

Know Your Customer Policy

Topc B.V.

(A company registered in Curaçao with registration number
163568)

Registered Office: Korporaalweg 10, Curaçao

Effective Date: 20.07.2025

1. Policy Statement

Topc B.V., the company registered in Curaçao, with its company number 163568, with registered office at Korporaalweg 10, Curacao (hereinafter referred to as the “Company”, “we”, “us”, or “our”), is fully committed to the prevention of money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

The purpose of this Know Your Customer (KYC) Policy is to establish a clear framework for identifying and verifying the identity of customers, monitoring customer relationships, and ensuring compliance with applicable anti-money laundering (AML) and counter-terrorist financing (CFT) regulations. This policy outlines the procedures and responsibilities required to prevent the misuse of the company’s products and services for illicit activities such as money laundering, terrorist financing, fraud, and other financial crimes.

Implementing effective KYC measures also enhances the integrity of the company’s operations and promotes transparency, trust, and regulatory compliance across all levels of the business.

1.1 Scope and Applicability

This KYC Policy applies to:

- All customers and users of the Company’s services, including individual and corporate clients;
- All business relationships established through the company’s platforms;
- All departments and staff engaged in onboarding, customer support, transaction monitoring, compliance, and risk management.

The policy is mandatory for all employees, contractors, and relevant third parties who process, review, or manage customer data and onboarding procedures.

This KYC Policy is applicable throughout the lifecycle of the customer relationship and extends to periodic reviews, monitoring, and suspicious activity reporting.

1.2 Legal Framework

This policy is designed in accordance with the laws and regulatory guidelines of **Curaçao**, specifically:

- **National Ordinance on the Identification When Rendering Services (LID)** – Establishes the requirement to identify and verify the identity of customers before the provision of certain services.
- **National Ordinance on the Reporting of Unusual Transactions (LMOT)** – Sets out obligations to monitor and report unusual or suspicious transactions to the Financial Intelligence Unit (FIU) using the goAML system.
- **AML/CFT Supervision by the Curaçao Gaming Control Board (GCB)** – The GCB, acting under its supervisory authority, issues guidance and enforces compliance with AML/CFT obligations for entities operating under Curaçao gaming licenses.
- **GCB Requirements for Compliance Officer (Based on NOIS/NORUT)** – In accordance with the **National Ordinance on Identification Services (NOIS)** and **National Ordinance on the Reporting of Unusual Transactions (NORUT)**, the GCB mandates the appointment of a designated **Compliance Officer**.

This policy also aligns with international best practices, particularly those outlined by the Financial Action Task Force (FATF), to ensure a risk-based and globally consistent approach to KYC and AML/CFT compliance.

2. Definitions

The following definitions apply specifically within the context of this Policy:

- **Anti-Money Laundering (AML)** – a set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income within the online gaming environment.
- **CFATF (Caribbean Financial Action Task Force)** – a regional organization of twenty-four (24) states in the Caribbean Basin, Central and South America. Member states, including Curaçao, have committed to implementing common countermeasures to combat money laundering and terrorist financing.

