identified as high-risk, ensuring deeper scrutiny:

- **Triggers:**
 - Location in high-risk jurisdictions (Appendix A).
 - UBOs or Directors identified as PEPs or sanctioned persons.
 - SOF unverifiable or linked to high-risk sources.
- **Requirements:**
 - Certified copies of UBO identification.
 - Recent proof of address.
 - Detailed SOF documentation.
- **Process:** The Compliance Unit compiles a risk dossier, reviewed by the MLRO. Services are paused until EDD is completed and approved.

4.4 Ongoing Monitoring and Review

Sendosa BV maintains continuous oversight of B2B relationships:

- **Annual Assessment:** The Data Analytics Team compares actual payment volumes and reported player activity against onboarding projections, flagging deviations.
- **Automated Tools:** Software monitors transaction frequency and volume, alerting the Compliance Unit to anomalies.
- **Manual Review:** The Compliance Unit investigates flagged cases, requesting client explanations. Unresolved issues escalate to the MLRO for potential EDD or termination.
- **Frequency:** High-risk clients are reviewed semi-annually; standard-risk clients annually.

4.5 Contractual Obligations and Restrictions

Our B2B contracts enforce AML/CFT compliance:

- Clients must warrant that software use complies with local gaming laws and restricts play to individuals aged 18 or older.
- Non-compliance triggers immediate suspension of services, pending investigation by the Compliance Unit.
- Periodic audits verify adherence, conducted by the Operational Staff under MLRO oversight.

4.6 Source of Funds Verification

For contracts flagged as high-risk:

- **Evidence:** Clients submit financial statements, bank records, or ownership documents proving legitimate funding.
- **Validation:** The Compliance Unit cross-checks against independent sources.
- **Escalation:** Unverifiable SOF halts service provision until resolved, with the MLRO deciding on termination if suspicion persists.

4.7 Internal Record Management

- **Updates:** Changes to client details are logged and reviewed by the MLRO within 48 hours.
- **Storage:** All due diligence records are encrypted and stored for 10 years post-relationship, accessible only to authorized personnel.
- **Blacklist:** Terminated high-risk clients are added to an internal blacklist, maintained securely by the MLRO.

5. Technology and Innovation Risk Management

Sendosa BV recognizes that the introduction of new products, business practices, or technologies in our B2B gaming software distribution could create vulnerabilities exploitable by money launderers, terrorist financiers, or proliferators. This section outlines our robust procedures for assessing and managing these risks to ensure compliance with Curaçao and EU legislation, protecting our platform from misuse while fostering innovation responsibly.

5.1 Pre-Launch Risk Assessment

Before deploying any new software, service, or technological enhancement, Sendosa BV conducts a thorough AML/CFT risk assessment:

- **Responsibility:** The Data Analytics Team, under MLRO oversight, leads the evaluation, collaborating with Operational Staff to analyze technical specifications.
- **Scope:** The assessment examines potential weaknesses that could facilitate financial crime.
- **Methodology:** Risks are rated (low, medium, high) based on likelihood and impact, using historical data, industry benchmarks, and FATF guidance on technology-related ML/TF risks.
- **Documentation:** A detailed risk report is compiled, identifying vulnerabilities and potential exploitation scenarios, submitted to the MLRO.

5.2 Risk Mitigation Strategies

Upon identifying risks, Sendosa BV implements tailored controls to address them before launch:

- **Testing:** Proposed controls are stress-tested in a sandbox environment, simulating ML/TF scenarios to confirm effectiveness.
- **Timeline:** Mitigation plans are finalized with progress tracked via a project log maintained by the Data Analytics Team.

5.3 Implementation and Approval

Once risks are mitigated, the new technology or product moves to implementation:

- **Rollout:** Operational Staff deploy the technology, with initial use monitored to detect unforeseen issues.
- **Training:** Staff receive targeted training on the new system's AML/CFT features, delivered by the MLRO prior to launch.

