



CANARY ALLEY B.V.

AML AND KYCPOLICY

Version:
Approved By:
Review Frequency:
Effective Date:

2.0
Board of Directors
Annual or upon material regulatory change
09/06/2026

Previous Version	Current Version	Edit Date	Changes	Editor	Signature
---	1.0	10/07/2025	First Version	MO	
1.0	2.0	09/06/2026	Second version –rewritten to comply with LOK 24th December 2024 - Official English Translation, AML Policy – Document Template for License Applicants and Holders 30 January 2026, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction.	MO	Signed by:  8737E2B30CF043F... Director: Signed by:  E9C1A4A3F74E4ED... Director:



PART 1

AML, CFT & CPF GOVERNANCE, POLICY STATEMENT AND COMPLIANCE PROGRAMME

1.1 Purpose

The purpose of this AML, Counter-Terrorist Financing and Counter-Proliferation Financing Compliance Manual ("Manual") is to establish the governance framework, policies, procedures, systems and controls through which Canary Alley B.V. identifies, assesses, manages, mitigates and reports risks associated with:

- Money Laundering ("ML");
- Terrorist Financing ("TF");
- Proliferation Financing ("PF");
- Sanctions Evasion;
- Fraud and Financial Crime.

This Manual forms part of the Company's overall compliance framework and shall apply to all activities conducted under its Curaçao licence.

The Company acknowledges that preventing the misuse of its products and services for financial crime is a fundamental licensing obligation and a core component of player protection and regulatory compliance.

1.2 AML Policy Statement

Canary Alley B.V. adopts a zero-tolerance approach towards money laundering, terrorist financing, proliferation financing, sanctions breaches and other forms of financial crime.

The Company shall not knowingly:

- establish a business relationship with persons engaged in criminal conduct;
- facilitate the concealment of criminal proceeds;
- permit the use of its products or services for terrorist financing;
- facilitate sanctions evasion;
- facilitate proliferation financing activities.

The Company shall maintain effective systems and controls proportionate to its risk profile and regulatory obligations.

All personnel are required to support the Company's AML programme and cooperate fully with compliance activities.



1.3 Regulatory Framework

This Manual has been developed having regard to:

Primary Legislation

- National Ordinance on Games of Chance (LOK);
- National Ordinance on Identification when Rendering Services (NOIS);
- National Ordinance on Reporting Unusual Transactions (NORUT);
- Applicable Sanctions Legislation;
- Applicable Proliferation Financing Requirements.

Regulatory Requirements

- Curaçao Gaming Authority AML/CFT/CPF Regulations (January 2025);
- Curaçao Gaming Authority AML Policy Template (January 2026);
- Curaçao Gaming Authority Licence Conditions;
- Applicable Guidance issued by the Curaçao Gaming Authority.

International Standards

- FATF Recommendations;
- FATF Risk-Based Approach Guidance;
- FATF Guidance for Online Gambling Operators;
- FATF Guidance on Virtual Assets (where applicable).

Where multiple requirements apply, the most stringent requirement shall prevail unless otherwise approved by the Compliance Officer.

1.4 Scope

This Manual applies to:

Personnel

- Directors;
- Officers;
- Employees;
- Contractors;
- Consultants;
- Temporary Staff;



- Outsourced Service Providers.

Activities

- Customer onboarding;
- Customer due diligence;
- Ongoing monitoring;
- Payment processing;
- Withdrawal processing;
- Customer support;
- Responsible Gaming interactions;
- Fraud prevention;
- Compliance investigations.

Products and Services

The Manual applies to all gambling products and services offered under the Company's Curaçao licence.

1.5 AML Programme Objectives

The Company's AML programme shall seek to:

Prevent Criminal Abuse

Prevent the misuse of products and services for financial crime.

Identify Higher-Risk Customers

Identify customers presenting elevated ML/TF/PF risks.

Detect Suspicious Activity

Identify unusual and suspicious behaviour promptly.

Support Regulatory Compliance

Ensure compliance with all applicable AML obligations.

Protect the Company

Reduce legal, regulatory, operational and reputational risks.

Support Law Enforcement

Assist competent authorities through timely reporting of unusual and suspicious activity.



1.6 Risk-Based Approach

The Company shall apply a risk-based approach to AML/CFT/CPF compliance.

Resources and controls shall be allocated according to identified risks.

Risk assessments shall consider:

- customer risk;
- product risk;
- service risk;
- geographical risk;
- payment risk;
- technological risk;
- delivery channel risk.

The Company shall not adopt a "one-size-fits-all" approach.

1.7 Three Lines of Defence Model

The Company shall operate a Three Lines of Defence model.

First Line of Defence

Business and operational functions.

Responsibilities include:

- customer onboarding;
- transaction processing;
- customer interaction;
- identification of unusual activity;
- escalation of concerns.

First-line personnel own and manage AML risks within their operational areas.

Second Line of Defence

Compliance Function.

Responsibilities include:



- AML oversight;
- policy development;
- monitoring;
- investigations;
- regulatory reporting;
- risk assessments;
- training.

The Compliance Officer acts as the second-line control function.

Third Line of Defence

Independent Assurance.

Responsibilities include:

- independent review;
- independent testing;
- audit activities;
- assessment of control effectiveness.

Independent reviews may be conducted internally or externally.

1.8 Board Responsibilities

The Board of Directors retains ultimate responsibility for AML/CFT/CPF compliance.

The Board shall:

- approve this Manual;
- approve material AML policies;
- approve the Business Risk Assessment;
- oversee AML risk management;
- review material compliance issues;
- review AML reporting;
- ensure sufficient resources are available;
- ensure independence of the Compliance Function.



The Board may delegate operational responsibilities but cannot delegate ultimate accountability.

1.9 Compliance Officer

The Company shall appoint a suitably qualified Compliance Officer.

The Compliance Officer shall possess:

- sufficient authority;
- sufficient independence;
- sufficient resources;
- unrestricted access to information.

The Compliance Officer shall report directly to senior management and the Board where necessary.

1.10 Responsibilities of the Compliance Officer

The Compliance Officer shall:

Governance

- maintain AML policies;
- maintain AML procedures;
- maintain compliance frameworks.

Risk Management

- maintain the Business Risk Assessment;
- maintain customer risk methodologies;
- oversee risk reviews.

Monitoring

- oversee transaction monitoring;
- oversee customer monitoring;
- oversee sanctions screening.

Investigations

- investigate suspicious activity;
- assess unusual transactions;



- determine escalation requirements.

Reporting

- submit required regulatory reports;
- liaise with competent authorities;
- prepare Board reporting.

Training

- deliver AML training;
- maintain training records.

1.11 Independence of the Compliance Function

The Compliance Function shall operate independently from revenue-generating functions.

The Compliance Officer shall have authority to:

- reject customers;
- require additional due diligence;
- suspend transactions;
- escalate concerns;
- recommend account restrictions.

Commercial considerations shall not override AML requirements.

1.12 AML Governance Committee

Where appropriate, management may establish an AML Governance Committee.

The Committee may review:

- high-risk customers;
- PEP relationships;
- sanctions concerns;
- suspicious activity trends;
- AML risk assessments.

Meeting minutes shall be retained.



1.13 AML Reporting Framework

The Compliance Officer shall provide periodic reporting to management.

Reports shall include:

Risk Exposure

- emerging risks;
- high-risk customer volumes;
- jurisdictional risks.

Monitoring Activity

- alerts generated;
- investigations completed;
- escalations.

Regulatory Reporting

- unusual transaction reports;
- sanctions issues;
- material incidents.

Control Effectiveness

- training completion;
- monitoring effectiveness;
- audit findings.

