

## AML POLICY - Curaçao

**Version:** 1.0 **Date:** 19 May 2025

### Key Information

- **Approving Official(s):** Vivian Victoria Ersilia
- **Responsible Office:** Compliance Department
- **Effective Date:** 19 May 2025
- **Next Review Date:** 19 May 2026

### 1. Policy Statement

**Starlink International N.V.** is firmly committed to ensuring that its products, services, and operations are not used, either directly or indirectly, for the purposes of **Money laundering (ML)**, **Terrorist Financing (TF)**, or the **Financing of Proliferation (FP)** of weapons of mass destruction.

As part of this commitment, **Starlink International N.V.** operates exclusively for individual (natural person) customers. The use of its platform by legal entities, business accounts, or individuals acting on behalf of third parties is strictly prohibited. All customers must confirm that they are acting solely in their personal capacity and not on behalf of any organization or other person.

- 1) To uphold this commitment, **Starlink International N.V.** fully complies with all applicable **Anti-Money Laundering (AML)** and **Countering the Financing of Terrorism (CFT)** laws and regulations in Curaçao, including but not limited to:
  - The **National Ordinance on Identification when Rendering Services (NOIS)**
  - The **National Ordinance on the Reporting of Unusual Transactions (NORUT)**
  - The **Sanctions National Ordinance**
  - The **Kingdom Sanction Act**
  - All applicable guidance and regulations issued by the **Curaçao Gaming Control Board (GCB)**
  - **Financial Action Task Force (FATF)** Recommendations
2. This AML/CFT Policy establishes a robust internal framework, governance structure, operational procedures, and control mechanisms designed to:

- Identify, assess, and mitigate money laundering, terrorist financing, and proliferation financing (ML/TF/FP) risks;
  - Detect, investigate, and report suspicious or unusual transactions in accordance with legal obligations;
  - Maintain continuous alignment with both local and international AML/CFT standards;
  - Embed a culture of compliance, integrity, and risk awareness at all organizational levels;
  - Ensure that all customer relationships involve **only natural persons acting on their own behalf**, with strict prohibition of business entities, intermediaries, or third-party representation.
- 2) This policy applies to all directors, officers, employees, and relevant third-party service providers engaged in the activities of **Starlink International N.V.**. All individual covered by this policy is expected to understand and comply with its provisions and to actively contribute to the effectiveness of the company's AML/CFT program.

## 2. Purpose

The purpose of this policy is to:

- 1) **Establish a comprehensive, risk-based Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) compliance program** in full alignment with the legal and regulatory requirements of Curaçao, including all relevant obligations under national and international standards.
- 2) **Prevent the misuse of Starlink International N.V.'s online gambling platform for money laundering, terrorist financing, or other illicit financial activity**, by ensuring all customers are subject to appropriate due diligence, transaction monitoring, and risk assessments.
- 3) **Define clear roles, responsibilities, and procedures for AML/CFT compliance** across all levels of the organization, ensuring consistent implementation of controls and effective internal oversight.
- 4) **Facilitate the timely identification, escalation, and reporting of suspicious or unusual activities** to the Financial Intelligence Unit (FIU) Curaçao in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT) and other applicable regulations.
- 5) **Promote a strong, organization-wide culture of integrity, transparency, and regulatory compliance**, supported by employee training, management accountability, and ongoing monitoring of AML/CFT risks.

- 6) **Reinforce that the platform is accessible solely to individual (natural person) customers**, with a strict prohibition on the registration or use of services by corporate entities, organizations, or individuals acting on behalf of others.

### 3. Definitions

For the purposes of this policy, the terms below are defined in accordance with applicable Curaçao legislation and regulatory guidance issued by the Curaçao Gaming Control Board (GCB):

