CAMARA NACIONAL DE NEGOCIOS S.A.C.

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

General Corporate AML/CFT Policy

Version	1.0
Effective Date	05 September 2026
Scope	Multi-jurisdictional educational services
Status	Approved for internal implementation and compliance submissions

Policy statement. Camara Nacional de Negocios S.A.C. is committed to conducting its educational business with integrity and to preventing its services, payment channels, accounts, personnel, customers, counterparties, and business relationships from being used for money laundering, terrorist financing, fraud, sanctions evasion, or other financial crime.

The Company is not a bank, remittance company, deposit-taking institution, or virtual-asset service provider. This policy applies a proportionate, risk-based approach and supports the compliance requirements of banks, payment service providers, and other regulated partners used by the Company.

1. Purpose and Objectives

This Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Policy establishes the principles and internal controls used by Camara Nacional de Negocios S.A.C. (the “Company”) to identify, assess, mitigate, monitor, and escalate risks related to money laundering, terrorist financing, sanctions evasion, fraud, identity misuse, and other financial crime.

- Protect the Company and its payment channels from misuse for unlawful activity.
- Apply proportionate customer due diligence and enhanced due diligence based on risk.
- Identify unusual or suspicious transactions and escalate them for review.
- Maintain reliable records and cooperate with competent authorities and regulated payment partners when legally or contractually required.
- Promote a culture of compliance among management, employees, and relevant contractors.

2. Scope and Business Model

This policy applies to management, employees, contractors, sales and customer-service personnel, finance personnel, and any third party acting on behalf of the Company in relation to customer onboarding, enrollment, invoicing, collections, refunds, payments, or access to payment platforms.

The Company provides educational services, professional training, courses, diploma programs, certifications, and related digital services to individual and corporate customers across multiple jurisdictions. Customers pay for the Company’s own products and services. The Company does not receive or transfer funds on behalf of unrelated third parties and does not operate a remittance, money-transfer, deposit-taking, or virtual-asset business.

3. Compliance Framework and General Principles

The Company will comply with the laws and regulatory requirements applicable to its activities in the jurisdictions where it operates, and with lawful compliance requirements imposed by banks, payment service providers, card acquirers, and other regulated partners.

This policy does not represent that the Company is a regulated financial institution or that every obligation applicable to financial institutions applies to the Company. Where a specific statutory reporting, registration, screening, or recordkeeping obligation applies, the Company will follow that obligation.

4. Governance and Responsibilities

General Management has ultimate responsibility for approving this policy, allocating reasonable resources, and ensuring that material AML/CFT risks are addressed. Management may designate an internal responsible person or function for day-to-day implementation.

- Maintain and periodically review this policy and related procedures.
- Review higher-risk customers, counterparties, transactions, refunds, and payment patterns.
- Ensure relevant records are retained and available for legitimate compliance requests.
- Coordinate responses to banks, payment service providers, auditors, legal advisers, and competent authorities.
- Provide or arrange periodic AML/CFT awareness training for relevant personnel.

5. Risk-Based Approach

The Company applies controls in proportion to the level of risk. Risk is assessed using information reasonably available to the Company, including customer type, geographic exposure, payment method, transaction behavior, relationship purpose, third-party payer use, refund activity, transaction size and frequency, and any sanctions or politically exposed person (PEP) indicators.

Risk may be classified as Low, Medium, or High. A higher-risk classification does not automatically mean wrongdoing; it requires greater scrutiny, additional information, and management approval when appropriate.

6. Customer Due Diligence (CDD)

For ordinary individual customers purchasing educational services, the Company will obtain information sufficient to identify the customer and support the commercial purpose of the transaction. Depending on the payment channel and risk level, this may include full name, country, email, telephone number, enrollment/purchase information, payment confirmation, transaction reference, and additional verification where required.

The Company will not knowingly open or maintain anonymous or fictitious customer relationships and may request additional information to resolve a mismatch between the customer, payer, invoice, beneficiary, or refund recipient.