1.14 Escalation Framework

Employees must immediately escalate:

- suspicious activity;
- sanctions concerns;
- fraudulent activity;
- unusual transactions;
- attempted circumvention of controls.

Escalations shall be made to the Compliance Officer without delay.

Failure to escalate concerns may constitute a disciplinary matter.



1.15 Confidentiality

AML investigations and reporting activities shall remain confidential.

Personnel must not disclose:

- investigations;
- regulatory reports;
- monitoring activity;
- internal escalations.

Unauthorised disclosure may constitute tipping-off and may result in disciplinary action.

1.16 Cooperation with Authorities

The Company shall cooperate fully with:

- Curaçao Gaming Authority;
- Financial Intelligence Unit;
- Law Enforcement Agencies;
- Competent Authorities.

Requests for information shall be handled promptly and professionally.

1.17 Resource Requirements

The Company shall ensure sufficient:

- staffing;
- technology;
- training;
- systems;
- expertise

to operate an effective AML programme.

Resource requirements shall be reviewed periodically.

1.18 Record Keeping



The Company shall maintain records sufficient to demonstrate compliance with:

- legal obligations;
- regulatory obligations;
- licence conditions.

Records shall be retained in accordance with applicable retention requirements.

1.19 Policy Breaches

Failure to comply with this Manual may result in:

- retraining;
- formal warnings;
- access restrictions;
- disciplinary action;
- termination of employment or engagement.

Serious breaches shall be escalated immediately.

1.20 Annual Review

This Manual shall be reviewed at least annually and following:

- material regulatory change;
- material business change;
- significant incidents;
- audit findings;
- changes to the Company's risk profile.

The review shall be documented and approved by the Board.



PART 2

AML RISK MANAGEMENT FRAMEWORK, BUSINESS RISK ASSESSMENT (BRA) AND CUSTOMER RISK ASSESSMENT (CRA)

2.1 Purpose

The purpose of this section is to establish the framework through which Canary Alley B.V. identifies, assesses, manages, mitigates and monitors money laundering, terrorist financing and proliferation financing risks.

The Company recognises that an effective risk-based approach is the foundation of an effective AML/CFT/CPF programme.

All AML controls implemented by the Company shall be proportionate to the risks identified through its risk assessment process.

The Company shall maintain documented and auditable risk assessment methodologies capable of demonstrating compliance with applicable legal and regulatory requirements.

2.2 Risk-Based Approach

The Company shall apply a risk-based approach to AML/CFT/CPF compliance.

The risk-based approach requires the Company to:

- identify risks;
- assess risks;
- document risks;
- implement controls;
- monitor risks;
- review risks.

Resources shall be allocated according to identified risk exposure.

Higher-risk activities shall receive enhanced controls and oversight.

Lower-risk activities may receive simplified controls where legally permissible.

2.3 AML Risk Management Framework

The AML Risk Management Framework shall consist of:

Business Risk Assessment (BRA)

Assessment of risks affecting the Company.



Customer Risk Assessment (CRA)

Assessment of risks presented by individual customers.

Product Risk Assessment

Assessment of risks arising from products and services.

Jurisdiction Risk Assessment

Assessment of geographical exposure.

Technological Risk Assessment

Assessment of technology-related ML/TF/PF risks.

Ongoing Monitoring

Continuous reassessment of risk exposure.

2.4 Responsibility for Risk Assessments

The Compliance Officer shall be responsible for:

- preparing risk assessments;
- maintaining methodologies;
- reviewing risks;
- documenting findings;
- reporting results.

Senior Management shall support the risk assessment process.

The Board shall approve material risk assessments.

BUSINESS RISK ASSESSMENT (BRA)

2.5 Purpose of the Business Risk Assessment

The Company shall maintain a documented Business Risk Assessment ("BRA").

The BRA shall identify and assess ML/TF/PF risks associated with:

- customers;
- products;
- services;



- delivery channels;
- payment methods;
- jurisdictions;
- technology.

The BRA forms the foundation of the Company's AML programme.

2.6 Frequency of Review

The BRA shall be reviewed:

At Least Annually

A full documented review.

Following Material Change

Including:

- new products;
- new markets;
- new payment methods;
- mergers;
- acquisitions;
- significant incidents.

Following Regulatory Change

Where regulatory requirements change.

2.7 Customer Risk Assessment Factors

The BRA shall evaluate risks associated with customer types.

Examples include:

Lower Risk

- standard recreational customers;
- customers from lower-risk jurisdictions.

Higher Risk

- high-spending customers;



- customers using multiple payment methods;
- politically exposed persons;
- customers from higher-risk jurisdictions.

2.8 Product Risk Assessment

The BRA shall assess risks associated with products and services.

Factors may include:

- transaction speed;
- transaction volume;
- anonymity potential;
- transferability of value;
- fraud exposure.

Each product shall receive a documented risk assessment.

2.9 Payment Method Risk Assessment

The Company shall assess risks associated with payment methods.

Factors include:

- traceability;
- ownership verification;
- fraud exposure;
- sanctions exposure.

Payment methods presenting elevated risk shall receive enhanced scrutiny.

2.10 Jurisdiction Risk Assessment

The Company shall assess risks associated with geographical exposure.

Assessment criteria may include:

- FATF publications;
- sanctions programmes;
- corruption indices;



- regulatory standards;
- law enforcement cooperation.

The Compliance Officer shall maintain a jurisdiction risk matrix.

2.11 Delivery Channel Risk Assessment

The Company shall assess risks associated with customer interaction channels.

Examples include:

- fully remote onboarding;
- online verification;
- customer support interactions.

Controls shall be proportionate to identified risks.

2.12 Technological Risk Assessment

The Company shall assess technological risks capable of facilitating ML/TF/PF.

Examples include:

- identity fraud;
- account takeover;
- automation abuse;
- payment abuse;
- synthetic identity risks.

Technology controls shall be reviewed periodically.

2.13 Proliferation Financing Risk Assessment

The Company shall assess risks associated with proliferation financing.

Assessment factors include:

- sanctions exposure;
- jurisdictional exposure;
- customer exposure;
- payment activity.



The assessment shall be reviewed periodically.

2.14 Inherent Risk Assessment

Before considering controls, the Company shall determine inherent risk levels.

Inherent risk represents exposure before mitigation measures are applied.

Assessment factors shall be documented.

2.15 Residual Risk Assessment

Residual risk represents the remaining risk after controls are applied.

The Company shall assess whether residual risk remains acceptable.

Where residual risk exceeds appetite, additional controls shall be implemented.

2.16 Risk Rating Methodology

The Company shall maintain a documented risk scoring methodology.

Risk assessments shall consider:

Likelihood

Probability of occurrence.

Impact

Potential consequences.

Control Effectiveness

Strength of mitigating controls.

2.17 Risk Rating Categories

The Company shall utilise the following categories:

Rating	Description
Low	Limited exposure
Medium	Moderate exposure
High	Significant exposure



Rating Description

Very High Material exposure requiring enhanced controls

2.18 Risk Appetite

The Company shall define and document its AML risk appetite.

The Company shall not knowingly accept:

- sanctioned persons;
- terrorist organisations;
- persons engaged in criminal activity;
- prohibited customers.

Higher-risk customers may only be accepted subject to enhanced controls.

CUSTOMER RISK ASSESSMENT (CRA)

2.19 Customer Risk Assessment Framework

Every customer shall be assigned a risk rating.

The rating shall determine:

- level of due diligence;
- level of monitoring;
- escalation requirements.

The CRA shall be applied prior to or during onboarding and throughout the customer relationship.

2.20 Customer Risk Factors

Risk assessments shall consider:

Identity Risk

Reliability of identification.

Jurisdiction Risk

Country of residence and activity.



Behavioural Risk

Gaming and payment behaviour.