- I. **Customer Due Diligence (CDD):** The process of verifying the identity of a natural person customer, understanding the nature and intended purpose of the relationship, and performing ongoing monitoring to ensure the customer's activities align with their risk profile. CDD under this policy is strictly applied to individuals acting in their personal capacity.
- II. **Enhanced Due Diligence (EDD):** Additional, more rigorous due diligence measures required for higher-risk individual customers or situations. These include customers from high-risk jurisdictions, those displaying unusual or complex financial behaviour. EDD includes verification of the individual's background, source of funds and wealth, and heightened monitoring of transactions.
- III. **Financing of Proliferation (FP):** The provision or facilitation of financial resources, whether directly or indirectly, for the development, acquisition, transportation, stockpiling, or use of nuclear, chemical, or biological weapons and their delivery systems.
- IV. **Financial Intelligence Unit (FIU) Curaçao:** The designated national authority in Curaçao responsible for receiving, analyzing, and disseminating financial disclosures related to suspected proceeds of crime or potential TF/ML activity. All suspicious transaction reports (STRs) are submitted to the FIU via the goAML platform.
- V. **Money Laundering (ML):** The act of concealing the illicit origin of criminal proceeds by integrating them into the legitimate financial system. This includes the conversion, transfer, concealment, acquisition, or use of property derived from criminal activity.
- VI. **Politically Exposed Person (PEP):** A natural person who currently holds, or has previously held, a prominent public function domestically, internationally, or within an international organization (e.g., heads of state, senior politicians, military officials). This definition includes the person's immediate family and close associates. PEPs are not permitted to register on the platform.
- VII. **Risk-Based Approach (RBA):** A strategic methodology that ensures AML/CFT controls are proportional to the risks identified. The company allocates resources and applies controls based on individual customer risk profiles, transaction patterns, delivery channels, and jurisdictional exposure.

- VIII. **Simplified Due Diligence (SDD):** A reduced level of due diligence permitted only in well-justified low-risk scenarios, as determined through the BRA and CRA. The application of SDD must comply with GCB guidance and be properly documented.
- IX. **Source of Funds:** The specific origin of funds used in a transaction or for account activity (e.g., wages, gaming winnings, sale of assets).
- X. **Source of Wealth:** The broader origin of a customer's total wealth and financial standing (e.g., accumulated wealth through investments or inheritance).
- XI. **Suspicious Transaction/Activity:** Any transaction or behavior that raises reasonable grounds for suspicion of involvement in ML, TF, FP, or other criminal activity. Indicators may include anomalies from typical customer behavior, transaction irregularities, or links to high-risk jurisdictions or persons.
- XII. **Targeted Financial Sanctions (TFS):** Restrictive measures (e.g., asset freezes, service bans) imposed on designated individuals under UN Security Council Resolutions, EU lists, or Curaçaoan law. All customers are screened against applicable sanctions lists during onboarding and at regular intervals.
- XIII. **Terrorist Financing (TF):** The act of providing, collecting, or using funds whether legally or illegally obtained with the intent or knowledge that they will be used, in whole or in part, to carry out terrorist acts.

#### 4. Audience

- 1) This policy applies to all individuals involved in the operations of **Starlink International N.V.**, regardless of their employment status, contractual arrangement, or geographic location. It defines the responsibilities of all personnel in maintaining the integrity of the company's AML/CFT framework and ensuring that services are provided exclusively to individual (natural person) customers. The policy applies to, but is not limited to:
- **Employees** at all levels, including full-time, part-time, temporary, and contract staff.
  - **Senior management**, including directors, executives and officers.
  - **Compliance personnel**, including the appointed Compliance Officer and designated AML/CFT team members.
  - **Customer-facing staff**, such as support agents, account managers, and onboarding specialists.
  - **Risk management and operations teams** responsible for transaction monitoring, due diligence, or customer risk assessments.

- **Relevant third-party service providers**, including outsourced compliance support, KYC/AML vendors, and affiliates involved in customer acquisition or transaction processing.
- 2) This policy is particularly critical for individuals or teams involved in any of the following activities:
- Direct or indirect interaction with **individual customers**.
  - Processing or reviewing **customer transactions and withdrawal requests**.
  - Performing **Customer Due Diligence (CDD)** and **Enhanced Due Diligence (EDD)** in accordance with regulatory obligations.
  - Identifying, escalating, and reporting **unusual or suspicious activity** to the Compliance Officer or FIU Curaçao.
  - Designing, implementing, or maintaining **AML/CFT controls, systems, and procedures**.
- 3) All employees and relevant third parties must understand that **Starlink International N.V.** operates strictly on a **natural person-only basis**. The onboarding or servicing of business accounts, legal entities, or individuals acting on behalf of third parties is explicitly prohibited. Any attempt to circumvent this restriction must be reported immediately for escalation.

