

Know Your Customer (KYC) Policy

Corporate issue - Version 1.3

Operator	New Origin B.V.
Brand / Domain	ohmywin.com (and associated domains)
Jurisdiction	Curaçao (B2C licence application)
Document	Know Your Customer (KYC) Policy
Version	1.3
Effective date	25 May 2026

This standalone policy sets out the minimum KYC standards applicable to New Origin B.V. and is intended to remain consistent with the Operator's AML/CFT, responsible gaming, complaints, payment, and customer terms framework. English version prevails.

1. Purpose & Scope

This Policy defines the minimum KYC standards that apply to all relevant customer, internal company, and counterparty touchpoints of New Origin B.V. It is designed to support compliance with Curaçao licensing expectations, applicable AML/CFT requirements, sanctions obligations, and responsible gaming safeguards, while retaining the greatest possible commercial flexibility permitted by law.

It complements and must be read together with the **Terms & Conditions, AML/CFT Policy and Procedures, Responsible Gaming Policy, Information Security Policy, Privacy Policy, and Complaints Policy.**

- all natural persons who open or attempt to open an account and/or use the services;
- the Operator's internal company due diligence and governance records;
- relevant counterparties, vendors, PSPs, platform providers, affiliates, consultants, and other business partners where due diligence is appropriate;
- all relevant staff, contractors, and outsourced providers involved in onboarding, customer operations, payments, fraud prevention, compliance, or reporting.

2. Regulatory Context

This Policy has been prepared for Curaçao licensing purposes and reflects the Operator's current understanding of the practical expectations applicable to a **standalone KYC Policy**. It is intended to reflect the Operator's actual onboarding flow, monitoring process, thresholds, systems, service providers, and internal responsibilities.

The Policy follows a risk-based approach and should be interpreted consistently with:

- applicable Curaçao licensing and AML/CFT obligations;
- applicable sanctions frameworks;
- the Operator's AML/CFT Policy and Procedures;
- internal compliance controls and responsible gaming safeguards; and
- data protection obligations applicable to relevant customers and markets.

3. Definitions

Customer: any natural person who opens an account, attempts to open an account, or uses the Operator's services.

Counterparty: any external business party relevant to the Operator's operations, including PSPs, platform vendors, suppliers, affiliates, consultants, and other third parties where due diligence is required.

Standard CDD: identity verification and supporting checks carried out based on risk and/or when a trigger is reached.

EDD: enhanced due diligence applied to higher-risk customers or counterparties, including where PEP, sanctions, source of funds, unusual activity, or crypto-related concerns arise.

Documentary evidence: may include government-issued photo ID, proof of address, payment method ownership evidence, source of funds / source of wealth evidence, and any other reasonably requested documents.

Threshold: the cumulative deposit threshold of XCG 4,000 (or currency equivalent), at which additional KYC controls apply.

4. Risk-Based Approach

Risk is assessed across four main dimensions:

- customer profile, including identity information, age and eligibility, occupation where relevant, public profile, linked-account indicators, adverse media, and whether the customer presents characteristics associated with higher fraud, AML/CFT, or responsible gaming risk;
- geography, including country of residence, country of access, payment-routing geography, sanctioned or restricted jurisdictions, FATF-related risk, and any other location factor relevant to legal, regulatory, fraud, or AML/CFT exposure;
- product and behavioural risk, including the type of products used, intensity and pattern of play, unusual or inconsistent activity, reversed withdrawals, device or IP anomalies, bonus abuse indicators, and any behaviour suggesting elevated fraud, AML/CFT, or responsible gaming risk; and
- funding and payment method risk, including source and ownership of funds, type of payment method used, multiple payment-method changes, third-party funding indicators, wallet or crypto-related concerns, chargeback patterns, and any inconsistency between the customer profile and the payment behaviour.

Risk ratings drive the depth of CDD/EDD, the frequency of review, the type of supporting documentation requested, the level of escalation and approval required, and any restriction, suspension, or termination decision.