Financial Risk

Source of funds concerns.

Sanctions Risk

Potential sanctions exposure.

PEP Risk

Political exposure.

2.21 Low-Risk Customers

Customers may be categorised as lower risk where:

- identity is verified;
- jurisdiction is lower risk;
- activity is consistent;
- no adverse information exists.

2.22 Medium-Risk Customers

Medium-risk customers may require:

- enhanced monitoring;
- periodic review;
- additional documentation.

2.23 High-Risk Customers

Examples include:

- PEPs;
- higher-risk jurisdictions;
- unusual transaction patterns;
- adverse media findings.

High-risk customers shall be subject to Enhanced Due Diligence.



2.24 Dynamic Risk Assessment

Customer risk ratings shall not remain static.

The Company shall reassess risk whenever:

- behaviour changes;
- payment patterns change;
- adverse information emerges;
- regulatory concerns arise.

2.25 Trigger Events

Risk reassessment shall occur following:

- significant deposits;
- significant withdrawals;
- unusual activity;
- sanctions alerts;
- PEP identification.

2.26 Enhanced Monitoring of High-Risk Customers

High-risk customers shall receive enhanced monitoring.

Monitoring may include:

- transaction review;
- payment review;
- source of funds review;
- source of wealth review.

2.27 Risk Assessment Records

The Company shall retain evidence supporting:

- customer risk ratings;
- risk reviews;



- risk escalations;
- risk decisions.

Records shall be available for regulatory inspection.

2.28 Escalation of Risk Concerns

Material risk concerns shall be escalated to the Compliance Officer.

The Compliance Officer may:

- require EDD;
- restrict activity;
- suspend activity;
- recommend termination.

2.29 Management Reporting

The Compliance Officer shall provide reporting regarding:

- customer risk profiles;
- high-risk customer volumes;
- emerging threats;
- jurisdictional risks.

Material concerns shall be escalated.

2.30 Annual Risk Review

The AML Risk Management Framework shall undergo annual review.

The review shall consider:

- regulatory developments;
- internal incidents;
- external threats;
- audit findings.

The results shall be documented and presented to the Board.



PART 3

CUSTOMER ACCEPTANCE POLICY (CAP), CUSTOMER DUE DILIGENCE (CDD), IDENTIFICATION AND VERIFICATION

3.1 Purpose

The purpose of this Part is to establish the policies, procedures and controls governing customer onboarding, customer acceptance, customer identification, customer verification and customer due diligence.

The Company recognises that effective customer due diligence forms the cornerstone of its AML/CFT/CPF programme and is critical to:

- preventing financial crime;
- identifying higher-risk customers;
- supporting transaction monitoring;
- supporting sanctions compliance;
- protecting the integrity of gaming operations;
- complying with legal and regulatory obligations.

No customer relationship shall be established unless the Company is satisfied that the customer has been identified and verified in accordance with this Manual.

3.2 Customer Acceptance Policy

The Company shall maintain a documented Customer Acceptance Policy ("CAP").

The purpose of the CAP is to ensure that the Company only establishes business relationships with customers whose risks can be appropriately identified, understood and managed.

The Company reserves the right to reject, restrict, suspend or terminate any customer relationship where AML, TF, PF, sanctions, fraud or reputational concerns arise.

Acceptance of a customer relationship shall never be automatic.

3.3 Risk-Based Customer Acceptance

Customer acceptance decisions shall be based upon:

- customer risk rating;
- jurisdiction risk;
- sanctions exposure;



- PEP exposure;
- source of funds considerations;
- adverse media findings;
- fraud indicators;
- regulatory restrictions.

Higher-risk customers shall be subject to enhanced scrutiny before acceptance.

3.4 Prohibited Customers

The Company shall not knowingly establish or maintain a business relationship with:

Sanctioned Persons

Any individual or entity subject to applicable sanctions.

Terrorists or Terrorist Organisations

Any known or suspected terrorist or terrorist organisation.

Criminal Organisations

Persons reasonably believed to be engaged in criminal activity.

False Identity Users

Persons providing false, misleading or fraudulent information.

Impersonators

Persons attempting to use another person's identity.

Restricted Jurisdictions

Persons located in jurisdictions prohibited by law, regulation, licence conditions or Company policy.

Persons Failing CDD

Customers who fail to provide required information or documentation.

3.5 Customer Due Diligence Principles

Customer Due Diligence ("CDD") shall be conducted in accordance with:

- applicable laws;
- regulatory requirements;
- licence conditions;



- risk-based principles.

CDD shall seek to establish:

- who the customer is;
 - whether the customer is genuine;
 - whether the customer presents elevated risk;
 - whether the relationship may proceed.
-

3.6 Timing of CDD

CDD shall be conducted:

Before Establishing a Business Relationship

Where required by law or regulation.

Before Processing Certain Transactions

Where required by regulatory obligations.

Upon Trigger Events

Where risk concerns arise.

During Ongoing Monitoring

As part of continuing due diligence.

3.7 Information Collected During Onboarding

The Company shall collect information sufficient to identify and verify the customer.

Information may include:

- full legal name;
- date of birth;
- residential address;
- nationality;
- country of residence;
- email address;
- telephone number.

Additional information may be required according to risk.



3.8 Identification Requirements

The Company shall obtain information necessary to identify the customer.

Information must be:

- complete;
- accurate;
- current;
- consistent.

Customers providing incomplete or inconsistent information may be subject to enhanced review.

3.9 Verification Requirements

The Company shall take reasonable measures to verify customer identity using reliable and independent sources.

Verification may utilise:

- identity documents;
- electronic verification systems;
- trusted databases;
- approved third-party providers.

Verification procedures shall be documented.

3.10 Acceptable Identity Documents

Acceptable documents may include:

Passport

Valid government-issued passport.

National Identity Card

Government-issued identity card.

Residence Permit

Government-issued residence permit.

Other Documents



Other documents approved by the Compliance Officer.

Expired documents shall generally not be accepted unless permitted under documented procedures.

3.11 Address Verification

Where required, address verification may be performed using:

- utility bills;
- bank statements;
- government correspondence;
- electronic verification sources.

The Company may accept alternative evidence where appropriate.

3.12 Electronic Verification

The Company may utilise electronic identity verification solutions.

Electronic verification systems shall:

- utilise reliable sources;
- generate auditable records;
- support regulatory compliance.

Reliance upon electronic verification shall not remove the Company's responsibility for compliance.

3.13 Age Verification

The Company shall take reasonable measures to ensure customers meet applicable age requirements.

Customers who cannot demonstrate eligibility shall not be permitted to use Company services.

Accounts suspected of involving underage persons shall be escalated immediately.

3.14 Verification Failures

Where verification cannot be completed satisfactorily:

- the relationship shall not proceed;
- transactions may be restricted;



- the account may be suspended.

The Compliance Officer may require additional information.

3.15 Customer Risk Profiling

Customers shall be assigned a risk rating as described within the Customer Risk Assessment framework.

Risk ratings shall influence:

- monitoring levels;
- due diligence requirements;
- review frequency.

Risk ratings shall be documented.

3.16 Source of Funds Considerations

The Company shall consider whether source of funds enquiries are required.

Factors include:

- customer risk level;
- transaction activity;
- unusual behaviour;
- jurisdictional concerns.

Source of funds requirements are addressed further in Part 4.

3.17 Politically Exposed Persons

The Company shall determine whether a customer is:

- a Politically Exposed Person ("PEP");
- a family member of a PEP;
- a close associate of a PEP.

PEP screening shall occur during onboarding and periodically thereafter.

PEP relationships shall be subject to Enhanced Due Diligence.

3.18 Sanctions Screening



Customers shall be screened against applicable sanctions lists.