## 5. Policy Implementation

- 1) A comprehensive **Risk-Based Approach (RBA)** is adopted to address Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), and the Financing of Proliferation (FP), in alignment with international standards and the legal and regulatory framework of Curaçao.
- 2) The RBA ensures that AML/CFT/FP measures are proportionate to the level and nature of the risks identified, allowing resources to be allocated efficiently and effectively. It emphasizes the importance of understanding and continuously evaluating the specific risks faced in the context of business operations, customer profiles, products, services, delivery channels, and geographic exposure.
- 3) Key elements of the RBA include:
- **Risk Identification:** Assessing potential threats and vulnerabilities related to money laundering, terrorist financing, and proliferation financing based on data, typologies, and sector-specific indicators.

- **Risk Assessment:** Conducting and regularly updating a **Customer Risk Assessment (CRA)** for all individual customers, based on factors such as identity, geography, source of funds, and transaction behavior.
  - **Risk Mitigation:** Applying risk-appropriate measures, including **Enhanced Due Diligence (EDD)** for higher-risk customers and **Simplified Due Diligence (SDD)** only in clearly justified low-risk cases. All decisions must be supported by documented risk analysis.
  - **Ongoing Monitoring:** Continuously monitoring transactions, customer behavior, and risk indicators to detect suspicious activities and ensure that risk profiles remain current.
  - **Adaptability:** Regularly reviewing and enhancing the RBA in response to evolving risks, regulatory changes, and lessons learned from internal reviews or external findings.
- 4) By applying a structured and dynamic risk-based methodology, the AML/CFT framework remains responsive, targeted, and proportionate to the scale, complexity, and nature of operations.

## 5.1 Customer Risk Assessment (CRA)

- 1) As part of its risk-based approach, **Starlink International N.V.** conducts a **Customer Risk Assessment (CRA)** for each individual customer at the time of onboarding and updates it regularly throughout the customer relationship lifecycle. The CRA is central to determining the appropriate level of due diligence and monitoring to be applied, based on the customer's individual risk profile.
- 2) The CRA supports the effective implementation of Customer Due Diligence (CDD) by identifying customers who may pose elevated risks of money laundering (ML), terrorist financing (TF), or other illicit activity. This ensures that risk mitigation measures are tailored, proportionate, and aligned with regulatory requirements.
- 3) Each customer's risk level is assessed using a range of qualitative and quantitative indicators, which may include:
  - **Customer identity and profile** – including full legal name, age, nationality, residential address, and occupation.
  - **Transaction behavior** – including the frequency, volume, complexity, and pattern of transactions relative to the customer's declared purpose and typical behaviour.
  - **Source of funds and source of wealth** – to verify the legitimacy and transparency of financial flows.

- 4) Based on the outcome of the CRA, customers are assigned a **risk classification**—such as **Low**, **Medium**, or **High**. This classification determines the depth of due diligence required and the frequency and intensity of ongoing monitoring applied. The CRA framework and scoring methodology are detailed in **Annex 2: Customer Risk Assessment Methodology & Matrix**.

## 5.2 Customer Due Diligence (CDD)

### 1) Customer Declaration Before Account Activation

Before accessing **Starlink International N.V.**'s services, customers must complete a **mandatory self-declaration** confirming:

- They are acting solely on their own behalf as a natural person. Business accounts, legal entities, or individuals acting on behalf of third parties are not permitted to use the platform under any circumstances.
- They are not a citizen, resident, or otherwise affiliated with any country subject to international sanctions (e.g., UN, EU, OFAC, Kingdom of the Netherlands).
- They are not a Politically Exposed Person (PEP) or associated with a PEP. Customers identified as PEPs or linked parties are prohibited from using the platform.

Acceptance of these declarations must be recorded electronically (e.g., via checkbox, digital acknowledgment, or electronic signature) prior to account activation.

### 2) Identification and Verification at Withdrawal

Customer Due Diligence (CDD) is enforced **prior to the first withdrawal** and includes:

- **Photographic Verification (Selfie):**

Customers must submit a clear photograph (selfie) holding both of following:

- i. Customer's original **government-issued ID** or **passport** displayed clearly alongside the note.
- ii. A handwritten note stating (printed notes won't be accepted):
  - "For **Starlink International N.V.** use only"
  - Today's **date**
  - Customer **signature**

- **Document Review Requirement:**

To ensure compliance with our verification procedures, all submitted identification documents must meet the following criteria:

- i. The submitted identification document must be **valid**, **government-issued**, **unexpired**, and must **accurately match** the personal information registered

on the account.

