CAMARA NACIONAL DE NEGOCIOS S.A.C.

CYBERSECURITY, DATA PROTECTION AND PRIVACY PROGRAM

Programa de Ciberseguridad, Protección de Datos y Política de Privacidad

Legal name	CAMARA NACIONAL DE NEGOCIOS S.A.C.
Version	1.0
Issue date	September 5, 2026

CORPORATE DOCUMENT - COMPLIANCE USE

This document contains no personal names, ID numbers, personal phone numbers, home addresses, or personal email addresses of shareholders, representatives, or staff.

https://camaranacionaldenegocios.com/

Contents

1. Purpose and scope

This document establishes the corporate cybersecurity, data protection and privacy program of CAMARA NACIONAL DE NEGOCIOS S.A.C. Its purpose is to define risk-based controls to protect information relating to students, customers, prospects, vendors and the company, and to set transparent rules for the processing of personal data.

It applies to training, diploma programs, courses, professional education and the commercial, administrative, technology and payment support activities that use information in physical or digital form. The company may offer services and receive payments from customers located in multiple jurisdictions.

Compliance scope
This program is adopted as an internal corporate policy and may be presented to payment providers, financial institutions, counterparties and compliance teams as evidence of the organization's security and data protection framework. It is designed for a digital operation serving customers across multiple jurisdictions and is supplemented by any legal or contractual requirements applicable in each market.

Compliance and reference framework

- Data protection and privacy requirements applicable in the jurisdictions where the company offers services or processes personal data.
- Contractual and compliance requirements applicable from payment providers, financial institutions, technology platforms and counterparties.
- Risk-based security practices including least privilege, defense in depth, continuity and incident response.

This document is a corporate policy and does not constitute individualized legal advice. The company will review its suitability when its processes, systems, vendors, markets or applicable regulatory requirements change.

2. Governance and responsibilities

General Management approves this program, allocates reasonable resources and oversees compliance. Operational duties may be assigned by role without publishing personal information in this document.

Role	Minimum responsibilities	Evidence
General Management	Approve policies, prioritize risks, authorize critical access and review material incidents.	Annual internal approval or record.
Security & Privacy Responsible Role	Maintain controls, coordinate incidents, review access, backups, vendors and privacy requests.	Review/action records.
Authorized Users	Use individual credentials,	Policy

Role	Minimum responsibilities	Evidence
	protect devices and report incidents.	acknowledgement/training.
Technology Vendors	Meet contractual security, confidentiality and data protection obligations.	Contracts, terms, DPA or equivalent evidence.

3. Security and privacy principles

- Lawfulness, purpose limitation and transparency.
- Data minimization: collect only what is necessary for a legitimate purpose.
- Need-to-know and least privilege access.
- Confidentiality, integrity and availability.
- Security by design and by default for new processes and integrations.
- Reasonable traceability and accountability.
- Timely incident response and continuous improvement.

4. Information inventory and classification

Classification	Examples	Handling	Access
Public	Published commercial information, course catalog, institutional content.	May be disclosed under corporate authorization.	General.
Internal	Procedures, operational reports, work materials.	Do not publish without authorization.	Authorized personnel.
Confidential	Customer/student data, contracts, financial reports, operational credentials.	Secure transmission/storage where feasible; restricted access.	Need-to-know only.
Restricted	Passwords, API keys, tokens, sensitive financial data or ID documents when necessary.	Highest restriction; do not share through insecure channels.	Minimum necessary users.

5. Identity and access control

- Users must use individual credentials and must not share passwords.
- Strong, unique passwords will be used, preferably with a password manager.
- Multi-factor authentication (MFA/2FA) will be enabled where supported, prioritizing corporate email, CRM, payment platforms, cloud storage and administrative accounts.

- Access is assigned by role and based on least privilege.
- Access for former staff or users who no longer require a service will be revoked promptly.
- Privileged access will be reviewed at least semi-annually and after material personnel/vendor changes.