Screening shall occur:

- during onboarding;
- periodically thereafter;
- following material changes.

Potential matches shall be investigated promptly.

3.19 Adverse Media Screening

The Company may conduct adverse media screening.

Adverse media may include information relating to:

- financial crime;
- corruption;
- organised crime;
- sanctions violations;
- terrorism.

Relevant findings shall be assessed by Compliance.

3.20 Ongoing Due Diligence

CDD is not a one-time exercise.

The Company shall maintain ongoing due diligence throughout the customer relationship.

Ongoing due diligence shall include:

- monitoring;
 - reviews;
 - updates;
 - risk reassessment.
-

3.21 Trigger Events Requiring Review

CDD shall be refreshed where:

- customer information changes;



- risk ratings increase;
- unusual activity occurs;
- sanctions alerts occur;
- adverse information emerges.

The Company may require updated documentation.

3.22 Customer Information Updates

Customers may be required to update:

- identity information;
- address information;
- contact information;
- supporting documentation.

Failure to cooperate may result in account restrictions.

3.23 Reliance on Third Parties

The Company may utilise third-party providers to assist with identity verification.

However, responsibility for compliance remains with the Company.

The Company shall maintain oversight of third-party verification providers.

3.24 Failed or Refused Due Diligence

The Company shall not establish or continue a relationship where:

- required information cannot be obtained;
- verification cannot be completed;
- information appears false;
- fraud is suspected.

The Company shall consider whether escalation is required.

3.25 Escalation Procedures

CDD concerns shall be escalated to the Compliance Officer.



Examples include:

- identity discrepancies;
- suspected fraud;
- sanctions concerns;
- adverse media findings.

Escalations shall be documented.

3.26 Customer Restrictions

The Company may apply restrictions where:

- verification remains incomplete;
- additional information is required;
- investigations are ongoing.

Restrictions shall be proportionate to risk.

3.27 Refusal of Business Relationships

The Company reserves the right to reject customers where:

- AML risks cannot be mitigated;
- information is unreliable;
- regulatory concerns exist;
- sanctions concerns exist.

Reasons shall be documented internally.

3.28 Record Keeping

The Company shall retain records relating to:

- customer identification;
- verification;
- risk assessments;
- screening results;
- onboarding decisions.



Records shall be retained in accordance with legal and regulatory requirements.

3.29 Quality Assurance

The Compliance Officer shall periodically review onboarding activities to ensure:

- procedures are followed;
- documentation is complete;
- risk ratings are appropriate.

Deficiencies shall be remediated.

3.30 Management Reporting

Management reporting shall include:

- onboarding statistics;
- verification failures;
- sanctions matches;
- PEP volumes;
- high-risk customer volumes.

Material issues shall be escalated.

3.31 Annual Review

The Customer Acceptance Policy and CDD framework shall be reviewed at least annually.

Reviews shall consider:

- regulatory developments;
- audit findings;
- incidents;
- emerging risks.

Updates shall be approved in accordance with governance requirements.



PART 4

ENHANCED DUE DILIGENCE (EDD), POLITICALLY EXPOSED PERSONS (PEPs), SOURCE OF FUNDS (SOF) AND SOURCE OF WEALTH (SOW)

4.1 Purpose

The purpose of this Part is to establish the enhanced controls that Canary Alley B.V. shall apply to higher-risk customers and higher-risk business relationships.

The Company recognises that certain customers, jurisdictions, behaviours and transaction patterns present elevated risks of:

- money laundering;
- terrorist financing;
- proliferation financing;
- corruption;
- sanctions evasion;
- fraud.

Accordingly, the Company shall apply Enhanced Due Diligence ("EDD") measures where heightened risks are identified.

EDD measures shall be proportionate to the nature and severity of the identified risks.

4.2 EDD Principles

Enhanced Due Diligence shall seek to:

- obtain a deeper understanding of the customer;
- establish legitimacy of funds;
- establish legitimacy of wealth;
- understand the purpose of the relationship;
- identify potential criminal indicators;
- identify sanctions exposure;
- support ongoing monitoring.

EDD shall not be viewed as a one-time event.

EDD relationships shall remain subject to ongoing enhanced monitoring.



4.3 Customers Subject to EDD

EDD shall be applied where the Company identifies elevated risk.

Examples include:

Politically Exposed Persons

PEPs, family members and close associates.

High-Risk Jurisdictions

Customers connected to higher-risk countries.

High-Value Customers

Customers engaging in significant gambling activity.

Complex Ownership Structures

Where beneficial ownership is unclear.

Adverse Media Cases

Customers linked to allegations of financial crime.

Sanctions Concerns

Customers presenting sanctions-related concerns.

Unusual Behaviour

Customers displaying suspicious or unusual activity.

4.4 Trigger Events Requiring EDD

EDD may be triggered by:

- customer risk rating increases;
- unusual deposit patterns;
- unusual withdrawal patterns;
- unusual betting behaviour;
- significant changes in customer activity;
- adverse media findings;
- sanctions alerts;
- regulatory concerns.

The Compliance Officer may require EDD at any time.



POLITICALLY EXPOSED PERSONS

4.5 Definition of a PEP

For the purposes of this Manual, a Politically Exposed Person ("PEP") is an individual who is or has been entrusted with a prominent public function.

Examples may include:

- heads of state;
- ministers;
- members of parliament;
- senior judges;
- senior military officers;
- senior executives of state-owned enterprises;
- senior political party officials.

The definition shall be interpreted in accordance with applicable legal and regulatory requirements.

4.6 Family Members

The Company shall consider whether a customer is a family member of a PEP.

Examples may include:

- spouses;
- partners;
- children;
- parents;
- siblings.

4.7 Close Associates

The Company shall consider whether a customer is a close associate of a PEP.

Examples may include:

- business partners;



- beneficial owners of shared entities;
 - individuals with close business relationships.
-

4.8 PEP Screening

PEP screening shall occur:

During Onboarding

Before acceptance where possible.

During Ongoing Monitoring

At periodic intervals.

Following Trigger Events

Where circumstances change.

Potential matches shall be investigated.

4.9 PEP Risk Assessment

PEP status does not automatically prohibit a relationship.

However, PEP relationships shall be considered high risk unless otherwise determined by the Compliance Officer.

The assessment shall consider:

- position held;
 - jurisdiction;
 - corruption exposure;
 - source of wealth;
 - source of funds.
-

4.10 Approval Requirements for PEPs

Relationships involving PEPs shall require:

- Compliance review;
- Enhanced Due Diligence;
- documented approval.

The approval decision shall be retained.



4.11 Ongoing Monitoring of PEPs

PEP relationships shall be subject to enhanced monitoring.

Monitoring shall include:

- transaction reviews;
- payment reviews;
- behavioural reviews;
- adverse media reviews.

Reviews shall be documented.

SOURCE OF FUNDS

4.12 Purpose of Source of Funds Reviews

The Company shall establish the origin of funds used for gambling where required by risk.

The objective is to determine whether funds originate from legitimate sources.

Source of Funds ("SOF") relates to the specific funds used for gambling activity.

4.13 SOF Triggers

SOF reviews may be required where:

- transaction volumes increase significantly;
- deposits exceed expected levels;
- customer behaviour changes materially;
- risk ratings increase;
- suspicious activity indicators arise.

The Compliance Officer may require SOF at any time.

4.14 Acceptable SOF Evidence

Examples may include:

Employment Income



- payslips;
- employment contracts;
- bank statements.

Business Income

- company accounts;
- dividend statements;
- tax records.

Investments

- investment statements;
- portfolio reports.

Property Transactions

- sale agreements;
- completion statements.

Inheritance

- probate documents;
- estate documentation.