- Compliance Officer – a senior management-level individual, independent from day-to-day operations, appointed by the Company to oversee the implementation of AML/CTF controls and to ensure effective detection and prevention of money laundering and terrorist financing.
- Customer Due Diligence (CDD) – the standard process of collecting and verifying information about a customer's identity, financial activities, and risk profile before allowing them to participate in gaming activities.
- Enhanced Due Diligence (EDD) – additional, more rigorous checks performed on customers who present a higher risk (e.g., Politically Exposed Persons or those with large or unusual transactions), including deeper investigation into the source of funds and wealth.
- FATF (Financial Action Task Force) – an international intergovernmental body established in 1989. FATF develops and promotes global standards and policies to protect the financial system from money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.
- FATF Recommendations – a set of globally accepted guidelines issued by the FATF. These recommendations serve as a foundation for the Company's internal policies and procedures aimed at combating money laundering, terrorist financing, and related threats.
- FIU (Financial Intelligence Unit Curaçao) – the national authority responsible for receiving, analyzing, and reporting unusual transaction reports, as defined in Article 2 of the NORUT. The Company reports all relevant suspicious activity to the FIU in compliance with applicable law.
- Financing of proliferation (FP) – the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.
- Financial Transactions:
 - For online operations: includes player deposits and withdrawals. Bonuses are excluded. Wagers and winnings are considered gambling transactions and are not classified as financial transactions under this Policy.
- Kingdom Sanctions Act – refers to the National Ordinance published under N.G. 2016 no. 54, which provides the legal basis for implementing international sanctions within the Kingdom of the Netherlands, including Curaçao.
- Know Your Customer (KYC) – the process by which a gaming operator verifies the identity of its customers, assesses their suitability, and understands the nature of their activities to prevent fraud and money laundering.
- NOIS (National Ordinance on Identification when Rendering Services) – the legal framework (N.G. 2017, no. 92) that mandates the Company to identify and verify the identity of clients prior to the provision of services.
- NORUT (National Ordinance on the Reporting of Unusual Transactions) – the legal requirement (N.G. 2017, no. 99) under which the Company must report certain transactions to the FIU based on specific indicators of unusual or suspicious activity.
- Other Online Games – includes all Company-offered online games beyond traditional casino games, such as sports betting, esports betting, fantasy sports, lotteries, bingo, skill-based games, and virtual sports.
- Politically Exposed Persons (PEPs):
 - Foreign PEPs: individuals entrusted with prominent public functions by a foreign country, including heads of state, senior politicians, military officials, and their close associates or family members.
 - Domestic PEPs: individuals holding similar positions within Curaçao or the Kingdom of the Netherlands.
 - International Organization PEPs: individuals who hold senior roles within international organizations (e.g., directors or board members).

- Risk-Based Approach (RBA) – a methodology where resources and controls are allocated according to the assessed risk level of customers, products, and transactions, allowing for more intensive scrutiny where the risk of money laundering is higher.
- Sanctions National Ordinance – refers to the national legislation published under N.G. 2014 no. 55, mandating compliance with international sanctions adopted by Curaçao.
- Source of Funds – the specific origin of the money used for a particular transaction by a customer, such as income, gambling winnings, property sale proceeds, savings, or legal compensation.
- Source of Wealth – the broader origin of a customer's overall accumulated wealth over time, including employment history, investments, inheritances, or business ownership.
- Suspicious Activity Report (SAR) – a formal report submitted to regulatory authorities when a gaming operator detects activities or transactions that may be linked to money laundering or other financial crimes.
- (Ultimate) Beneficial Ownership (UBO) – refers to the natural person(s) who ultimately own or control a customer or who benefit from a transaction. This includes individuals who exercise effective control over a legal entity, even if not directly listed as owners.
- Unusual Transaction – a transaction identified as unusual based on pre-defined indicators. Such transactions are subject to enhanced scrutiny and reporting obligations.
- Weapons of Mass Destruction (WMD) – a category of weapons designed to cause widespread harm and destruction, primarily encompassing nuclear, chemical, and biological weapons.

3. Customer Acceptance Policy

Customer Acceptance Policy (CAP)

The Customer Acceptance Policy (CAP) outlines the conditions under which the Company enters into or maintains a business relationship with players. It operates in conjunction with the Customer Risk Assessment (CRA) to ensure an RBA to managing player onboarding and engagement.

The CAP supports the Company's compliance with its Anti-Money Laundering, Countering the Financing of Terrorism (AML/CFT), and Counter-Proliferation Financing obligations. It ensures that all customers are assessed consistently and proportionately in line with the level of ML/TF/PF risk they present.

The CAP has the following primary objectives:

- To ensure customers posing a higher-than-average ML/TF/PF risk are identified and subject to enhanced scrutiny;
- To categorize customers according to risk (low, medium, high);
- To determine and apply the appropriate level of **CDD**;
- To implement procedures for refusing or terminating relationships with unacceptable risk;
- To comply with regulatory requirements related to **PEPs** and **Sanctions Screening**;
- To align customer onboarding practices with the Company's **risk appetite** and regulatory environment.