Customers and counterparties outside accepted risk appetite may be refused, restricted, suspended, or terminated.

5. On-Boarding & Early-Stage Controls

Registration

At registration, customers must provide, at a minimum, their full name, permanent residential address, and date of birth, together with any other mandatory onboarding fields required by the Operator's registration flow.

The onboarding process is designed to remain commercially efficient while applying minimum legal and risk-based safeguards. Automated controls may include age and eligibility checks, IP and geo checks, device fingerprinting, fraud and duplication checks, and automated sanctions / PEP screening triggers where supported.

As a general rule, documentary KYC is not requested at registration unless an alert, inconsistency, legal requirement, or risk trigger justifies earlier intervention.

These minimum registration details are collected before the account is opened, without prejudice to any later documentary verification required under this Policy.

Unverified Accounts

Unverified accounts are capped at 50 EUR/USD (or currency equivalent) in total deposits and no withdrawals are permitted. The Operator may apply stricter controls where required by law, risk scoring, sanctions / PEP alerts, payment method concerns, fraud indicators, or AML/CFT considerations.

Initial Deposit

At first funding, the Operator may run automated sanctions, PEP, fraud, velocity, device, and payment checks. Deposits may be accepted unless a positive hit, material alert, or internal block is triggered.

First Withdrawal

Before the first withdrawal is released, the customer must normally provide valid photo ID and proof of address. Evidence of payment method ownership may also be requested where justified by risk, including where the payment method is inconsistent with the customer profile, does not clearly appear to be in the customer's own name, has changed repeatedly, or otherwise gives rise to concern.

Additional documents may be requested earlier where justified by risk.

6. Responsibility & Governance

The Operator maintains a lean but clearly segregated KYC governance structure designed to ensure effective oversight, operational efficiency, and compliance with applicable AML/CFT, sanctions, and licensing requirements.

Managing Directors / Board-level management retain ultimate accountability for the effectiveness of the KYC framework, the Operator's risk appetite, and the resourcing and independence of control functions. The Managing Director is responsible for final decision-making in material high-risk cases, confirmed PEP cases, significant exceptions, and termination decisions.

Customer Operations / Customer Support function, including the Customer Support Lead and any approved BPO support arrangement, is responsible for the day-to-day operational handling of customer KYC matters, including customer contact, document requests, reminders, collection of KYC information, communication of account restrictions, and escalation of non-standard cases.

Payments & Risk function, led by the Operator's Payments & Risk Owner and supported where applicable by outsourced payment operations under SLAs, is responsible for operational threshold controls, payment-method related reviews, withdrawal restrictions linked to KYC status, payment ownership issues, and escalation of unusual payment behaviour, multiple payment-method changes, or other payment-related red flags. The Operator remains fully responsible for compliance, oversight, and final decision-making.

Compliance Officer, appointed by the Operator and, at launch, expected to be outsourced via Allyant Group B.V. consistent with the Operator's Business Plan, is responsible for day-to-day KYC oversight, review of non-standard or higher-risk cases, review of escalations from Customer Operations / Payments / Risk, approval of enhanced due diligence measures in routine high-risk cases, policy maintenance, control review, and internal reporting. The Compliance Officer does not perform front-line operational customer support functions.

MLRO, appointed by the Operator and, at launch, expected to be outsourced via Allyant Group B.V. consistent with the Operator's Business Plan, is responsible for suspicious matter assessment, review of sanctions escalations, confirmed or suspected AML/CFT concerns, freezing / reporting decisions where legally required, liaison with competent authorities, and maintenance of relevant internal reporting and escalation records.

At launch, the Compliance Officer and MLRO functions are intended to be outsourced via Allyant Group B.V., with the named natural person(s) to be formally appointed prior to go-live. These functions must remain sufficiently senior, independent from operational roles, and capable of discharging the relevant responsibilities effectively.