- ii. The individual's **face must be clearly visible** without any obstructions (e.g., sunglasses, hats, masks).
  - iii. The **identity document** and **handwritten note** must be **fully legible**, with all text and images clearly readable.
  - iv. The selfie, including the identity document and handwritten note, must be captured in **full color**.
  - v. Black-and-white, low-quality, or heavily filtered images will not be accepted.
  - vi. The entire document and note must be **fully visible** in the image (no parts cut off or obscured).
- Withdrawal requests are **blocked** until this verification is successfully completed. Unsuccessful or suspicious verification attempts trigger escalation to Enhanced Due Diligence (EDD) procedures.

### 3) Timing and Thresholds

While basic onboarding checks apply at registration, **full verification (CDD)** must be completed **before**:

- Approving any deposit/withdrawal, regardless of amount.
- For withdrawals exceeding NAf. 4,000 or when otherwise deemed necessary, **Starlink International N.V.** requires customers to:
  - Complete standard identity verification (selfie with ID and handwritten note).
  - Declare the general source of funds via a simple online form (e.g., winnings, salary, investments).

### 4) Ongoing Monitoring

After successful CDD, all customer activities are monitored continuously. Behavior inconsistent with the declared purpose of the relationship will be investigated and may lead to escalation under EDD protocols.

## 5.3 Enhanced Due Diligence (EDD)

1) EDD is applied in higher-risk cases, particularly where:

- Customers originate from or are linked to **high-risk jurisdictions**.
- Customers present inconsistent, suspicious, or unusually complex transaction behavior.

- There is a **failure** or **refusal** to complete standard CDD requirements at withdrawal.

2) EDD Measures Include:

- Requiring additional supporting documents (e.g., secondary ID, utility bill, proof of source of funds/wealth).
- Detailed analysis of transaction patterns.

3) If a customer **cannot** satisfactorily complete EDD, **Starlink International N.V.** may suspend or terminate the account and report the case to the Financial Intelligence Unit (FIU) if necessary.

#### 5.4 Simplified Due Diligence (SDD)

- 1) SDD may be applied only in clearly defined, **low-risk scenarios** that are supported by **Customer Risk Assessment (CRA)**, and are permitted under applicable Curaçao Gaming Control Board (GCB) regulations.
- 2) Examples may include customers from reputable jurisdictions with transparent financial systems and low inherent risk indicators.

Before applying SDD:

- The rationale must be clearly documented and justified based on risk-based analysis.
  - SDD must not be applied where there are any signs of elevated risk.
  - All such cases remain subject to periodic review and monitoring.
- 3) The application of SDD must be **proportionate, justified, and recorded**, and it does not exempt the company from ongoing monitoring obligations.

#### 5.5 Targeted Financial Sanctions

- 1) All customers must be screened against relevant sanctions lists—such as those issued by the **United Nations (UN)** and **European Union (EU)**—at the time of onboarding and on a periodic basis thereafter.
- 2) Where a match is identified or a customer is linked to a designated person or entity:
  - **Immediate action** must be taken to **freeze assets** and **block transactions**, in accordance with applicable laws and without prior notice to the affected party (“no tipping off” principle).

- The incident must be **promptly reported** to the relevant regulatory and enforcement authorities, including the FIU, as required by national legislation and guidance.
- 3) Internal procedures must ensure continuous compliance with sanction obligations, including up-to-date list screening, employee awareness, and recordkeeping of all actions taken.

## 5.6 Reliance on Third Parties

- 1) Reliance on third parties to conduct elements of the Customer Due Diligence (CDD) process is permitted only under strict conditions as outlined in Curaçao Gaming Control Board (GCB) regulations.
- 2) Where such reliance occurs, the following requirements must be met:
- The third party must be **appropriately regulated and supervised** for AML/CFT compliance in a jurisdiction with equivalent standards;
  - **Customer consent** must be obtained for reliance on a third party;
  - All identification and verification data must be **readily accessible** upon request and without delay.
- 3) The regulated entity remains **ultimately responsible** for ensuring full compliance with AML/CFT obligations, regardless of any delegation or reliance.