The Company classifies customers into the following risk tiers, each of which requires a specific level of CDD:

Low Risk

Customers with:

- Low transaction volumes;
- Transparent and consistent behavior.

CDD Measures:

- Standard CDD at onboarding;
- Routine monitoring of transactional behavior;
- Periodic review in line with regulatory timelines.

Medium Risk

Customers with:

- Moderate or increasing transaction volumes;
- Irregular gambling patterns or cross-border activity
- Frequent use of anonymous payment methods

CDD Measures:

- Enhanced verification;
- More frequent transactional reviews;
- Ongoing due diligence and monitoring triggers.

High Risk

Customers with:

- PEP status or close associations with PEPs;
- Residency or origin in high-risk jurisdictions;
- Unusual or unexplained betting behavior;
- Signs of structuring, anonymity, or third-party interactions.

CDD Measures:

- EDD, including detailed scrutiny of source of wealth;
- Senior management approval required to onboard or retain;
- Transaction monitoring on a continuous basis;
- Periodic reassessment based on player activity and regulatory changes.

The Company reserves the right to refuse or terminate service under the following circumstances:

- The customer fails to provide satisfactory identification or CDD documentation;
- The customer is identified on a sanctions list or linked to a terrorist organization;
- The customer is non-cooperative or provides misleading information;
- The risk profile exceeds the Company's established risk appetite;
- The customer is associated with illegal activities or attempted ML/TF/PF.

PEPs and Sanctions Screening

In accordance with AML/CFT requirements, the CAP includes:

- **Mandatory screening** for all customers against PEP and sanctions databases at onboarding and regularly thereafter;
- Enhanced CDD and ongoing monitoring for identified PEPs and their close associates or family members;
- Immediate review and reporting obligations in the event a match is found with:
 - United Nations Sanctions Lists;
 - OFAC, EU, and other relevant bodies' lists;
 - Local regulatory or law enforcement watchlists.

4. CDD and EDD

CDD is a cornerstone of the Company's AML/CFT framework. It ensures the identification and verification of customers, ongoing monitoring of business relationships, and detection of suspicious behavior, with the ultimate goal of preventing money laundering, terrorist financing, and proliferation financing.

Casinos are prohibited from keeping anonymous or fictitious accounts. The Company shall not establish or maintain a business relationship without first conducting proper CDD. No occasional or ongoing transaction may be permitted without sufficient information about the customer's identity and risk profile.

CDD measures shall be applied:

At the time of onboarding;

When there is doubt about the authenticity or adequacy of previously obtained customer information;

When there are indications of suspicious activity.

4.1 Individual Clients

The Company undertakes CDD in the following scenarios:

- a. When a player engages in a transaction equal to or above **NAf 4,000** (or equivalent in another currency);
- b. When carrying out occasional transactions above **NAf 4,000**, including linked transactions which cumulatively exceed the threshold;
- c. When there is a **suspicion of money laundering, terrorist financing, or proliferation financing**;
- d. When the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

Occasional transactions are typically associated with one-off interactions, especially in land-based settings, but are applicable to online operations when no formal account is opened.

4.2 Core CDD Measures

CDD comprises the following components:

a. Identification of the Player

- Required minimum information:
 - Full name
 - Permanent residential address
 - Date of birth
 - Place of birth
 - Nationality
 - Government-issued ID number

In **low-risk cases**, only the name, address, and date of birth may be collected. In **high-risk cases**, additional identifying data may be required.

b. Verification of the Player's Identity

- Must be based on reliable and independent documents, including:
 - Government-issued ID (passport, national ID)
 - Proof of address (bank statement, utility bill, letter from public authority, not older than 6 months)
- Supplementary methods:
 - Email/phone verification
 - Biometric checks
 - IP address and geo-location data
 - Social media or public registries
 - Cross-checks using internal and external databases

c. Understanding the Nature and Purpose of the Business Relationship

- A clear risk-based profile must be developed, considering:
 - Stated purpose (e.g. gaming entertainment);
 - Expected activity levels;
 - **Source of wealth** and **source of funds**, particularly in high-risk scenarios;
 - Information may be supplemented by:
 - Income declarations
 - Publicly available data (e.g. Transparency International, KnowYourCountry.com)
 - Statistical data on average income in the jurisdiction

d. Ongoing Due Diligence and Monitoring

- Monitor transactions for consistency with the player's profile;
- Identify and investigate deviations or suspicious activity;
- Update player information as necessary.