The roles of Compliance Officer and MLRO are treated as distinct control functions. At the launch stage, both roles may be performed by the same appropriately appointed external person, provided that such person is sufficiently senior, independent from operational functions, and able to discharge both responsibilities effectively.

Approved service providers / vendors may perform elements of screening, document collection, operational payment handling, or verification support, but the Operator remains ultimately responsible for compliance, oversight, and final decision-making.

Escalation principles

Standard KYC cases are handled operationally by Customer Operations / Customer Support and Payments & Risk in accordance with this Policy and the Operator's procedures.

Non-standard or higher-risk KYC cases are escalated to the Compliance Officer.

Suspected AML/CFT matters, sanctions alerts, confirmed or suspected true matches, freezing cases, and reporting considerations are escalated without delay to the MLRO.

Material high-risk cases, confirmed PEP cases, significant exceptions, and termination decisions are escalated to the Managing Director for final decision.

High-risk matters, material EDD concerns, account termination proposals, and other significant escalations must be documented, together with the rationale for the decision taken.

7. Timing of Customer Due Diligence

CDD/KYC may be performed:

- at onboarding, where risk triggers, legal requirements, or system alerts justify this;
- prior to the first withdrawal;
- once the cumulative deposit threshold of XCG 4,000 is reached;
- where unusual or inconsistent activity is detected;
- where customer information becomes outdated or incomplete;
- where the customer's risk profile changes;
- where a PEP, sanctions, fraud, or adverse media trigger arises;
- where source of funds or source of wealth needs to be verified; and
- during periodic or event-driven ongoing monitoring.

As a general rule, the Operator applies a commercially light onboarding model and requests documentary KYC at the earliest mandatory or risk-justified stage. The Operator reserves the right to request KYC documentation earlier whenever justified by the risk-based approach.

8. Documents and Information Requested

Depending on the circumstances, the Operator may request:

- government-issued photo ID;
- proof of address;
- payment method ownership evidence;
- selfie / liveness check where reasonably required;
- source of funds evidence;
- source of wealth evidence where justified by the risk profile or circumstances of the case;
- explanation of account behaviour or payment flows; and
- additional verification documents required by risk, sanctions, AML, fraud, or responsible gaming considerations.

For identity verification purposes, acceptable documentary evidence may include a valid government-issued photo identification document, such as:

- passport;
- national identity card; or
- driver's licence.

The identity document must be valid, clear, legible, and must contain sufficient information to verify the customer's identity, including the customer's name, photograph, date of birth, and document details.

For residential address verification purposes, acceptable documentary evidence may include:

- utility bill;
- bank statement;
- official government correspondence, including tax statements or similar official notices;
- official municipal, tax authority, or other public authority correspondence; or
- other reliable independent evidence accepted by the Operator on a risk-sensitive basis.

The document used to verify residential address must show the customer's name and residential address and must not be older than six (6) months at the time it is reviewed. Documents used to verify residential address should not refer only to a P.O. Box, care-of address, or other non-residential address unless additional supporting evidence is obtained and accepted.

As a general rule, photo ID and proof of address are required before the first withdrawal, while payment method ownership evidence is requested on a risk basis where ownership, consistency, or transaction behaviour gives rise to concern.

Previously obtained documents may be re-requested or refreshed on a trigger basis where validity, adequacy, consistency, or risk requires renewed review.

9. Customer Due Diligence Criteria

As part of KYC and customer risk assessment, the Operator may review:

- identity details;
- age and eligibility;
- address and residence information;
- payment method ownership and consistency;
- transaction behaviour and deposit / withdrawal patterns;
- source of funds where relevant;
- source of wealth where justified by the risk profile or circumstances of the case;
- jurisdiction risk;
- payment method risk;
- PEP exposure;
- sanctions exposure;
- adverse media;
- account inconsistencies;
- linked-account indicators;
- fraud indicators;

- device, IP, or behavioural anomalies; and
- any other factor relevant to the business model or risk appetite.