5.4 Post-Launch Monitoring

After deployment, Sendosa BV ensures ongoing vigilance:

- **Regular Audits:** The Compliance Unit conducts quarterly reviews of the technology's performance, assessing metrics like false positive rates in monitoring systems or security incidents.
- **Feedback Loop:** Operational Staff report anomalies to the Data Analytics Team, triggering a re-assessment if needed.
- **Updates:** Software patches or procedural adjustments are implemented, with MLRO oversight.

6. Record Retention and Management

Sendosa BV maintains meticulous records of all B2B client interactions, transactions, and due diligence activities to comply with legislative requirements. This section outlines our policies and procedures for retaining, retrieving, and securing these records, ensuring they are available to support internal audits, regulatory inquiries, and investigations.

6.1 Retention Obligations

- **Duration:** All records related to client relationships and transactions are retained for a minimum period post-relationship or final transaction. This includes client identification documents, source of funds evidence, payment records, and risk assessments.
- **Scope:** Retention applies to both active and terminated B2B relationships, covering onboarding data, ongoing monitoring logs, and correspondence with clients or authorities.

6.2 Storage Protocols

- **Formats:** Records are maintained in both electronic and hard copy formats to ensure redundancy and accessibility.
- **Security:** Electronic records are stored on encrypted servers with industry-standard protocols.
- **Backup:** Regular backups of electronic records are performed.

7. Suspicious Activity Reporting and Internal Controls

Sendosa BV maintains a robust internal reporting system to detect and address potential money laundering (ML), terrorist financing (TF), or proliferation financing (PF) risks arising from our B2B gaming software distribution activities. This section outlines the procedures for staff to recognize suspicious transactions, report them to the Money Laundering Reporting Officer (MLRO), and ensure compliance with Curaçao and EU legislation, protecting our operations and supporting efforts to combat financial crime.

7.1 Money Laundering Reporting Officer (MLRO)

- **Designation:** Sendosa BV appoints an MLRO to oversee AML/CFT compliance. The current MLRO is Philip Bugeja.
- **Contact Details:**
 - **Address:** Zuikertuintjeweg Z/N, Curaçao
 - **Email:** philip@igagroup.com

- **Responsibilities:**

- Receive and assess internal reports of suspicious activity from staff.
- Investigate reported suspicions and determine if external reporting to authorities is required.
- Maintain oversight of day-to-day client account activities and high-risk cases identified by senior management.
- Ensure access to all necessary systems, files, and documents to evaluate reports thoroughly.

The MLRO is supported by all staff, who are required to cooperate fully in fulfilling these duties.

7.2 Recognizing Suspicious Activities

Staff are trained to identify unusual or suspicious activities during B2B client interactions, such as:

- Revenue patterns inconsistent with onboarding projections.
- Source of funds that cannot be readily verified or appears unnecessarily complex.
- Client behavior indicating excessive secrecy or intent to conceal transactions from authorities.
- Difficulty in explaining business operations or lack of industry knowledge.
- Funds linked to jurisdictions with elevated ML/TF risks (Appendix A).

Staff must remain vigilant, documenting any concerns and following the reporting process below.

7.3 Internal Reporting Process

- **Obligation:** All staff must report suspicions of ML, TF, or PF to the MLRO promptly, using the Internal Suspicion Report Form (Appendix B). Failure to report knowledge or suspicion encountered in the course of duties is a criminal offense under Curaçao law.
- **Submission:**
 - Complete the Internal Suspicion Report Form with a detailed description of the suspicion and supporting evidence.
 - Submit to the MLRO via secure email or in-person delivery within 24 hours of identification.
- **Content:** Reports must be clear, legible, and comprehensive, enabling the MLRO to assess potential breaches of AML/CFT legislation.
- **Tipping Off Prohibition:** Staff must not disclose suspicions to clients or third parties, as this could prejudice investigations and is an offense punishable by imprisonment.
- **Clarification:** The MLRO may direct staff to seek additional client information to resolve suspicions, ensuring requests are discreet to avoid tipping off, with findings forwarded for further evaluation.