7. Corporate Customers and Beneficial Ownership

For corporate or institutional customers, particularly where transaction values or frequency are material, the Company may obtain the legal name, registration or tax number, registered jurisdiction, business activity, authorized representative, and supporting corporate documentation. Where risk warrants it, the Company may request information about ultimate beneficial owners or persons exercising control.

8. PEP, Sanctions and Restricted-Party Screening

Where required by a payment partner, where risk is elevated, or where reliable screening tools are available, the Company will take reasonable steps to identify whether a customer, beneficial owner, controlling person, or counterparty is a PEP or appears on applicable sanctions or restrictive lists.

A PEP relationship is not automatically prohibited. It requires enhanced review, confirmation of the legitimate purpose of the relationship, and, where appropriate, additional information regarding source of funds and management approval. The Company will not knowingly process transactions that violate applicable sanctions or legal prohibitions.

9. Transaction Monitoring

The Company reviews transactional activity using a proportionate approach consistent with its educational business model. Monitoring may be manual, system-based, or performed through information and alerts provided by banks or payment service providers.

- Payments materially inconsistent with the stated educational product or normal pricing.
- Repeated payments by unrelated third parties without a clear commercial explanation.
- Unusual use of multiple cards, accounts, devices, or payer identities for the same customer or enrollment.
- Rapid purchase-and-refund cycles, repeated refund requests, or requests to refund to a different person or payment instrument.
- Attempts to split transactions into smaller amounts to avoid controls or verification requirements.
- Transactions involving restricted persons or jurisdictions, or presenting unusually high financial-crime risk.
- Customer reluctance to provide reasonable identification or transaction information when requested.
- Instructions that would unnecessarily complicate the transaction or obscure the true payer or beneficiary.

10. Enhanced Due Diligence (EDD)

When a relationship or transaction is assessed as higher risk, the Company may obtain additional identity or corporate documents, confirm the purpose of the transaction, request evidence regarding source of funds, verify the relationship between the payer and the student/customer, obtain management approval, or require a payment method that provides stronger traceability.

The Company may decline, suspend, or refund a transaction when requested information is not provided, the commercial purpose cannot be reasonably established, or the risk cannot be reduced to an acceptable level.

11. Source of Funds and Third-Party Payments

Where transaction size, frequency, customer profile, or other risk indicators justify additional review, the Company may request information or evidence regarding the source of funds. Unexplained third-party payments may be rejected or require evidence of the relationship between the payer and the customer.

The Company does not provide pass-through accounts, nominee payment services, or money-transfer services for unrelated third parties.

12. Suspicious Activity Escalation and Cooperation

Personnel must promptly escalate unusual or suspicious activity to the designated internal responsible person or General Management. The review should be documented and may result in approval, rejection, suspension, refund through the original payment channel, or escalation to a payment provider, bank, legal adviser, or competent authority as appropriate.

If the Company becomes subject to a legal obligation to file a suspicious transaction or other regulatory report, it will follow the applicable procedure and confidentiality requirements. The Company will not knowingly engage in prohibited "tipping off."

13. Refunds, Reversals and Chargeback Controls

Refunds should normally be returned through the original payment method and to the original payer whenever operationally possible. Requests to redirect refunds to another person, account, wallet, or payment instrument require additional review and may be refused. Records should link the original payment, the educational product, the customer, and the refund decision.

14. Prohibited Conduct

The Company prohibits personnel and representatives from knowingly engaging in the following conduct:

- Accepting or facilitating transactions known or reasonably suspected to involve proceeds of crime or terrorist financing.
- Creating, modifying, or concealing records to disguise the identity of a payer, beneficiary, customer, or transaction purpose.
- Advising a customer how to avoid identification, monitoring, sanctions, payment-provider, or transaction controls.
- Using Company accounts to receive, hold, transfer, exchange, or return funds for purposes unrelated to legitimate Company business.
- Processing a transaction that is prohibited by applicable law or a binding restriction imposed by a bank or payment provider.