Source of wealth is considered on a risk basis and is not treated as a routine requirement in all EDD cases.

10. Threshold Procedure at XCG 4,000

Once a customer reaches cumulative deposits of XCG 4,000 (or equivalent), the account is automatically flagged for additional KYC follow-up.

At that stage:

- the customer is requested to provide standard KYC documents, normally valid photo ID and proof of address;
- withdrawals are blocked until the requested documentation has been satisfactorily reviewed;
- deposits are not automatically blocked solely because the threshold has been reached, but may be restricted or limited where risk, account behaviour, payment concerns, or incomplete cooperation justify it; and
- payment method changes, promotional use, or other account activity may also be restricted if justified by risk.

The threshold is monitored by the Operator's systems and/or operational teams. Day-to-day follow-up is carried out by Customer Operations / Customer Support and/or Payments & Risk under the Operator's oversight, with non-standard or higher-risk cases escalated to Compliance.

An initial request for documents is issued promptly once the threshold is reached and recorded in the relevant case log.

11. Missing Documents at Threshold

If the threshold is reached and the required documents or information are not provided, the account remains subject to withdrawal restriction pending satisfactory completion of the KYC review.

The Operator will normally follow this reminder cycle:

- initial request promptly after the threshold is reached;
- first reminder after 7 days if the requested documents or information have not been satisfactorily provided; and
- second reminder after 21 days if the matter remains outstanding.

During this period, the case is tracked by the relevant operational team and may be escalated earlier to Compliance where there are additional risk factors, inconsistent explanations, payment concerns, fraud indicators, sanctions / PEP alerts, or other non-standard circumstances.

All requests, reminders, customer responses, restrictions, and escalations must be documented.

12. Thirty-Day Follow-Up

If the requested documents or information are still not satisfactorily provided within 30 days of the threshold being reached, the case must be formally reviewed.

At that stage:

- the matter is escalated to Compliance and, where relevant, to the MLRO;
- the account remains suspended for withdrawals and may be subject to further restriction; and
- the case is assessed to determine whether the relationship may continue, whether further review is justified, or whether the relationship should be terminated in accordance with this Policy and the Operator's Terms and Conditions.

Where the case involves material high-risk factors, confirmed PEP status, significant exceptions, or a proposed termination decision, the matter is escalated to the Managing Director for final decision.

The outcome, the rationale, and any restriction, suspension, or termination decision must be documented in the relevant internal records.

13. Enhanced Due Diligence (EDD)

EDD may be applied, including but not limited to, in the following situations:

- single transaction of EUR 10,000 (or equivalent) or more;
- 5 or more payment method changes within 90 days;
- crypto-originating deposits or funds linked to wallets, exchanges, or PSP blockchain tracing outputs;
- unusual or inconsistent patterns;
- device or IP anomalies;
- sanctions or PEP alerts;
- linked accounts, fraud indicators, syndicate patterns, or suspicious behaviour;
- source of funds concerns; and
- adverse media or jurisdictional concerns.

EDD may include one or more of the following, depending on the nature and severity of the risk:

- enhanced document requests;
- source of funds evidence;
- open-source review;
- additional payment ownership checks;
- additional identity verification steps, including selfie / liveness or other supporting evidence where justified;

- enhanced monitoring; and
- compliance or management approval where required.

As a general rule, source of funds may be requested in EDD cases where the origin of deposited or transacted funds requires clarification.

Source of wealth is not required as a routine element of all EDD cases. It may be requested where the case is materially high-risk or otherwise gives rise to heightened concern, including for example confirmed or likely PEP cases, significant AML concerns, unusually high or inconsistent spending patterns, profile-to-activity mismatch, unexplained high-value play, adverse media concerns, or other circumstances where the customer's broader financial standing and affordability reasonably need to be understood.