## 5.7 Reporting of Unusual Transactions

- 1) The company maintains robust procedures to identify, assess, and report any transactions or activities that may be unusual or potentially suspicious. These procedures are aligned with the National Ordinance on the Reporting of Unusual Transactions (NORUT), internal risk assessments, and applicable regulatory guidance.
- 2) Unusual transactions may be identified through objective indicators (as defined by law or regulators) and subjective indicators (based on internal assessments and staff observations). Transactions must be escalated regardless of whether they are ultimately deemed suspicious.
- 3) Certain transaction types must be reported when the total amount reaches **NAf. 5,000 or more per gaming day**. These include:
- Cashless transfers
  - Deposits
  - Chip sales
  - Cash-outs

- Other financial movements indicative of value exchange
- 4) This threshold applies to both single and aggregated transactions conducted by a customer within the same gaming day.
  - 5) All employees are required to promptly report any unusual or suspicious transactions to the Compliance Officer or designated Money Laundering Reporting Officer (MLRO). Upon receipt:
    - The Compliance Officer/MLRO conducts a timely and documented assessment.
    - If the transaction meets the criteria for suspicion, a **Suspicious Transaction Report (STR)** is submitted to the **Financial Intelligence Unit (FIU) Curaçao** via the **goAML platform**.
    - If the transaction does **not** warrant reporting, the rationale for non-submission must be clearly documented and retained for audit and regulatory review.
  - 6) Prior to submitting any STR, the organization must be registered with the goAML system. STRs must be submitted electronically in **English**, and in accordance with the required data format.  
Registration details, submission guidelines, and further information can be found on the FIU Curaçao website: <http://www.fiucuracao.cw>.
  - 7) All STR-related communications and actions are handled under the **strict "no tipping off"** principle. Records of internal reviews, justifications, STRs, and related correspondence are securely stored and made available to regulators upon request.

## 5.8 Record Keeping

- 1) Effective recordkeeping is a critical component of AML/CFT compliance and supports transparency, traceability, and accountability in all reporting and monitoring activities.
- 2) Key requirements include:
  - **Suspicious Transaction Reports (STRs)** must be logged internally, including the **submission timestamp** and the **unique reference number** issued by the goAML system.
  - Copies of all **submitted STRs**, related **investigative documentation**, and **supporting correspondence** must be securely retained for a **minimum of five (5) years**, or longer if legally required.
  - In the event of a **follow-up inquiry** from the Financial Intelligence Unit (FIU), the Compliance Officer must respond within the prescribed legal timeframe and ensure **full cooperation** with the authorities.

- 3) All records must be stored securely and made accessible only to authorized personnel, ensuring confidentiality and integrity in line with legal and regulatory standards.

## 5.9 Employee Screening and Training

- 1) To ensure effective implementation of AML/CFT measures, comprehensive employee screening and training procedures are implemented across all relevant levels of the organization:

- **Employee Screening**

All prospective employees whose roles are relevant to AML/CFT compliance are subject to screening prior to hiring. This process assesses the individual's integrity, reliability, and suitability for handling sensitive compliance functions, with a focus on preventing internal risks to the organization.

- **Training Program**

Mandatory AML/CFT training is provided to all relevant personnel, including general staff, customer-facing employees, risk teams, compliance staff, and senior management. The training program is tailored to job functions and responsibilities, and is conducted:

- **Upon onboarding**
- **At least annually thereafter**
- **As needed following regulatory changes or emerging risks**

- 2) Training records, including attendance and training materials, are maintained and regularly reviewed for quality and relevance (see **Annex 1: AML Training Log Template**).

## 6. Compliance and Consequences of Non-Compliance

- 1) Compliance with this AML/CFT Policy and all related internal procedures is mandatory for all individuals identified in **Section 4 (Audience)**, including employees, contractors, consultants, and any other persons acting on behalf of the organization.
- 2) All relevant personnel are expected to adhere to the highest standards of integrity and diligence in fulfilling their AML/CFT obligations. This includes full cooperation with internal controls, risk mitigation measures, customer due diligence (CDD) processes, suspicious transaction reporting (STR), and applicable legal and regulatory requirements.