4.3 Freezing of Funds and Reporting

If a player is identified as:

- A **designated person** under applicable sanctions;
- A **PEP** acting suspiciously;
- A **high-risk individual** linked to money laundering or terrorism;

Then the Company must:

1. **Immediately freeze the player's account** and block further transactions;
2. **File an Unusual Transaction Report (UTR)** with the **Financial Intelligence Unit (FIU) Curaçao**;
3. Avoid any action that could constitute **tipping-off** the player;
4. **Document the reasoning and actions taken** for compliance and audit purposes.

If the FIU determines the transaction is suspicious, it may refer the case for criminal investigation. The Company must **not disclose to the player** that a report has been made.

4.4 Tipping-Off Risk

The Company will continuously train its staff to avoid alerting a player when CDD, monitoring, or reporting actions are underway. Where performing CDD may increase the risk of tipping-off, the Company may defer the process and report directly to the FIU.

4.5 Third-Party Reliance Rules

The Company may rely on third parties (such as financial institutions, law firms, or regulated entities) to perform aspects of the CDD process, provided that:

The third party is subject to equivalent AML/CFT obligations;

Written agreements are in place to ensure access to relevant documentation without delay;

The Company remains ultimately responsible for the customer's CDD and risk assessment.

Third-party reliance must be documented and approved by the Compliance Officer.

4.6 Record Keeping Obligations

In accordance with Curaçao legislation (LID and LMOT), all customer due diligence documentation and transaction records must be securely stored for a minimum period of five (5) years after the termination of the business relationship or completion of a transaction.

Records must include:

Copies of identification and verification documents;

Information collected during ongoing monitoring;

Risk assessments and client classification;

Records of any suspicious activity reports (SARs).

All records must be easily retrievable and available to competent authorities upon request.

5. Transaction Monitoring

The Company will take all possible efforts to monitor transactions on a continuous basis to:

- Detect unusual or suspicious patterns that may indicate money laundering, terrorist financing, fraud, or other financial crimes;
- Identify transactions inconsistent with the customer's known profile, business, or risk level;
- Trigger Enhanced Due Diligence (EDD) procedures where necessary.

Automated or manual monitoring tools may be used, depending on the customer risk level and transaction volume. Alerts generated through monitoring must be reviewed by trained personnel and escalated to the Compliance Officer where appropriate.

Transactions requiring attention include:

- Large cash transactions;
- Rapid movement of funds in and out of accounts;
- Transfers involving high-risk or sanctioned jurisdictions;
- Unexplained changes in transaction behavior.

6. Risk Profile Updates

Each customer is assigned a risk classification (e.g., low, medium, high) during onboarding. This profile must be updated when:

- New information becomes available (e.g., change in ownership, business model, or residency);
- Suspicious behavior or transactions are detected;
- Trigger events occur (e.g., regulatory inquiries, adverse media).
- Changes to a customer's risk profile may result in enhanced monitoring, additional verification, or a decision to terminate the relationship.

Periodic reviews of customer profiles must be conducted at intervals proportionate to their risk classification:

High-risk customers: annually;

Medium-risk customers: every 2 years;

Low-risk customers: every 3 to 5 years.

The review process includes:

- Re-validation of identification documents;
- Updating contact and business information;
- Re-assessment of the customer's source of funds;
- Confirmation of ongoing alignment with expected activity.

Where discrepancies or red flags are identified, appropriate remedial actions must be taken, including escalation to the Compliance Officer and, if necessary, filing a Suspicious Activity Report (SAR).