7.4 MLRO Review and Decision-Making

- **Receipt:** The MLRO acknowledges report submissions within 24 hours, logging them in the Internal Suspicion Register.
- **Investigation:** The MLRO reviews the report, accessing client records, payment data, and due diligence files to validate the suspicion, completing the assessment within 5 business days.
- **Outcome:**
 - If suspicion is unfounded, the MLRO documents the rationale and closes the case, informing the reporting staff.
 - If suspicion persists, the MLRO prepares an external report for the authorities, as detailed below.
- **Record-Keeping:** All decisions and supporting documents are archived securely, with outcomes noted in the Internal Suspicion Register.

7.5 Management of Registers

- **Internal Suspicion Register:**
 - Tracks all internal reports, including submission date, staff name, client details, MLRO decision, and closure date.
 - Reviewed monthly by the MLRO to identify trends or recurring issues.
- **External Disclosure Register:**
 - Logs STRs filed with authorities, noting submission date, reference numbers, and acknowledgment from the authorities.
 - Kept secure and separate, with access restricted to the MLRO.
- **External Enquiries Register:**
 - Records inquiries from authorities or law enforcement, detailing date, inquiring officer, legal basis, and information provided.
 - Maintained indefinitely, with destruction only upon regulatory approval.

7.6 Staff Accountability and Legal Consequences

- **Duty:** Staff must understand their legal obligation to report suspicions, as failure to do so risks personal penalties, including imprisonment under Curaçao law.
- **Support:** The MLRO provides guidance on reporting procedures, ensuring staff can fulfill their responsibilities confidently.
- **Confidentiality:** All reporting is handled discreetly, protecting staff from reprisal while maintaining investigation integrity.

8. Staff Recruitment, Training, and Compliance Oversight

Sendosa BV recognizes that our staff and Directors are critical to maintaining a robust AML/CFT framework for our B2B gaming software distribution operations. This section outlines our comprehensive policies for screening, training, and overseeing personnel to ensure they possess the

expertise, integrity, and awareness needed to prevent financial crime, aligning with legislative requirements.

8.1 Staff Recruitment and Screening

- **Objective:** To ensure all employees uphold the highest standards of honesty and trustworthiness, reducing the risk of internal fraud or criminal facilitation.
- **Process:**
 - Background checks are conducted for all prospective staff, verifying identity, employment history, and any criminal records.
 - References from previous employers are required and authenticated by the Human Resources (HR) Unit to confirm reliability.
 - Senior staff and key roles undergo enhanced screening.
- **Documentation:** Screening results are recorded in secure personnel files, accessible only to HR and the MLRO, retained throughout employment and for a period post-termination as required by law.
- **Outcome:** Candidates failing to meet integrity standards are excluded from employment, with decisions logged for audit purposes.

8.2 AML/CFT Training Program

- **Purpose:** To equip staff with the knowledge and skills to recognize and report suspicious activities, ensuring compliance with AML/CFT obligations.
- **Frequency:**
 - All staff receive initial training upon onboarding, followed by annual refresher sessions.
 - Additional training is provided as needed following updates to laws, policies, or technology deployments.
- **Content:**
 - Understanding of ML, TF, and PF risks specific to gaming software distribution.
 - Responsibilities under this manual and potential legal consequences of non-compliance.
- **Delivery:**
 - Sessions are led by the MLRO, conducted in-person or via secure virtual platforms for remote staff.
 - Materials, including this manual, are distributed electronically, with staff required to acknowledge receipt and understanding in writing.
- **Assessment:** Periodic quizzes or evaluations are administered to verify comprehension.

8.3 Ongoing Compliance Monitoring

- **Responsibility:** The HR Unit, in coordination with the MLRO, oversees staff adherence to AML/CFT policies.
- **Tracking:**
 - Training completion is recorded in a secure register, reviewed quarterly by the MLRO to ensure full participation.
 - Staff performance in reporting suspicious activities is monitored and feedback provided by the MLRO.
- **Audits:** The Compliance Unit conducts semi-annual reviews of staff compliance, assessing adherence to screening, training, and reporting protocols, with findings reported to the Board of Directors.
- **Updates:** Changes to AML/CFT laws or internal procedures are communicated to staff within a set timeframe, with retraining scheduled as necessary.