The list is non-exhaustive.

4.15 Assessment of SOF Information

The Company shall assess whether:

- documentation appears authentic;
- documentation is consistent;
- funds are plausible;
- activity aligns with customer profile.

Concerns shall be escalated.

SOURCE OF WEALTH

4.16 Purpose of Source of Wealth Reviews



Source of Wealth ("SOW") relates to the origin of a customer's overall wealth.

SOW seeks to understand how the customer accumulated wealth over time.

4.17 SOW Triggers

SOW reviews may be required for:

- PEPs;
 - very high-value customers;
 - customers presenting elevated risks;
 - customers with unexplained wealth indicators.
-

4.18 Acceptable SOW Evidence

Examples include:

Employment Career

Professional history and earnings.

Business Ownership

Business interests and exits.

Investments

Long-term investment activity.

Property Holdings

Real estate ownership and sales.

Inheritance

Inheritance receipts.

Other Legitimate Sources

Any documented lawful source.

4.19 SOW Assessment

The Company shall determine whether:

- wealth is plausibly explained;
- documentation is consistent;



- information supports the customer profile.

Where concerns remain unresolved, escalation shall occur.

4.20 Inability to Verify SOF or SOW

Where the Company cannot obtain satisfactory SOF or SOW information:

- additional enquiries may be conducted;
- account restrictions may be applied;
- the relationship may be terminated;
- escalation may be required.

The decision shall be documented.

HIGH-RISK JURISDICTIONS

4.21 Higher-Risk Countries

The Company shall identify jurisdictions presenting elevated ML/TF/PF risk.

Sources may include:

- FATF publications;
 - sanctions programmes;
 - governmental advisories;
 - internal risk assessments.
-

4.22 Enhanced Measures for Higher-Risk Jurisdictions

Enhanced measures may include:

- additional verification;
- additional documentation;
- enhanced monitoring;
- management approval.

The level of enhancement shall be proportionate to risk.



ONGOING EDD MONITORING

4.23 Ongoing Monitoring Requirements

EDD customers shall remain subject to enhanced monitoring.

Monitoring shall seek to identify:

- unusual activity;
 - changes in risk;
 - changes in behaviour;
 - adverse information.
-

4.24 Review Frequency

EDD relationships shall be reviewed more frequently than standard-risk relationships.

Review frequency shall be determined by risk.

The Compliance Officer shall establish review schedules.

4.25 Escalation of Concerns

Material concerns identified through EDD shall be escalated immediately.

Escalations may result in:

- additional due diligence;
 - account restrictions;
 - transaction restrictions;
 - suspicious activity review.
-

4.26 Documentation Requirements

EDD files shall contain:

- rationale for EDD;
- documentation obtained;
- reviews conducted;
- approvals;



- monitoring outcomes.

Files shall be retained for audit and regulatory purposes.

4.27 Record Keeping

The Company shall retain:

- PEP assessments;
- SOF reviews;
- SOW reviews;
- EDD approvals;
- monitoring records.

Retention shall comply with applicable requirements.

4.28 Management Reporting

The Compliance Officer shall provide reporting regarding:

- PEP relationships;
- EDD relationships;
- SOF reviews;
- SOW reviews;
- unresolved concerns.

Material matters shall be escalated.

4.29 Annual Review

The EDD framework shall be reviewed annually.

The review shall consider:

- regulatory developments;
- audit findings;
- emerging risks;
- industry guidance.

Updates shall be documented and approved.



PART 5

SANCTIONS COMPLIANCE, ASSET FREEZING AND PROLIFERATION FINANCING CONTROLS

5.1 Purpose

The purpose of this Part is to establish the framework through which Canary Alley B.V. identifies, prevents, detects and manages sanctions, proliferation financing ("PF") and sanctions evasion risks.

The Company recognises that sanctions compliance is a fundamental component of its AML/CFT/CPF obligations and forms an essential element of its regulatory responsibilities under Curaçao law and applicable international standards.

The Company shall maintain systems and controls designed to prevent its products and services from being used:

- by sanctioned individuals or entities;
 - to facilitate sanctions evasion;
 - to support proliferation financing;
 - to support terrorist financing;
 - to support other prohibited financial activity.
-

5.2 Sanctions Policy Statement

Canary Alley B.V. shall not knowingly:

- establish or maintain a relationship with a sanctioned person;
- process transactions involving sanctioned persons;
- facilitate transactions prohibited by sanctions laws;
- facilitate sanctions evasion;
- facilitate proliferation financing.

The Company shall take immediate action where sanctions concerns are identified.

5.3 Risk-Based Sanctions Framework

The Company shall maintain a sanctions compliance framework incorporating:

- sanctions screening;
- sanctions investigations;



- escalation procedures;
- asset freezing procedures;
- ongoing monitoring;
- employee training;
- record keeping.

The framework shall be reviewed periodically.

5.4 Responsibility for Sanctions Compliance

The Compliance Officer shall be responsible for:

- sanctions oversight;
- sanctions investigations;
- sanctions escalations;
- sanctions reporting;
- sanctions training.

Ultimate responsibility remains with the Board.

5.5 Applicable Sanctions Programmes

The Company shall maintain awareness of sanctions programmes applicable to its operations.

The Company may consider sanctions information originating from:

- United Nations;
- European Union;
- Kingdom of the Netherlands;
- Curaçao authorities;
- other applicable competent authorities.

The Compliance Officer shall determine which sanctions programmes apply.

SANCTIONS SCREENING

5.6 Customer Screening



All customers shall be screened against applicable sanctions lists.

Screening shall occur:

At Onboarding

Before acceptance where possible.

During Ongoing Monitoring

Periodic re-screening.

Following Trigger Events

Where circumstances change.

5.7 Screening of Existing Customers

The Company shall periodically screen existing customers.

The frequency of screening shall be determined by risk.

Higher-risk customers may be screened more frequently.

5.8 Screening Data

Screening shall utilise information including:

- name;
- date of birth;
- nationality;
- country of residence;
- other identifying information.

The objective is to improve match accuracy.

5.9 Payment Screening

The Company shall assess whether sanctions controls should be applied to:

- deposits;
- withdrawals;
- payment instruments;
- counterparties.



Payment-related concerns shall be escalated.

5.10 Supplier Screening

The Company may conduct sanctions screening of:

- suppliers;
- service providers;
- business partners.

Higher-risk suppliers shall receive enhanced scrutiny.

5.11 Employee Screening

Where appropriate and legally permissible, sanctions screening may be conducted for:

- employees;
- contractors;
- consultants.

Results shall be handled confidentially.

SANCTIONS MATCH MANAGEMENT

5.12 Potential Match Identification

Potential sanctions matches shall be investigated promptly.

The existence of a potential match does not automatically mean a true match exists.

Investigation shall be conducted before a determination is made.

5.13 False Positives

The Company recognises that screening systems may generate false positives.

Investigations shall consider:

- identifying information;
- supporting documentation;
- risk factors.



False positives shall be documented.

5.14 True Matches

Where a true sanctions match is identified, the Company shall immediately escalate the matter to the Compliance Officer.

No further activity shall be permitted without appropriate review.

5.15 Escalation Procedures

The Compliance Officer shall determine:

- whether a true match exists;
- whether restrictions are required;
- whether reporting obligations arise;
- whether account suspension is required.

All decisions shall be documented.

ASSET FREEZING

5.16 Asset Freezing Obligations

Where required by applicable law, regulation or sanctions obligations, the Company shall implement asset freezing measures.

The objective is to prevent:

- access to funds;
 - movement of funds;
 - withdrawal of funds;
 - indirect benefit from frozen assets.
-

5.17 Immediate Actions

Where a freezing obligation arises, the Company may:

- suspend the account;
- block withdrawals;



- restrict transactions;
- preserve records.