7. Source of Funds and Source of Wealth Checks

As part of the due diligence process, the company may request a clear understanding of:

- **Source of Funds (SoF)** – The specific origin of the funds used for a transaction or deposit (e.g., salary, company revenue, inheritance, investment income).
- **Source of Wealth (SoW)** – The origin of the customer's total wealth or net worth (e.g., business ownership, real estate holdings, long-term investments).

These checks are especially important for:

- High-risk clients (including PEPs and clients from high-risk jurisdictions);
- Clients engaging in large or unusual transactions;
- Complex legal structures.

Documentation or evidence of SoF/SoW may include:

- Bank statements;
- Employment contracts or pay slips;
- Tax returns;
- Sale agreements;
- Audited financial statements.

Where the source of funds or wealth cannot be reasonably verified, the relationship should be rejected or terminated, and a Suspicious Activity Report (SAR) may be submitted to the Financial Intelligence Unit (FIU).

8. Suspicious Activity Reporting (SAR/STR)

All employees, contractors, engaged persons should be trained to recognize indicators of suspicious behavior and escalate concerns to the Compliance Officer. Suspicious activity may include, but is not limited to:

- Unexplained changes in customer behavior or transaction patterns;
- Transactions inconsistent with the customer's known profile;
- Attempts to conceal identity or ownership structure;
- Use of third parties or proxies without clear justification;
- Use of high-risk or sanctioned jurisdictions.

If, after internal investigation, the Compliance Officer reasonably suspects that a transaction or activity involves criminal conduct, a **Suspicious Activity Report (SAR)** — also referred to as a **Suspicious Transaction Report (STR)** — must be submitted **without alerting the customer**.

SARs must be submitted promptly and in compliance with prescribed timelines and formats.

9. goAML System Usage

All reporting of unusual or suspicious transactions must be conducted via the **goAML portal**, the official reporting platform of the **FIU Curaçao**.

Key goAML requirements include:

- Registration of the institution and Compliance Officer with the FIU;
- Secure login and controlled access to the system;
- Use of the appropriate reporting forms (e.g., objective vs. subjective indicators);
- Accurate and complete data entry;
- Timely responses to follow-up requests from FIU authorities.

10. Threshold-Based Reporting

Certain transactions must be reported to the FIU even if there is no suspicion of criminal activity. These objective indicators are defined by law and include transactions that:

Involve cash or equivalents above a specified monetary threshold (e.g., ANG 25,000 or its equivalent in foreign currency);

Fall under transaction types explicitly listed by the FIU (e.g., international wire transfers over a set amount);

Involve jurisdictions or sectors identified as high-risk by the GCB or FIU.

11. Sanctions Screening

The Company must screen all players against international and local sanctions and PEP lists at onboarding and periodically thereafter.

Sanctions Screening:

- Players are checked against:
 - o UN Sanctions List: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>
 - o EU Sanctions Map: <https://www.sanctionsmap.eu>
 - o Any local list issued by Curaçao authorities

PEP Screening:

- Sources include:
 - o Publicly available news sources
 - o The Transparency International Corruption Perceptions Index
 - o www.knowyourcountry.com
 - o PEP Caribbean List
- Where a customer is identified as a PEP, EDD is applied, including:
 - o Senior management approval;
 - o Identification of the source of wealth/funds;
 - o Continuous enhanced monitoring.

12. Data Protection & Confidentiality

The company is committed to maintaining the highest standards of data protection and confidentiality in handling customer information. All personal and financial data collected during the KYC and due diligence process must be securely stored, accessed only by authorized personnel, and protected from unauthorized disclosure, loss, or misuse.

This policy ensures compliance with applicable data protection laws in Curaçao and relevant international standards

Storage of KYC Documents

All KYC-related documents and customer records must be:

- Stored in a secure, encrypted digital environment with restricted access;
- Backed up regularly to prevent loss or corruption;
- Retained for a minimum of **five (5) years** following the end of the business relationship or the completion of the last transaction, as required by the **LID** and **LMOT**;
- Made readily available to competent authorities (e.g., FIU Curaçao, Gaming Control Board) upon lawful request.