15. Banks, Payment Service Providers and Other Third Parties

The Company seeks to use reputable banks, payment processors, and service providers that operate lawful compliance programs. The Company will provide reasonable KYC/KYB, ownership, transaction, or policy information requested by such partners for legitimate compliance purposes, subject to confidentiality and data-protection requirements.

Use of a third-party payment provider does not remove the Company's responsibility to understand its own customers and commercial activity at a level proportionate to risk.

16. Record Retention and Audit Trail

The Company will maintain appropriate records of customer identification information, invoices, payment confirmations, transaction references, refunds, higher-risk reviews, screening results where applicable, and relevant communications for at least five (5) years from the end of the relationship or transaction, unless a longer period is required by applicable law, tax rules, litigation hold, or a contractual obligation with a regulated partner.

Records should be stored securely, protected against unauthorized alteration, and retrievable within a reasonable time for legitimate compliance, audit, or regulatory purposes.

17. Training and Staff Awareness

Personnel involved in sales, customer support, enrollment, finance, refunds, and payment operations will receive proportionate AML/CFT awareness guidance. Training will cover customer identification, suspicious payment indicators, refund risks, escalation procedures, confidentiality, and the prohibition on helping customers bypass controls.

18. Data Protection and Confidentiality

AML/CFT information will be accessed only by personnel who need it for legitimate business, compliance, legal, or audit purposes. Personal and corporate information collected under this policy will be handled in accordance with applicable privacy/data-protection requirements and the Company's internal privacy and cybersecurity policies.

19. Testing, Review and Policy Updates

This policy will be reviewed at least annually and sooner when there is a material change in the Company's business model, payment methods, jurisdictions, legal requirements, or payment-partner expectations. Management may perform or commission periodic checks to confirm that the controls described in this policy are operating as intended.

20. Approval and Effective Date

This policy is approved by General Management of Camara Nacional de Negocios S.A.C. and is effective from 05 September 2026. It remains in force until amended or replaced by a later approved version.

Annex A - Practical AML/CFT Risk Matrix

This matrix is a practical reference for an educational-services business. It is not exhaustive and must be applied together with professional judgment, available transaction information, and the requirements of banking/payment partners.

Risk Area	Lower-Risk Example	Higher-Risk Indicator	Typical Control
Customer	Individual buying a normal course for own use	Identity inconsistency, unverifiable details, unexplained third-party payer	Request clarification/verification; escalate if unresolved
Payment	Single traceable payment consistent with published price	Split payments, multiple unrelated payers, unusual payment instruments	Review transaction history and payer relationship
Refund	Refund to original payment method	Request to send refund to a different person/account	Normally refund only to original method; require justification
Geography	Customer in ordinary operating market	Restricted/sanctioned exposure or unusually high-risk jurisdiction	Screen, apply EDD, decline if legally prohibited
Corporate client	Registered entity with clear training purpose	Opaque ownership or no clear commercial link	Request corporate and beneficial ownership information
Behavior	Normal enrollment and service usage	Pressure to bypass controls or provide false information	Escalate and consider rejection/suspension

Annex B - Operational Checklist

- Confirm the payment is linked to a legitimate Company product or service.
- Confirm payer/customer information is reasonably consistent with the transaction.
- Escalate unexplained third-party payments, repeated split payments, or unusual refund requests.
- Use the original payment channel for refunds whenever operationally possible.
- Do not receive, hold, transfer, or exchange funds for unrelated third parties.
- Retain transaction and review records in accordance with this policy.
- Escalate sanctions/PEP alerts, suspicious patterns, or requests to bypass controls.

Approval

Legal Entity	Camara Nacional de Negocios S.A.C.
Approved by	General Management
Signature / Stamp	_____
Date	05 September 2026