Actions shall be documented.

5.18 Preservation of Evidence

The Company shall preserve:

- account information;
- transaction records;
- communications;
- investigation records.

Evidence shall be retained securely.

5.19 Confidentiality

Sanctions investigations shall remain confidential.

Personnel must not:

- disclose investigations;
- disclose reporting activity;
- alert customers to investigations.

Unauthorised disclosure may constitute tipping-off.

PROLIFERATION FINANCING

5.20 Proliferation Financing Policy

The Company recognises that proliferation financing risks may arise through attempts to support the development, acquisition or movement of weapons of mass destruction.

The Company shall maintain controls proportionate to its PF risk exposure.

5.21 PF Risk Assessment

PF risks shall form part of the Business Risk Assessment.

Factors shall include:



- jurisdictional exposure;
- customer exposure;
- sanctions exposure;
- payment risks.

The assessment shall be reviewed periodically.

5.22 PF Indicators

Examples of PF indicators may include:

- sanctions-related concerns;
- unusual payment patterns;
- unusual geographical links;
- attempts to obscure beneficial ownership.

Indicators shall be assessed on a risk basis.

5.23 PF Escalations

Potential PF concerns shall be escalated immediately to the Compliance Officer.

Escalations shall be documented.

The Compliance Officer shall determine whether further action is required.

ONGOING SANCTIONS MONITORING

5.24 Ongoing Monitoring

The Company shall monitor for:

- sanctions changes;
- new designations;
- geopolitical developments;
- regulatory developments.

Monitoring activities shall support ongoing compliance.



5.25 Rescreening Following List Updates

Where sanctions lists are updated, the Company may conduct rescreening activities.

The extent of rescreening shall be determined by risk.

5.26 Higher-Risk Jurisdictions

The Company shall maintain awareness of jurisdictions presenting elevated sanctions or PF risks.

Such jurisdictions may require:

- enhanced due diligence;
 - enhanced monitoring;
 - additional approvals.
-

TRAINING AND AWARENESS

5.27 Sanctions Training

Relevant personnel shall receive sanctions training.

Training shall cover:

- sanctions obligations;
- sanctions screening;
- escalation procedures;
- tipping-off risks.

Training records shall be retained.

5.28 Compliance Officer Training

The Compliance Officer shall maintain appropriate knowledge regarding:

- sanctions developments;
- PF developments;
- regulatory expectations.

Training shall be documented.



RECORD KEEPING

5.29 Record Retention

The Company shall retain records relating to:

- sanctions screening;
- investigations;
- false positives;
- true matches;
- asset freezing actions;
- PF investigations.

Records shall be retained in accordance with legal requirements.

5.30 Sanctions Register

The Compliance Officer shall maintain a Sanctions Register.

The register shall include:

- case reference;
- date identified;
- customer reference;
- outcome;
- actions taken.

The register shall be available for inspection.

REPORTING

5.31 Management Reporting

The Compliance Officer shall provide periodic reporting regarding:

- sanctions alerts;
- sanctions investigations;
- PF concerns;



- unresolved cases.

Material concerns shall be escalated promptly.

5.32 Board Reporting

The Board shall receive periodic information regarding:

- sanctions risks;
- sanctions incidents;
- PF risks;
- material developments.

The Board shall ensure adequate oversight.

5.33 Annual Review

The sanctions and PF framework shall be reviewed annually.

The review shall consider:

- regulatory developments;
- sanctions developments;
- audit findings;
- industry guidance.

Updates shall be documented and approved.



PART 6

TRANSACTION MONITORING, ONGOING MONITORING, UNUSUAL TRANSACTIONS, SUSPICIOUS ACTIVITY AND REPORTING TO THE FIU

6.1 Purpose

The purpose of this Part is to establish the framework through which Canary Alley B.V. identifies, investigates, escalates and reports potentially suspicious or unusual activity.

The Company recognises that effective monitoring and reporting are critical components of an AML/CFT/CPF programme and are essential for:

- detecting financial crime;
- identifying suspicious activity;
- protecting the integrity of gaming operations;
- supporting regulatory compliance;
- supporting competent authorities.

The Company shall maintain systems and controls proportionate to its risk profile and business model.

6.2 Monitoring Objectives

The Company's monitoring programme shall seek to:

- identify unusual activity;
- identify suspicious activity;
- identify sanctions concerns;
- identify fraud indicators;
- identify ML/TF/PF risks;
- identify changes in customer behaviour.

Monitoring shall be both automated and manual where appropriate.

6.3 Risk-Based Monitoring

Monitoring activities shall be proportionate to risk.

Higher-risk customers shall be subject to enhanced monitoring.

Risk factors include:



- customer risk rating;
 - jurisdiction;
 - payment methods;
 - transaction values;
 - behavioural indicators;
 - source of funds concerns.
-

6.4 Responsibility for Monitoring

The Compliance Officer shall oversee:

- monitoring frameworks;
- alert management;
- investigations;
- reporting.

Operational teams shall support monitoring activities and escalate concerns promptly.

ONGOING CUSTOMER MONITORING

6.5 Ongoing Due Diligence

The Company shall conduct ongoing due diligence throughout the customer relationship.

Ongoing monitoring shall ensure:

- customer information remains current;
- activity remains consistent with the customer's profile;
- risk ratings remain appropriate.

Monitoring shall not cease after onboarding.

6.6 Customer Behaviour Reviews

The Company shall review customer behaviour to identify unusual activity.

Reviews may consider:

- deposits;



- withdrawals;
- betting activity;
- account usage;
- payment methods;
- device usage.

Material deviations from expected behaviour shall be investigated.

6.7 Risk-Based Reviews

The frequency of customer reviews shall be determined by risk.

Low Risk

Periodic review.

Medium Risk

Enhanced periodic review.

High Risk

Frequent review and enhanced monitoring.

EDD Customers

Ongoing enhanced review.

6.8 Trigger-Based Reviews

Customer reviews shall be performed following trigger events.

Examples include:

- significant deposits;
 - significant withdrawals;
 - unusual activity;
 - adverse media findings;
 - sanctions alerts;
 - PEP identification.
-

TRANSACTION MONITORING



6.9 Transaction Monitoring Framework

The Company shall maintain transaction monitoring controls designed to identify potentially unusual or suspicious activity.

Monitoring may include:

- automated rules;
- manual reviews;
- behavioural analysis;
- exception reporting.

6.10 Monitoring Scope

Monitoring shall cover:

Deposits

Incoming payments.

Withdrawals

Outgoing payments.

Gaming Activity

Customer betting activity.

Account Activity

Changes to customer profiles.

Payment Behaviour

Use of payment methods.

6.11 Monitoring Scenarios

The Company shall maintain monitoring scenarios appropriate to its risk profile.

Examples include:

- unusual deposit activity;
- unusual withdrawal activity;
- rapid movement of funds;
- inconsistent gambling activity;



- unusual account behaviour.

Monitoring scenarios shall be reviewed periodically.

6.12 Velocity Monitoring

The Company may monitor transaction frequency.

Examples include:

- multiple deposits within a short period;
- multiple withdrawals within a short period;
- unusual changes in transaction frequency.

6.13 Value-Based Monitoring

The Company may monitor transaction values.

Examples include:

- significant deposits;
- significant withdrawals;
- activity inconsistent with customer profile.

6.14 Payment Method Monitoring

The Company shall monitor use of payment methods.

Indicators may include:

- multiple payment methods;
- unusual payment patterns;
- payment ownership concerns.

6.15 Withdrawal Monitoring

Withdrawals shall be subject to monitoring.

Indicators may include:

- withdrawals inconsistent with gambling activity;
- unusual withdrawal requests;



- rapid withdrawal behaviour.