Documents include, but are not limited to:

- Identification documents;
- Proof of address;
- Corporate registration records;
- Source of funds/wealth documentation;
- Transaction history;
- Risk assessments and internal reports.

Where hard copies exist, they must be stored in physically secure, access-controlled environments.

Data Privacy Alignment

Customer data must be collected and processed only for legitimate purposes related to customer due diligence, regulatory compliance, and risk management. The company commits to the following principles:

- **Lawfulness, fairness, and transparency** – Customers must be informed of the purpose for collecting personal data;
- **Purpose limitation** – Data is used strictly for AML/CFT, compliance, and related operational needs;
- **Data minimization** – Only information that is relevant and necessary for due diligence is collected;
- **Accuracy** – Customer data must be kept accurate and up to date;
- **Integrity and confidentiality** – Technical and organizational measures must be in place to protect data from unauthorized access or breaches;
- **Right to access** – Where applicable, customers may request access to their personal data, subject to legal limitations.

13. Compliance Officer

13.1 Appointment & Responsibilities

The company shall formally appoint a **Compliance Officer (CO)** who is **independent from operational functions**. This appointment fulfills statutory requirements under the **National Ordinance on the Identification of Clients when Rendering Services (NOIS)** and the **National Ordinance on the Reporting of Unusual Transactions (NORUT)**. The Compliance Officer shall have **timely and unrestricted access** to all customer identification data, CDD files, transaction records, and other relevant documentation.

The Compliance Officer shall act independently and is entrusted with the following key responsibilities:

- Design, implement, and regularly update the company's AML/CFT compliance program.
- Ensure compliance with Curaçao's NOIS, NORUT, and guidance issued by the GCB.
- Monitor internal adherence to AML policies and procedures.
- Conduct transaction monitoring and analysis to identify suspicious activity.
- Review and investigate unusual transaction reports (UTRs) and determine escalation requirements.
- Submit Suspicious Transaction Reports (STRs) to the FIU Curaçao via goAML.
- Maintain complete and accurate records of all internal and external reporting activity.
- Develop internal procedures for account blocking/freezing when warranted by UTRs or STRs.
- Deliver AML/CFT training to relevant staff members.
- Stay updated on changes in AML/CFT legislation and provide advisory support to management.

- Prepare periodic AML reports to management and regulators.

13.2 Training, Independence & Fit-and-Proper Requirements

Per GCB guidelines, the Compliance Officer must meet **fit-and-proper criteria** and demonstrate **professional competence and integrity**, including:

- At least **2 years of AML/CFT experience** with a **relevant degree** or **recognized AML certification** (e.g., **CAMS, AMLFC**),

or

At least **4 years of AML/CFT experience** in a reporting role;

- Alternatively, **2 years of experience as an MLRO** or equivalent role in another jurisdiction;
- Knowledge of Curaçao's AML laws and familiarity with EU/OFAC sanctions list screening.

The appointed individual must submit to the GCB a completed **Personal History Disclosure Form**, supported by a CV and documentation allowing for a full due diligence review. Areas of assessment include:

- Professional and personal history (including regulatory or legal issues);
- Reputation checks, including references and industry background;
- Ongoing commitment to AML/CFT education (minimum **10 hours of training annually**).

13.3 Conflict of Interest and Role Exclusivity

To ensure functional independence, the role of Compliance Officer **must not be combined** with the following positions:

- CEO, CFO, COO, UBO
- Casino Manager, Slot Manager
- Other operational, audit, or revenue-generating functions

The Compliance Officer role must remain fully independent and report directly to senior management or the board.

13.4 Outsourcing and Jurisdictional Scope

- The compliance function may be **outsourced** to a reputable third party, subject to GCB approval. The outsourcing contract and qualifications of the responsible person must be provided upon request.
- A Compliance Officer may act in the same role for multiple licensed entities, but **no more than 10 operators** (including roles in other jurisdictions), unless specifically approved by the GCB.
- Individuals may hold concurrent MLRO positions in other jurisdictions only if they have the **time and capacity** to fulfill all duties effectively.