Where source of wealth is requested, the Operator may consider supporting documents and other reasonably reliable information, including open-source information where appropriate, and will assess the plausibility and consistency of the information against the customer's profile and activity.

Routine non-standard EDD cases may be reviewed and approved by the Compliance Officer. Cases involving suspected AML/CFT concerns, sanctions, possible true matches, or other reporting considerations must be escalated to the MLRO. Material high-risk cases, confirmed PEP cases, significant exceptions, and cases where continuation of the relationship requires senior management decision must be escalated to the Managing Director for final approval.

14. Ongoing Monitoring

The Operator maintains ongoing monitoring of customer activity in order to detect unusual activity, potential money laundering, terrorist financing, fraud, sanctions exposure, responsible gaming concerns, or any activity inconsistent with the customer's known profile and risk rating.

Ongoing monitoring may be automated, manual, or a combination of both, depending on system capability, customer risk level, activity pattern, and seriousness of any trigger identified.

Monitoring may include review of:

- deposit spikes or unusual increases in deposit value or frequency;
- unusual withdrawal behaviour;
- deposits followed by withdrawals with limited or no genuine gaming activity;
- reversed or cancelled withdrawals;
- repeated failed deposits or payment attempts;
- multiple or frequent payment method changes;
- use of payment methods inconsistent with the customer profile;
- device, IP, geolocation, VPN, proxy, or linked-account indicators;
- unusual or inconsistent betting or transaction behaviour;
- bonus abuse, collusion, syndicate, or arbitrage indicators;
- crypto-originating funds, wallet risk, or PSP blockchain tracing outputs where applicable;
- sanctions, PEP, or adverse media updates;

- material account events such as large wins, high-value payouts, or rapid balance movements; and
- any other activity inconsistent with the customer's expected profile, risk level, source of funds, or previous behaviour.

The timing, depth, and type of monitoring depends on the customer's risk level.

Low-risk customers are subject to standard automated and/or routine monitoring. Their activity is reviewed through system alerts, threshold controls, sanctions / PEP screening, and periodic risk-based review. Low-risk customers are normally reviewed at least annually, or earlier where a trigger arises, such as unusual activity, outdated information, payment inconsistency, adverse media, sanctions / PEP alert, or the XCG 4,000 threshold being reached.

Medium-risk customers are subject to enhanced scrutiny compared with low-risk customers. Monitoring may include closer review of deposit and withdrawal patterns, payment method consistency, changes in risk profile, customer explanations, and supporting documents where appropriate. Medium-risk customers are normally reviewed at least quarterly, or earlier where a trigger arises. Medium-risk treatment may be triggered by, for example, cumulative deposits reaching XCG 4,000, payment method changes, inconsistent activity, higher transaction values, adverse media concerns, use of higher-risk payment methods, or activity that does not fully align with the customer's expected profile.

High-risk customers are subject to enhanced due diligence and closer ongoing monitoring. High-risk treatment may be triggered by, for example, confirmed or likely PEP status, sanctions concerns, high-risk jurisdictions, significant adverse media, suspicious activity indicators, crypto-related concerns, repeated payment method changes, large or unusual transactions, linked-account or fraud indicators, unexplained high-value play, or material inconsistency between the customer profile, source of funds, and account activity. High-risk customers may be reviewed monthly, event-driven, or more frequently where required by the nature of the risk.