6. Device, network and application security

6.1 Devices

- Keep operating systems, browsers, applications and security tools reasonably up to date.
- Use device login protection and automatic screen locking on devices with corporate information.
- Avoid unauthorized or untrusted software.
- Do not store credentials or sensitive information in unprotected plain-text files.
- Report loss, theft or compromise of any device with corporate access immediately.

6.2 Email, browsing and phishing

- Verify senders, domains, links and attachments before opening them.
- Never disclose passwords, MFA codes, API keys or payment credentials in response to unverified requests.
- Confirm unusual requests for bank-account changes, fund withdrawals or beneficiary changes through a second verified channel.

6.3 Cloud applications and services

- Prefer reputable providers with appropriate security and privacy controls.
- Configure file/folder permissions to avoid unnecessary public links.
- Review third-party integrations and access tokens periodically.
- Separate administrative accounts from daily-use accounts where reasonably possible.

7. Personal data protection and Privacy Policy

7.1 Data controller

CAMARA NACIONAL DE NEGOCIOS S.A.C. is the controller of personal data collected directly in connection with its activities. Privacy requests are handled through the corporate channels published at https://camaranacionaldenegocios.com/. No personal information of representatives, shareholders or employees is published in this document.

7.2 Categories of data

- Identification and contact data provided by the user (for example, name, identification when necessary, phone, email and location or jurisdiction where relevant).
- Academic/enrollment data relating to courses, diploma programs, certifications and student support.
- Billing and transaction data necessary for payments, refunds and reconciliation. The company seeks not to store full card details and uses authorized payment processors.
- Commercial and support interaction data, including inquiries, consents, communication preferences and service records.
- Reasonable technical/security data such as login logs, IP, device or events where generated by the systems used.

7.3 Purposes

- Manage inquiries, enrollments, access to services, certifications and support.
- Process payments, reconciliation, refunds, invoicing and fraud prevention.
- Meet legal, tax, accounting and compliance obligations.
- Protect systems, prevent unauthorized access and resolve incidents.
- Send marketing communications where a valid basis exists and provide reasonable opt-out mechanisms.
- Improve processes and user experience using aggregated or minimized information where possible.

7.4 Legal basis and consent

Processing is based on the contractual or pre-contractual relationship, legal obligations, compatible legitimate interests where applicable and/or consent when required. Where consent is required, it should be freely given, prior, informed, express and unambiguous as applicable.

7.5 Processors and third parties

The company may use hosting, CRM, messaging, email, analytics, storage, invoicing, support and payment-processing providers. Only the data needed for the relevant purpose will be shared, and the company will seek providers with appropriate security and confidentiality commitments.

7.6 International transfers

Because technology and payment providers may use international infrastructure, some data may be processed or hosted in different jurisdictions. The company will seek appropriate contractual, technical and organizational safeguards and reasonable traceability of relevant providers.

7.7 Retention

Data will be retained only as long as needed for the purpose, commercial relationship, certification records, support requests, tax/accounting requirements, dispute defense and legal or regulatory obligations. Afterwards, data will be deleted, anonymized or restricted as appropriate.

7.8 Data subject rights

Data subjects may exercise rights recognized by applicable law, including access, rectification, cancellation/deletion and objection, as well as withdrawal of consent where applicable. Requests will be reasonably verified to protect against unauthorized access.

7.9 Minors

Services are primarily intended for persons able to contract on their own behalf. Where a service involves minors' data, enhanced safeguards and, where applicable, consent or involvement of a parent or legal representative will be used.

7.10 Cookies and similar technologies

Websites and digital tools may use cookies or similar technologies for functionality, security, measurement and user experience. Where required by law or by the nature of the technology, appropriate information and choice mechanisms will be provided.

8. Payment security and fraud prevention

- Payments will be processed through authorized providers or specialized platforms, reducing direct storage of card data by the company.
- Controls such as 3-D Secure, risk screening, velocity checks, device validation or other anti-fraud mechanisms will be used when available from the payment provider and applicable.
- Refund instructions or changes to settlement bank accounts require additional verification of authority and request legitimacy.
- Refunds should, where possible, return to the original payment method or payer, subject to provider and business rules.
- Reasonable evidence of enrollment, terms acceptance, service delivery/access and relevant communications will be retained to manage disputes and chargebacks.