6.16 Gambling Behaviour Monitoring

Monitoring shall consider whether gambling activity appears consistent with legitimate gambling behaviour.

Examples of concern may include:

- minimal gameplay relative to deposits;
- activity inconsistent with customer profile;
- activity lacking a reasonable commercial rationale.

The Company shall avoid prescriptive assumptions and assess cases holistically.

6.17 Geographical Monitoring

Monitoring may identify activity involving:

- higher-risk jurisdictions;
- unusual geographical connections;
- sanctions concerns.

Relevant findings shall be reviewed.

6.18 Device and Access Monitoring

Monitoring may include review of:

- unusual device usage;
- account sharing indicators;
- unusual access patterns.

Findings shall be assessed appropriately.

ALERT MANAGEMENT

6.19 Alert Generation

Monitoring activities may generate alerts.

Alerts may arise from:



- automated systems;
- manual reviews;
- customer interactions;
- supplier notifications.

6.20 Alert Triage

Alerts shall be reviewed promptly.

The reviewer shall determine whether:

- the alert can be closed;
- additional information is required;
- escalation is required.

The rationale shall be documented.

6.21 Alert Investigation

Investigations shall seek to establish:

- the nature of the activity;
- customer explanations;
- supporting evidence;
- risk implications.

Investigations shall be proportionate to risk.

6.22 Documentation of Investigations

The Company shall document:

- alert details;
- investigative steps;
- findings;
- conclusions;
- actions taken.

Records shall be retained.



UNUSUAL TRANSACTIONS

6.23 Unusual Transaction Framework

The Company shall maintain procedures for identifying and assessing unusual transactions.

An unusual transaction is a transaction or activity that deviates from expected behaviour or otherwise gives rise to concern.

Not every unusual transaction is suspicious.

However, every unusual transaction shall be assessed appropriately.

6.24 Indicators of Unusual Activity

Indicators may include:

- unusual transaction values;
- unusual frequency;
- unusual payment behaviour;
- unusual account activity;
- unusual jurisdictional connections.

The list is illustrative rather than exhaustive.

6.25 Internal Escalation

Employees identifying unusual activity shall escalate the matter to Compliance promptly.

Escalations shall be documented.

SUSPICIOUS ACTIVITY

6.26 Definition of Suspicious Activity

Suspicious activity is activity that gives rise to knowledge, suspicion or reasonable grounds to suspect that:

- criminal property may be involved;
- money laundering may be occurring;



- terrorist financing may be occurring;
- sanctions evasion may be occurring;
- proliferation financing may be occurring.

6.27 Suspicious Activity Indicators

Examples may include:

Customer Behaviour

- refusal to provide information;
- provision of misleading information;
- attempts to circumvent controls.

Transaction Behaviour

- activity inconsistent with profile;
- unexplained movement of funds;
- unusual transaction structures.

Other Indicators

- sanctions concerns;
- adverse media concerns;
- fraud indicators.

The list is not exhaustive.

6.28 Internal Suspicious Activity Reports

Employees shall submit internal reports to the Compliance Officer where suspicion exists.

Reports shall include:

- customer details;
- activity details;
- reasons for concern;
- supporting evidence.

Internal reports shall remain confidential.



6.29 Compliance Officer Assessment

The Compliance Officer shall assess:

- facts;
- evidence;
- explanations;
- risk indicators.

The assessment shall be documented.

6.30 Escalation Outcomes

Following review, the Compliance Officer may:

- close the matter;
 - seek additional information;
 - conduct further investigation;
 - apply restrictions;
 - determine reporting obligations.
-

REPORTING TO THE FIU

6.31 Reporting Obligations

The Company shall comply with applicable unusual transaction and suspicious activity reporting obligations.

The Compliance Officer shall determine whether external reporting is required.

6.32 Reporting Decisions

Reporting decisions shall be based upon:

- facts available;
- risk indicators;
- legal obligations;
- regulatory guidance.

Decisions shall be documented.



6.33 FIU Reporting

Where reporting obligations arise, reports shall be submitted to the competent authority using approved reporting mechanisms.

Reports shall be submitted by authorised personnel only.

6.34 Record Keeping

The Company shall retain:

- internal reports;
- investigation records;
- supporting evidence;
- reporting records.

Retention shall comply with legal requirements.

TIPPING-OFF

6.35 Tipping-Off Prohibition

Personnel must not disclose:

- that a report has been submitted;
- that an investigation is underway;
- that authorities have been notified.

This prohibition applies to:

- customers;
- third parties;
- unauthorised employees.

6.36 Confidentiality Requirements

Monitoring and investigation activities shall remain confidential.

Access shall be restricted to authorised personnel.



ACCOUNT RESTRICTIONS

6.37 Risk-Based Restrictions

The Company may apply restrictions where concerns arise.

Restrictions may include:

- temporary suspension;
- withdrawal restrictions;
- account review requirements;
- additional due diligence.

Restrictions shall be proportionate and documented.

6.38 Relationship Termination

The Company may terminate a customer relationship where:

- risks cannot be mitigated;
- due diligence cannot be completed;
- regulatory concerns arise.

Termination decisions shall be documented.

MANAGEMENT INFORMATION

6.39 Monitoring Metrics

The Compliance Officer shall maintain metrics relating to:

- alerts generated;
 - alerts closed;
 - investigations conducted;
 - unusual transactions identified;
 - reports submitted.
-

6.40 Management Reporting



Management reporting shall include:

- monitoring effectiveness;
- alert volumes;
- investigation outcomes;
- suspicious activity trends;
- emerging risks.

Material issues shall be escalated.

6.41 Board Reporting

The Board shall receive periodic reporting regarding:

- significant cases;
- monitoring effectiveness;
- AML risks;
- regulatory developments.

6.42 Annual Review

The transaction monitoring and reporting framework shall be reviewed annually.

The review shall consider:

- regulatory developments;
- audit findings;
- emerging risks;
- industry guidance;
- effectiveness of controls.



PART 7

RECORD KEEPING, EMPLOYEE SCREENING, AML TRAINING, INDEPENDENT AML AUDIT, COMPLIANCE TESTING, MANAGEMENT REPORTING AND ANNUAL AML REVIEW

7.1 Purpose

The purpose of this Part is to establish the framework through which Canary Alley B.V. ensures that:

- AML records are properly maintained;
- employees are appropriately screened;
- AML training is delivered and documented;
- AML controls are independently tested;
- AML compliance is monitored;
- management receives appropriate AML reporting;
- the AML programme is subject to continuous improvement.

The Company recognises that even well-designed AML controls can become ineffective without proper oversight, testing and review.

RECORD KEEPING

7.2 Record Keeping Principles

The Company shall maintain complete, accurate and retrievable records sufficient to demonstrate compliance with:

- LOK;
- NOIS;
- NORUT;
- AML/CFT/CPF Regulations;
- Licence Conditions;
- Regulatory Guidance;
- Internal Policies.

Records shall be capable of supporting:

- regulatory inspections;



- audits;
- investigations;
- law enforcement requests;
- internal reviews.

7.3 Responsibility for Record Keeping

The Compliance Officer shall oversee AML record retention.

Operational departments shall ensure that records generated within their functions are:

- accurate;
- complete;
- accessible;
- retained appropriately.

7.4 Customer Due Diligence Records

The Company shall retain records relating to:

- customer identification;
- customer verification;
- customer risk ratings;
- sanctions screening;
- PEP screening;
- adverse media screening;
- Source of Funds reviews;
- Source of Wealth reviews;
- EDD reviews.

7.5 Transaction Records

The Company shall retain records relating to:

- deposits;
- withdrawals;



- transfers;
- account activity;
- gaming activity;
- financial transactions.