13.5 Transitional Arrangements

If an appointed Compliance Officer does not fully meet the GCB's **competency requirements**, the operator:

- Must comply **immediately** with personal history and integrity checks;
- Has up to **6 months** to meet responsibilities and independence requirements;
- Has up to **12 months** to close any educational or experience gaps, subject to submission of a formal **training plan** for GCB monitoring.

14. Employee Screening and Training Program

The Company shall follow high ethical standards and compliance with financial laws through rigorous employee screening, including criminal background checks.

A comprehensive training program is provided to all employees who handle customer transactions or AML-related duties. Training is tailored by role:

New employees: General AML/CTF awareness, internal policies, and reporting obligations.

Frontline staff (dealers, cashiers): Specific training on recognizing and responding to money laundering risks in gambling operations.

Audit staff: Updates on regulatory changes and AML enforcement.

AML Compliance staff: Advanced training on emerging risks and regulatory expectations.

Supervisors and managers: In-depth instruction on AML policies and oversight responsibilities.

Senior management and board: Regular briefings on AML risks and reputational impacts.

Refresher training is conducted regularly, and detailed records of all training activities, participants, content, and outcomes are maintained.

15. Record Retention Policy

The Company shall retain all relevant customer, transactional, and compliance-related records in accordance with legal obligations set forth under the **National Ordinance on the Identification of Clients when Rendering Services (NOIS)** and the **National Ordinance on the Reporting of Unusual Transactions (NORUT)**. This section outlines the mandatory retention periods and the procedures for secure archiving and access control.

15.1 Retention Periods

The Company is required to retain the following records for a minimum of five (5) years, unless otherwise mandated by law or instructed by a competent authority:

- Customer Identification Data: including KYC documents, identification records, and verification information.
- Customer Due Diligence (CDD) Files: including risk assessments, source of funds/wealth checks, and beneficial ownership documentation.
- Transaction Records: including financial transaction history, payment logs, and internal audit trails.
- Suspicious Transaction Reports (STRs): both internally reported and those submitted to the FIU Curaçao.
- Internal Investigation Files: including notes, memos, or other documentation related to escalations or unusual activity.
- Training and Compliance Logs: records of AML/CFT training provided to staff and audit trails of compliance-related reviews.

The five-year period begins from the date of the last transaction or the termination of the customer relationship, whichever is later.

Where an investigation is ongoing or records are requested by law enforcement or a regulator, the Company shall retain the relevant files until explicitly authorized to delete them.

15.2 Secure Archiving Procedures

To protect the integrity, confidentiality, and availability of records:

- All documents shall be stored in **secure, access-controlled environments**, whether in **digital or physical** form.

- **Digital records** must be encrypted and backed up regularly on secure servers located in jurisdictions compliant with applicable data protection laws.
- **Physical records** (if maintained) must be stored in locked cabinets within restricted access premises.
- Access to archived records shall be **limited to authorized personnel** only, and any access or retrieval must be **logged and auditable**.
- The Company shall establish **disaster recovery protocols** to ensure data preservation in case of system failure or breach.
- At the end of the legally required retention period, documents may only be destroyed following a **documented and secure disposal process**, which includes:
 - **Digital files:** Secure deletion using data wiping tools;
 - **Physical files:** Shredding or certified destruction by an authorized provider.

16. Periodic Review

The Compliance Officer shall ensure that the KYC/AML Policy is formally **reviewed at least annually** or more frequently under the following circumstances:

- Updates to applicable laws, ordinances, or guidance (e.g., NOIS, NORUT, GCB guidance);
- Changes in the Company's business model, product offerings, or risk exposure;
- Findings from internal audits, regulatory inspections, or compliance reviews;
- Material breaches or deficiencies identified in policy implementation;
- Emerging AML/CFT typologies, technologies, or industry risks.

The review process shall assess the **continued adequacy, clarity, and effectiveness** of the policy and associated procedures.

The results of each review, including proposed changes and rationale, must be **documented** and presented to senior management for approval.

17. Policy History

This is a new policy established to formalize the Company's AML and CFT framework in compliance with Curacao regulations.

Version 1.0

Effective Date 20 July 2025