Indicative monitoring framework

Risk level	Indicative monitoring timing	Typical measures	Typical escalation
Low risk	Standard automated/routine monitoring; at least annual review or earlier if triggered	Threshold monitoring, sanctions / PEP screening, basic transaction review, document refresh where triggered	Escalation to Compliance only if non-standard trigger arises
Medium risk	At least quarterly review or earlier if triggered	Closer transaction scrutiny, payment method consistency review, updated KYC where needed, source of funds where relevant	Escalation to Compliance for review of non-standard or unresolved concerns
High risk	Monthly, event-driven, or more frequent review depending on risk	EDD, source of funds, source of wealth where justified, enhanced monitoring, possible account restrictions	Compliance review; MLRO escalation for AML/CFT, sanctions, suspicious activity or reporting concerns; Managing Director approval for material high-risk decisions

Where monitoring identifies unusual activity or activity inconsistent with the customer's risk profile, the Operator may apply one or more of the following measures:

- request an explanation from the customer;
- request updated KYC documentation;
- request source of funds evidence;
- request source of wealth evidence where the case is materially high-risk or otherwise justifies broader review;
- request payment method ownership evidence;
- apply enhanced monitoring;
- restrict withdrawals pending review;
- restrict deposits, payment method changes, promotions, or other account functionality where justified by risk;
- escalate the case to the Compliance Officer;
- escalate suspected AML/CFT, sanctions, freezing, or reporting concerns to the MLRO; and/or
- suspend or terminate the relationship where continuation is no longer appropriate.

Where the matter involves suspected money laundering, terrorist financing, sanctions, suspicious activity reporting, possible true matches, or legal freezing considerations, the case must be escalated without delay to the MLRO. Where the case involves material high-risk factors, confirmed PEP status, significant exceptions, or proposed termination, it may also be escalated to the Managing Director for final decision.

All monitoring alerts, reviews, customer explanations, documents requested, restrictions, escalations, decisions, and rationale must be documented in the relevant internal records.

As part of ongoing monitoring, the Operator also assesses whether previously obtained KYC documents and information remain valid, sufficient, and consistent with the customer's current profile and activity. Full KYC refresh is normally completed at least every five years, or sooner where triggered by risk, expiry, inconsistency, regulatory requirement, or material change.

15. PEP Screening

Customers and relevant counterparties may be screened for PEP exposure at onboarding, during ongoing monitoring, at relevant risk events, and when the risk profile changes.

As a minimum operational standard:

- screening is performed at onboarding or account registration through the Operator's screening tools and/or approved service providers;
- re-screening is performed automatically at least every 24 hours where the relevant screening provider or system supports this, or otherwise whenever relevant list updates are captured and implemented; and

- additional event-driven screening may be performed prior to withdrawal, upon material account changes, when unusual or inconsistent activity is detected, when customer information changes, or when other risk triggers arise.

Potential matches are reviewed by the Compliance Officer or an appropriately delegated compliance reviewer. Where the alert remains unresolved, indicates elevated risk, or suggests a possible true match, the case must be escalated without delay to the MLRO.

PEPs are treated as higher-risk and may require enhanced due diligence, source of funds and/or source of wealth evidence, enhanced monitoring, and management approval where the case is material or otherwise justifies escalation.

Confirmed PEP cases and other material high-risk PEP cases are escalated to the Managing Director for final decision on whether the relationship may continue and under what conditions.

16. Sanctions Screening

Customers and relevant counterparties may be screened against applicable sanctions lists, including UN, EU, OFAC, and any other lists required by applicable law or internal controls.

As a minimum operational standard:

- screening is performed at onboarding or account registration through the Operator's screening tools and/or approved service providers;
- re-screening is performed automatically at least every 24 hours where the relevant screening provider or system supports this, or otherwise whenever relevant list updates are captured and implemented; and
- additional event-driven screening may be performed prior to withdrawal, when payment methods are changed, when material customer information changes, when unusual or inconsistent activity is detected, or when other sanctions-related risk triggers arise.

Potential sanctions alerts must be reviewed promptly. False positives must be documented and cleared. Where an alert remains unresolved or suggests a possible true match, the case must be escalated immediately to the MLRO.

Where a confirmed match or other legally relevant sanctions concern arises, the Operator may freeze or restrict the relevant account and/or funds without delay, must avoid tipping off, and must consider reporting to the relevant competent authorities where legally required. The decision, rationale, action taken, and reporting steps must be documented.