Transaction records shall be sufficient to permit reconstruction of activity.

7.6 Monitoring Records

The Company shall retain records relating to:

- alerts;
 - investigations;
 - monitoring reviews;
 - escalations;
 - decisions.
-

7.7 Reporting Records

The Company shall retain records relating to:

- internal suspicious activity reports;
 - unusual transaction assessments;
 - FIU reports;
 - sanctions investigations;
 - regulatory communications.
-

7.8 Training Records

The Company shall maintain records relating to:

- training attendance;
 - training completion;
 - assessment results;
 - training materials.
-



7.9 Audit Records

The Company shall maintain records relating to:

- audits;
 - compliance reviews;
 - testing activities;
 - corrective actions.
-

7.10 Retention Periods

AML records shall be retained for at least the minimum period required by applicable law and regulation.

Where multiple retention periods apply, the longest applicable period shall generally be applied unless otherwise determined by the Compliance Officer.

7.11 Record Security

AML records shall be protected against:

- unauthorised access;
- loss;
- destruction;
- alteration.

Access shall be restricted to authorised personnel.

EMPLOYEE SCREENING

7.12 Employee Integrity Standards

The Company recognises that personnel integrity is fundamental to effective AML compliance.

The Company shall take reasonable measures to assess the suitability of individuals performing AML-sensitive functions.

7.13 Pre-Employment Screening

The Company shall conduct risk-based screening before employment or engagement.

Screening may include:



- identity verification;
- employment history verification;
- reference checks;
- qualification verification;
- sanctions screening.

Screening shall be proportionate to the role.

7.14 Screening of Compliance Personnel

Personnel performing AML functions may be subject to enhanced screening.

The objective is to ensure:

- competence;
 - integrity;
 - trustworthiness.
-

7.15 Ongoing Screening

Where appropriate, the Company may conduct ongoing screening of employees.

Material concerns shall be escalated.

7.16 Employee Disclosure Obligations

Employees shall promptly disclose circumstances that may affect their suitability.

Examples include:

- criminal proceedings;
- sanctions issues;
- regulatory concerns.

Disclosures shall be reviewed appropriately.

AML TRAINING

7.17 AML Training Programme



The Company shall maintain a documented AML training programme.

The programme shall be proportionate to:

- business activities;
 - regulatory requirements;
 - identified risks.
-

7.18 Training Objectives

Training shall seek to ensure that personnel:

- understand AML obligations;
 - understand Company procedures;
 - recognise suspicious activity;
 - understand escalation procedures;
 - understand reporting obligations.
-

7.19 Induction Training

New personnel shall receive AML training as part of onboarding.

Training shall occur before or shortly after access to systems is granted.

7.20 Annual Refresher Training

Personnel shall receive AML refresher training at least annually.

Training shall address:

- emerging risks;
 - regulatory developments;
 - policy changes;
 - lessons learned.
-

7.21 Role-Specific Training

Additional training shall be provided for:

Compliance Personnel



Advanced AML requirements.

Customer Support Personnel

Customer interaction and escalation.

Payment Personnel

Payment-related risk indicators.

Senior Management

Governance and oversight responsibilities.

7.22 Compliance Officer Training

The Compliance Officer shall maintain current knowledge regarding:

- legislation;
- regulations;
- typologies;
- industry developments.

Professional development activities shall be documented.

7.23 Training Content

Training may include:

- AML fundamentals;
 - terrorist financing;
 - proliferation financing;
 - sanctions;
 - suspicious activity indicators;
 - tipping-off risks;
 - customer due diligence.
-

7.24 Training Assessments

The Company may require personnel to complete assessments.

Assessment results shall be retained.



INDEPENDENT AML AUDIT

7.25 Independent Review Requirement

The AML programme shall be subject to independent review.

The objective is to assess whether:

- controls are adequate;
 - controls operate effectively;
 - deficiencies exist.
-

7.26 Scope of Independent Reviews

Reviews may cover:

- governance;
 - risk assessments;
 - CDD;
 - EDD;
 - sanctions compliance;
 - transaction monitoring;
 - reporting;
 - training.
-

7.27 Independence Requirements

Reviews shall be performed by persons sufficiently independent from the activities being assessed.

Independence shall be documented.

7.28 Audit Frequency

Independent AML reviews shall occur periodically.

Frequency shall be determined according to:

- risk profile;



- regulatory expectations;
 - business complexity.
-

7.29 Audit Findings

Findings shall be categorised according to risk.

Categories may include:

- Critical;
 - High;
 - Medium;
 - Low.
-

7.30 Corrective Actions

Audit findings shall result in documented corrective actions.

Actions shall include:

- ownership;
 - deadlines;
 - progress tracking.
-

COMPLIANCE TESTING

7.31 Compliance Monitoring Programme

The Compliance Officer shall maintain a compliance monitoring programme.

Monitoring shall assess adherence to:

- AML policies;
 - procedures;
 - regulatory requirements.
-

7.32 Thematic Reviews

Compliance may conduct thematic reviews covering:



- onboarding;
- source of funds;
- sanctions screening;
- transaction monitoring.

Findings shall be documented.

7.33 File Reviews

The Company shall conduct periodic reviews of customer files.

Reviews shall assess:

- completeness;
 - accuracy;
 - appropriateness of risk ratings;
 - compliance with procedures.
-

7.34 Quality Assurance Reviews

Quality assurance reviews shall seek to identify:

- procedural weaknesses;
- training needs;
- recurring errors.

Corrective actions shall be documented.

MANAGEMENT REPORTING

7.35 AML Management Information

The Compliance Officer shall maintain AML Management Information ("MI").

MI shall support:

- risk management;
- decision-making;
- regulatory compliance.



7.36 AML Metrics

Metrics may include:

- customer volumes;
- high-risk customer volumes;
- PEP volumes;
- EDD volumes;
- alerts generated;
- investigations conducted;
- reports submitted.

7.37 Compliance Reporting

The Compliance Officer shall provide periodic reporting to Senior Management.

Reports shall address:

- emerging risks;
- monitoring outcomes;
- sanctions issues;
- audit findings;
- regulatory developments.

7.38 Board Reporting

The Board shall receive AML reporting at least annually and more frequently where appropriate.

Reports shall include:

- risk assessments;
 - significant incidents;
 - audit findings;
 - control effectiveness;
 - resource requirements.
-



ANNUAL AML REVIEW

7.39 Annual AML Programme Review

The Compliance Officer shall conduct an annual review of the AML programme.

The review shall assess:

- effectiveness;
 - adequacy;
 - compliance;
 - emerging risks.
-

7.40 Review Inputs

The annual review shall consider:

- Business Risk Assessment;
 - Customer Risk Assessment;
 - audit findings;
 - monitoring outcomes;
 - sanctions developments;
 - regulatory developments;
 - industry guidance.
-

7.41 Annual AML Report

The Compliance Officer shall prepare an Annual AML Report.

The report shall include:

Governance

AML framework status.

Risk Assessment

Current risk profile.

Monitoring

Monitoring outcomes.



Reporting

Regulatory reporting activity.

Audit

Audit and review findings.

Recommendations

Recommended improvements.

7.42 Board Approval

The Board shall review:

- the Annual AML Report;
- the Business Risk Assessment;
- material policy updates.

Board decisions shall be documented.

7.43 Continuous Improvement

The AML programme shall be subject to continuous improvement.

Improvements may arise from:

- audits;
 - inspections;
 - incidents;
 - regulatory developments;
 - emerging risks.
-

7.44 Policy Review

This Manual shall be reviewed:

- annually;
- following regulatory change;
- following material business change;
- following significant incidents.

Updates shall be approved through governance procedures.