### 3) **Consequences of Non-Compliance**

Failure to comply with this policy or associated procedures may result in serious consequences, including but not limited to:

- **Internal Disciplinary Action:** Breaches may lead to disciplinary measures, up to and including suspension, demotion, termination of employment, or termination of contractual relationships.
  - **Legal and Regulatory Penalties:** Individuals and the organization may be subject to civil or criminal liability under applicable laws and regulations. This may include significant fines, sanctions, disqualification from holding certain roles, and potential prosecution.
  - **Reputational Damage:** Non-compliance can lead to loss of stakeholder trust, damage to the organization's reputation, and adverse media exposure.
  - **Regulatory Action:** Regulatory authorities may impose corrective measures, increased supervision, or revocation of licenses in cases of serious or repeated violations.
- 4) All personnel have a responsibility to report actual or suspected non-compliance in accordance with internal reporting procedures. Good-faith reporting of concerns will be protected from retaliation, in line with applicable whistleblower protections.

## 7. Related Information

- 1) The following laws, regulations, and guidance documents form the legal and operational foundation of the AML/CFT framework. All relevant personnel are expected to be familiar with these references and consult them as needed to support compliance efforts:
- **Curaçao Gaming Control Board (GCB) AML/CFT Regulations** – Regulatory standards and obligations specific to the gaming sector.
  - **National Ordinance on Identification when Rendering Services (NOIS)** – Requirements related to customer identification and verification.
  - **National Ordinance on the Reporting of Unusual Transactions (NORUT)** – Obligations regarding the identification and reporting of unusual and suspicious transactions.
  - **Regulation Indicators Unusual Transactions** – Detailed indicators and typologies that may suggest money laundering or terrorist financing.
  - **Sanctions National Ordinance and Related Decrees** – Legal framework governing the application and enforcement of sanctions.

- **Kingdom Sanctions Act** – Applicable international sanctions adopted and enforced within the Kingdom of the Netherlands.
  - **Financial Action Task Force (FATF) Recommendations** – Global AML/CFT standards, including risk-based approaches and sector-specific guidance.
  - **FIU Curaçao Guidance and Publications** – Operational guidelines, typology reports, and filing instructions issued by the Financial Intelligence Unit Curaçao.
  - Internal policies and procedures manuals (e.g., Customer Due Diligence, Suspicious Transaction Reporting, Risk Assessment protocols).
- 2) Personnel should regularly review updates to these resources and consult the Compliance Officer or designated point of contact with any questions or uncertainties regarding application or interpretation.

## 8. Contact Information

- 1) For questions regarding this policy, please contact:
- **Name/Office:** Mahathir Mohamed Gelam Mohamed
  - **Phone:** +60129404100
  - **Email:** mahathir87@gmail.com

## 9. Policy History

- 1) This section outlines the version control and historical changes to the AML/CFT Policy. Updates may be driven by changes in legislation, regulatory guidance, business operations, or internal risk assessments.
- **Previous Version(s):** [If applicable, list version numbers and effective dates of prior versions]
  - **Current Version:** Version 1.0
  - **Effective Date:** [Insert date of adoption or implementation]
- 2) Future revisions will be documented in accordance with the organization's policy review and approval procedures.

## 10. Policy URL (if applicable)

<https://www.interwin.com>

---

## **ANNEXES**

*(Note: These annexes need to be developed in detail as separate documents or sections, tailored to the company's specific risks and procedures.)*

- **Annex 1: AML Training Log Template**
- **Annex 2: Customer Risk Assessment (CRA) Methodology & Matrix**
- **Annex 3: High-Risk Jurisdictions List**

## **Annex 1: AML Training Log**

### **Contents of Training**

#### **General Staff:**

- Overview of AML/CFT laws (NOIS, NORUT, Sanctions National Ordinance)
- Purpose of AML/CFT regulations in gambling
- What is money laundering and terrorist financing
- Red flags and suspicious behavior in gambling transactions
- Basics of CDD and when to escalate concerns
- Confidentiality and tipping-off prohibition

#### **Customer-Facing & Risk Staff:**

- Risk indicators and how to recognize suspicious transactions
- CRA and CDD practices in online gambling
- Handling PEPs and high-risk customers
- Sanctions screening obligations
- Internal reporting procedures (STRs)

#### **Compliance & Management:**

- Customer Risk Assessments (CRA)
- Internal controls, recordkeeping, and audit trails
- How to conduct internal investigations
- Reporting to FIU Curaçao via goAML
- Oversight of third-party reliance (KYC providers)
- Regulatory updates and FATF guidance