17. Freezing of Funds and Reporting

Operational review of sanctions alerts may be supported by compliance tools or service providers, but any unresolved alert, suspected true match, freeze decision, or reporting consideration must be escalated to the MLRO without delay.

Where a confirmed sanctions match or other legally relevant freeze / reporting event arises:

- the matter must be escalated without delay to the MLRO;
- funds and/or account functionality may be frozen or restricted as required by law;

- relevant competent authorities may be notified where legally required; and
- the entire process, rationale, and reporting steps must be documented.

Where funds are frozen or otherwise restricted for sanctions, legal, or AML/CFT reasons, any subsequent release, return, continued hold, or other balance handling decision must follow MLRO review and any applicable legal or authority requirements.

18. Withdrawals, Payment Method Ownership & AML Safeguards

As a general principle, deposits and withdrawals should be linked to payment instruments in the customer's own name, unless an alternative arrangement is expressly permitted and documented.

Unjustified chargebacks, payment abuse, or inconsistent ownership indicators may trigger account action. Proof of payment method ownership may be requested at first withdrawal or earlier based on risk.

Where a customer has reached the XCG 4,000 threshold and has not yet satisfactorily completed the requested KYC review, withdrawals remain blocked until the review is completed.

Where source of funds / source of wealth has been satisfactorily verified and no abuse or AML concern is present, the Operator may apply proportionate controls consistent with its Terms and Conditions and risk appetite.

19. Termination of the Business Relationship

The Operator may suspend or terminate a relationship where:

- required KYC / EDD documents are not provided;
- information is materially false, misleading, or inconsistent;
- fraud, sanctions, AML/CFT, or abuse concerns arise;
- the relationship falls outside the Operator's risk appetite; or
- the customer breaches applicable terms or legal requirements.

Where termination is being considered, the case must be reviewed through the relevant operational, compliance, and AML escalation channels. Routine non-standard KYC termination proposals may be reviewed by the Compliance Officer. Cases involving suspected AML/CFT concerns, sanctions issues, reporting considerations, material high-risk factors, or significant exceptions must be escalated to the MLRO and, where required under this Policy, to the Managing Director for final decision.

The Operator may suspend the account pending review, or terminate the relationship where continuation is no longer considered appropriate. The decision taken, the rationale, the approving function, and any related restrictions or escalation steps must be documented in the relevant internal records.

Outstanding balances will be handled in accordance with applicable law, AML/CFT requirements, sanctions obligations, PSP constraints, and the Operator's Terms and Conditions. As a general rule:

- where no legal restriction, sanctions issue, freeze obligation, reporting-related hold, or material AML concern prevents release of funds, the Operator may return any legitimate undisputed balance through an appropriate payment route permitted under its controls and payment arrangements; and

- where sanctions, a legal freeze, an authority instruction, PSP restriction, or a material AML/CFT concern applies, the Operator may withhold, freeze, or otherwise restrict the balance pending MLRO review, legal assessment, reporting, authority guidance, or other required action.

The Operator must avoid tipping off the customer where reporting, sanctions, or AML/CFT concerns are involved. Where required, the matter must be escalated for reporting consideration before any final balance handling decision is implemented.

20. Internal Company KYC and Counterparty KYC

This Policy also applies, where relevant, to the Operator's own internal and external due diligence processes.

20.1 Internal Company KYC

The Operator will maintain appropriate records and due diligence relating to:

- UBO(s);
- directors and key control persons;
- source of funds and source of wealth where relevant;
- corporate records and governance documentation; and
- changes in ownership or control.

20.2 Counterparty KYC

The Operator may perform proportionate due diligence on relevant counterparties, including:

- incorporation and ownership checks;
- directors / UBO identification where relevant;
- sanctions / PEP screening where appropriate;
- contractual and operational due diligence;
- AML, compliance, security, and reputational review; and
- ongoing refresh for higher-risk providers or business partners.