Scope note
The company does not hold itself out as a financial institution, remittance provider, wallet or payment processor. Funds collected relate to the company's own services. Payment providers operate the financial rails and controls within their scope.

9. Third-party and vendor management

- Vendor reputation and service purpose.
- Authentication, encryption and access-control capabilities.
- Data location and processing.
- Confidentiality and data-protection commitments.
- Incident notification capability.
- Backup, continuity and recovery mechanisms.
- Relevant subcontracting and ability to terminate/export data.

10. Backup, business continuity and recovery

- Maintain periodic backups of critical information, prioritizing academic records, administrative documentation and essential configurations.
- Keep at least one backup logically separated from production where reasonably possible.
- Test recovery of critical information periodically.
- Maintain alternate communication/access paths for material outages.
- Prioritize recovery of identity/access, communications, CRM/support, academic records, billing/payments and corporate files.

11. Incident and data breach management

Any event that may compromise confidentiality, integrity, availability or personal data will be handled through the following cycle:

1. Detect and record the event.
2. Contain the affected account, device, integration or access.
3. Preserve sufficient evidence to understand the incident.
4. Assess scope, affected data/users and risk.

5. Eradicate the cause (credential changes, token revocation, patching, blocking, etc.).
6. Restore services and verify secure operation.
7. Notify providers, data subjects or authorities where legally required or appropriate to the risk.
8. Document lessons learned and preventive actions.

Internal reporting
Any employee or provider with access must promptly report suspected phishing, compromised credentials, unauthorized access, lost devices, data leakage or unusual financial activity to the designated corporate responsible role.

12. Training and awareness

- Phishing and social engineering.
- Passwords, MFA and secure credential handling.
- Personal data protection and confidentiality.
- Secure use of CRM, email, storage and payment platforms.
- Fraud prevention, bank-account change verification and refunds.
- Incident reporting and continuity.

13. Data retention and disposal

Category	Retention criterion	Disposition
Academic/certification records	For the service period and a reasonable period needed to validate studies/certificates and answer requests.	Controlled retention; anonymize or delete when no longer needed.
Billing, payment and accounting	Per applicable tax, accounting, contractual and audit obligations.	Protected archive and deletion when the required period expires.
Prospects and marketing	While a valid relationship, consent or compatible legitimate basis exists and until opt-out where applicable.	Purge, delete or anonymize.
Security logs/evidence	Risk-based period appropriate to technical capability and incident investigation.	Rotation or secure deletion.
Credentials/secrets	Only while valid and necessary.	Revoke promptly when no longer required; do not retain obsolete secrets unnecessarily.

14. Monitoring, audit and continuous improvement

- Review this program annually or sooner after significant change.
- Periodically review privileged access, integrations and critical vendors.
- Track incidents, fraud, chargebacks and privacy-related complaints.
- Update controls when threats or used platforms change.
- Maintain reasonable evidence of reviews, training, incidents and risk decisions.

Suggested indicators: percentage of critical accounts with MFA; privileged access reviewed; incidents recorded/closed; access revocation time; tested backup restorations; fraud/chargeback rates; critical vendors assessed.

15. Operational appendices and approval

Appendix A - Monthly minimum checklist

- ☐ Review login/security alerts for critical accounts.
- ☐ Confirm active users still require their access.
- ☐ Verify operating system/browser updates.
- ☐ Confirm backups are running and review errors.
- ☐ Review changes to integrations, tokens and vendors.
- ☐ Review incidents, fraud, chargebacks and privacy requests.

Appendix B - Minimum incident register

Date	System	Description	Impact	Actions	Status

Appendix C - Corporate approval

This program becomes effective once internally approved and will be maintained for compliance, provider and audit review where applicable.

Company	CAMARA NACIONAL DE NEGOCIOS S.A.C.
Approved by	General Management
Signature / stamp and date	_____

Reference framework

Privacy, data protection, information security and e-commerce requirements that may apply in the jurisdictions where the company provides services or processes data.

Security and privacy good practices based on risk management, least privilege, defense in depth, business continuity, incident response and accountability.