### **AML Training Log**

| <b>Employee Name</b> | <b>Department</b> | <b>Date of Training</b> | <b>Training Module</b> | <b>Signature</b> |
|----------------------|-------------------|-------------------------|------------------------|------------------|
|                      |                   |                         |                        |                  |
|                      |                   |                         |                        |                  |
|                      |                   |                         |                        |                  |

\*Training records are retained for at least 5 years.\*

## Annex 2: Customer Risk Assessment (CRA) Methodology & Matrix

### Customer Risk Assessment Matrix

#### Risk Factors:

- Sanctions Risk
- Source of funds
- Transaction behaviour
- Delivery channel

#### Risk Scoring System:

| Factor                | Low (1) | Medium (2) | High (3) |
|-----------------------|---------|------------|----------|
| Sanctions Risk        |         |            |          |
| Source of Funds       |         |            |          |
| Transaction behaviour |         |            |          |
| Delivery channel      |         |            |          |

Final Risk Score = Sum of individual risk factors (Max score = 10)

#### Risk Levels:

| Risk Range | Risk Level | Action                                          |
|------------|------------|-------------------------------------------------|
| 1-3        | Low        | Apply standard CDD                              |
| 4-6        | Medium     | Enhanced monitoring, additional documents check |
| 7-10       | High       | Apply full EDD before withdrawal                |

#### Additional Requirements for High-Value Withdrawals.

For withdrawals exceeding NAf. 4,000 or when otherwise deemed necessary, **Starlink International N.V.** requires customers to:

- 1) Complete standard identity verification (selfie with ID and handwritten note);
- 2) Declare the general source of funds via a simple online form (e.g., winnings, salary, investments);

Customers are not initially required to submit formal supporting documents unless enhanced due diligence (EDD) is triggered based on risk indicators, suspicious behaviour, inconsistencies, or regulatory requirements.

If EDD is triggered, supporting documentation such as bank statements, payslips, or proof of crypto holdings may be requested on a case-by-case basis.

### **Annex 3: High-Risk Jurisdictions List**

The following jurisdictions are identified as high-risk due to significant strategic deficiencies in their AML/CFT regimes, as recognized by the FATF, the European Union (EU), and the Curaçao Gaming Control Board (GCB). Customers or transactions involving these jurisdictions require Enhanced Due Diligence (EDD):

#### **A. FATF – High-Risk Jurisdictions (Call for Action)**

These jurisdictions have significant strategic deficiencies and are subject to countermeasures:

- 1) North Korea (DPRK)
- 2) Iran

#### **B. FATF – Jurisdictions Under Increased Monitoring ("Grey List")**

These countries are actively working with FATF to address identified AML/CFT deficiencies:

- 1) Albania
- 2) Barbados
- 3) Burkina Faso
- 4) Cameroon
- 5) Democratic Republic of the Congo
- 6) Croatia
- 7) Haiti
- 8) Jamaica
- 9) Kenya
- 10) Mali
- 11) Mozambique
- 12) Nigeria
- 13) Panama
- 14) Philippines
- 15) Senegal
- 16) South Africa
- 17) South Sudan
- 18) Syria
- 19) Tanzania
- 20) Türkiye
- 21) Uganda
- 22) United Arab Emirates
- 23) Vietnam
- 24) Yemen

### **C. European Union – High-Risk Third Countries**

Under EU Delegated Regulation (EU) 2016/1675 and its amendments:

- 1) Afghanistan
- 2) Barbados
- 3) Burkina Faso
- 4) Cameroon
- 5) Democratic Republic of the Congo
- 6) Gibraltar
- 7) Haiti
- 8) Iran
- 9) Jamaica
- 10) Mali
- 11) Mozambique
- 12) Myanmar
- 13) Nigeria
- 14) North Korea
- 15) Panama
- 16) Philippines
- 17) Senegal
- 18) South Africa
- 19) South Sudan
- 20) Syria
- 21) Tanzania
- 22) Trinidad and Tobago
- 23) Uganda
- 24) United Arab Emirates
- 25) Vanuatu
- 26) Vietnam
- 27) Yemen

### **D. Additional Risk Factors for Consideration**

The following should also trigger EDD even if not formally listed above:

- Sanctioned Countries by the UN, OFAC, EU, or the Kingdom of the Netherlands
- Jurisdictions with high levels of corruption (based on Transparency International's Corruption Perceptions Index)
- Jurisdictions known for secrecy havens or offshore shell activity