8.4 Support and Guidance

- **Resources:** Staff have access to the MLRO for clarification on AML/CFT duties, with responses provided within a reasonable period to ensure operational continuity.
- **Escalation:** Complex issues or uncertainties are escalated to senior management or external legal advisors, with resolutions documented and shared to enhance staff understanding.
- **Continuous Improvement:** Feedback from training sessions and compliance reviews is used to refine programs, ensuring staff remain well-equipped to meet evolving risks.

9. Supporting Appendices

This section provides essential reference materials to support Sendosa BV's AML/CFT policies and procedures for our B2B gaming software distribution. These appendices assist staff and Directors in understanding risk classifications, key definitions, and internal documentation requirements, ensuring compliance with Curaçao and EU legislation.

9.1 Appendix 1 - Acceptable Jurisdictions

- **Purpose:** Identifies jurisdictions deemed low or medium risk for business dealings, based on their adherence to international AML/CFT standards.
- **Criteria:** Jurisdictions must have robust legal frameworks equivalent to those in Curaçao, with no significant ML/TF risks identified by global bodies like the FATF.
- **List:**

Risk Level	Countries
Low Risk	Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Norway, Poland, Romania, Slovakia, Slovenia, Sweden, Japan, New Zealand, Singapore, Switzerland
Medium Risk	Bulgaria, Croatia

- **Updates:** Reviewed quarterly by the MLRO to reflect changes in global risk assessments, with revisions approved by the Board.

9.2 Appendix 2 - Unacceptable and High-Risk Jurisdictions

- **Purpose:** Identifies jurisdictions where business dealings are restricted or require enhanced scrutiny due to elevated ML/TF/PF risks.
- **Criteria:** Based on FATF designations (February 2025 update), including jurisdictions under increased monitoring or subject to countermeasures for deficient AML/CFT controls.
- **Classifications and List:**

Risk Level	Countries
Medium Risk	Algeria, Angola, Burkina Faso, Cameroon, Côte d'Ivoire, Democratic Republic of the Congo, Haiti, Kenya, Lao PDR, Lebanon, Mali, Monaco, Mozambique, Namibia, Nepal, Nigeria, South Africa, South Sudan, Syria, Tanzania, Venezuela, Vietnam, Yemen
High Risk	Democratic People's Republic of Korea, Iran, Myanmar

- **Application:** High-risk jurisdictions trigger mandatory EDD; business with unacceptable jurisdictions is prohibited unless approved by the MLRO and Board under exceptional circumstances.
- **Maintenance:** Updated quarterly by the MLRO, aligned with FATF statements and EU/OFAC sanctions lists.

9.3 Appendix 3 - Politically Exposed Persons (PEPs) and High-Risk Customers (HRCs)

- **Definitions:**
 - **PEPs:** Individuals holding prominent public positions, their immediate family members, or close associates. Includes heads of state, government ministers, senior judicial or military officials, and executives of state-owned entities.
 - **HRCs:** Customers (or their beneficial owners) posing elevated ML/TF risks due to factors like jurisdictional ties, adverse media, or complex ownership structures, even if not PEPs.
- **Identification:** PEPs and HRCs are flagged during onboarding and ongoing monitoring via screening tools and internal risk assessments.
- **Handling:** Both categories require EDD, with records maintained in a dedicated register by the MLRO for review and audit purposes.

9.4 Appendix 4 - Internal Suspicion Report Form

- **Purpose:** Standardizes the reporting of suspicious activities identified by staff.
- **Template:**
 - **Date Submitted:**
 - **Staff Name:**
 - **Client Name:**
 - **Suspicion Details:**
 - **Evidence:**
- **Use:** Completed by staff upon identifying suspicious activity, submitted to the MLRO for review and action.
- **Retention:** Stored securely with client records, per Section 6 requirements.