The Operator may rely on a risk-based and commercially proportionate approach depending on the nature of the counterparty relationship.

21. Record-Keeping & Data Protection

The Operator retains KYC, screening, escalation, restriction, suspension, termination, and reporting records in a secure manner with access limited on a need-to-know basis.

Records may include, where relevant:

- customer identity documents;
- proof of address;

- payment method ownership evidence;
- source of funds and source of wealth documents;
- screening results, alerts, and false-positive clearance records;
- customer communications relating to KYC requests and reminders;
- internal escalation notes and case reviews;
- restriction, suspension, and termination decisions;
- sanctions, freezing, and reporting records; and
- operational logs relevant to KYC review and account handling.

For operational clarity, records are maintained as follows:

- Customer Operations / Customer Support and/or Payments & Risk maintain the operational case file, including customer contact, document requests, reminders, responses, and day-to-day account restriction notes;
- Compliance Officer maintains or oversees records relating to non-standard case review, escalations, enhanced due diligence reviews, restrictions, suspensions, terminations, and policy-related compliance oversight; and
- MLRO maintains records relating to internal suspicious matter escalations, sanctions escalations, freezing decisions, disclosures, reporting, and related AML/CFT records.

Where third-party providers support elements of KYC, screening, payments, or document handling, the Operator remains ultimately responsible for ensuring that relevant underlying records can be obtained and produced within a reasonable time upon request.

Retention will be at least 5 years after account closure or relationship termination, or longer where required by law, regulatory request, authority instruction, or ongoing investigation. Thereafter, data may be deleted, archived, or anonymised as appropriate in accordance with the Operator's retention and data protection practices.

Access to KYC and related case records must be limited to personnel and service providers with a legitimate business or compliance need. Records must be stored in a manner that supports auditability, retrieval, and regulatory inspection where required.

22. Third-Party Reliance & Vendors

Where third parties perform elements of KYC, screening, or verification, the Operator remains ultimately responsible for compliance.

The Operator will seek contractual assurance that underlying records can be made available within a reasonable time upon request, may conduct periodic due diligence or review of such providers, and may implement remediation, escalation, or replacement where material concerns arise.

Where records are created, held, or processed by third-party providers, the Operator must ensure through contractual and operational arrangements that such records remain accessible, retrievable, and

capable of being produced within a reasonable time for compliance, audit, regulatory, or reporting purposes.

23. Training & Awareness

Relevant staff and contractors involved in customer operations, payments, fraud, or compliance must receive appropriate KYC training at onboarding / induction, periodically thereafter, and after material regulatory or operational change. Training records should be retained.

Training should cover at least KYC triggers, document handling, escalation routes, sanctions / PEP awareness, payment ownership issues, suspicious activity escalation, and record-keeping expectations relevant to the staff member's role.

24. Policy Review & Change Control

This Policy will be reviewed at least annually, and also following material regulatory developments, material business or product changes, outsourcing changes, relevant incidents, audit findings, or control changes.

Updates must be approved through the Operator's internal governance process and version-controlled.

Operational appendices or SOPs may be maintained separately to support practical execution, including EDD document examples, risk indicators / red flags, approval levels and escalation matrix, screening / reminder workflow, document refresh logic, and counterparty due diligence checklists.

25. Appendices (Operational)

The Operator may maintain operational appendices or SOPs addressing the following, as appropriate to the stage of operations and outsourcing structure:

- EDD document examples and acceptable evidence;
- risk indicators / red flags;
- approval levels and escalation matrix;
- screening / reminder workflow;
- document refresh logic; and
- counterparty due diligence checklist.

Document Control

Document owner	Compliance Officer appointed by the Operator (at launch expected to be outsourced via Allyant Group B.V.)
Approved by	Managing Directors / Board-level management
Next review date	25 May 2027
Classification	Internal / Licensing Submission
Reference	New Origin B.V. - KYC Policy v1.3