COREACCESS SOLUTIONS S.A.

Anti-Money Laundering and Counter-

Financing of Terrorism Policy

As of 05.01.2026

1. INTRODUCTION

COREACCESS SOLUTIONS S.A. with registration number 155771915, address at World Trade Center, 7th floor, 53E Street, Marbella, Bella Vista, Panama City, Republic of Panama ("Company") aims to detect, manage and mitigate the risks associated with Money Laundering and the Financing of Terrorism ("ML/FT"). The Company does this to comply with corresponding laws and regulations of Panama ("PAM"), protect its reputation and uphold international standards of corporate responsibility.

The purpose of this policy is to:

a) Address the Company's current and future obligations under the:

Law No. 23 of 27 April 2015 (as amended from time to time, including by Law No. 21 of 2017 and Law No. 70 of 2019), Executive Decree No. 363 of 13 August 2015, Executive Decree No. 587 of 4 August 2015, applicable measures implementing United Nations Security Council sanctions, and any other relevant PAM laws, regulations, supervisory resolutions, and guidance, so far as they are known at present (collectively, the "AML/CFT Regulations");

b) Make employees, clients, and third parties aware of the meaning of AML/CFT;

c) Set out the responsibilities of key staff including those of an AML/CFT Compliance Officer;

d) Document measures taken and oversight exercised for:

• Applying clients due diligence;
• Monitoring for suspicious transactions;
• Record-keeping;
• Suspicious transactions reporting.

The Company has introduced strict policy aimed at the detection, prevention or mitigation, and warning the corresponding bodies of any suspicious activities performed by clients. A complex electronic system was implemented for identifying every Company's client and conducting a detailed history of all operations.

2. RISK-BASED APPROACH

The possibility of being used to assist with money laundering and terrorist financing poses many risks for the Company, including:

a) Prosecution for offenses under the AML/CFT Regulations;
b) Civil or criminal action against the Company as a whole or against individual partners or directors;
c) Damage to reputation leading to a loss of business.

The Company is required to constantly monitor its level of exposure to the risk of money laundering and the financing of terrorism.

The Company believes that if it knows its client well and understands its instructions thoroughly, it will be better placed to assess risks and spot suspicious activities.

The risk-based approach means that the Company focuses its resources on the areas of greatest risk. Higher risk clients will need higher levels of checking to be performed. In the case of clients assessed as low to medium risk, Standard CDD procedures will apply. In the case of clients assessed as high risk, Enhanced CDD procedures apply. The resulting benefits of this approach include:

a) More efficient and effective use of resources proportionate to the risks faced;
b) Minimizing compliance costs and burdens on clients;
c) Greater flexibility to respond to emerging risks as laundering and terrorist financing methods change.

It is towards these key risks that the Company will devote most of its compliance controls and resources, consistent with a risk based approach to AML/CFT compliance. In addition, Company's ongoing monitoring will consider several behavioral pattern risks or 'red flags' that will be built into ongoing client due diligence and monitoring.

3. PERSONNEL

AML/CFT Compliance Officer

The Company shall designate a suitably qualified employee (or appoint a suitably qualified person) as an AML/CFT Compliance Officer to administer and maintain the AML/CFT program.
The AML/CFT Compliance Officer will be fully responsible for the Company's AML and CFT program and report to the Board of the Company or a committee thereof any material breaches of the internal AML/CFT policy and procedures and of the AML/CFT Regulations and other relevant laws, codes and standards of good practice.
The duties of the AML/CFT Compliance Officer include:

a) Monitoring the Company's compliance with this policy and AML/CFT Regulations;
b) Overseeing communication and training for employees (training to be done at the beginning of employment and on an annual basis);
c) Ensuring that proper AML records be kept;
d) Ensuring Suspicious Transactions Reports ("SAR") be filed when necessary;
e) Ensuring that the Company has adequate client identification and verification procedures be in place (client due diligence).

Employees

All Company employees, managers and directors must be aware of this policy.

Employees, managers and directors who are engaged in AML/CFT related duties must be suitably vetted. This includes a criminal check done at the time of employment and monitoring during employment. Any violation of this policy or an AML/CTF program must be reported in confidence to the AML/CFT Compliance Officer, unless the violation implicates the AML/CFT Compliance Officer, in which case the employee must report the violation to the Chief Executive Officer.

Employees who work in areas that are susceptible to money laundering or financing terrorism schemes must be trained in how to comply with this policy or the AML/CFT program. This includes knowing how to be alert to money laundering and terrorism financing risks and what to do once the risks are identified.

Employee Training Programme

The Company provides AML/CFT training to employees who will be dealing with clients or will be involved in any AML checking, verification or monitoring processes. The Company may conduct its training internally or hire external third party consultants.

Each person employed within the Company is assigned a supervisor who teaches him or her in relation to all policies, procedures, client documentation forms and requirements, etc. There is a training plan for each new employee and tests which are being held for 2-3 months (depending on level within the business).

The Company's AML training programmes are aimed to ensure its employees receive appropriate training levels with regards to any possible AML/TF risks.

Content of training

The Company's AML/CFT and risk awareness training includes the following content:

• The Company's commitment to the prevention, detection and reporting of ML and TF crimes.
• Well known or recognised typologies, especially where made available by the FATF or AML/CFT Supervisors.
• The consequences of ML and TF for the Company, including potential legal liability.
• The responsibilities of the Company under the AML/CFT Regulations.
• Those particular responsibilities of employees as identified in this AML/CFT Policy, and how employees are expected to follow the Company's AML/CFT procedures.
• How to identify and report unusual activity that may be a suspicious transaction or attempted transaction.
• The rules that apply against unlawful disclosure of suspicious transactions ("tipping off").

Type and frequency of training

The Company selects the most effective method of training for its staff – any of online or web based learning, interactive workshops and face-to-face instruction.
The Company provides a refresher course on its AML/CFT training when there is something new in the AML/CFT regime for all staff that occupies AML/CFT related roles.
Staff employed in a senior management role will undergo training every 12 months in order to maintain a high level of engagement in any changes and updates to the Company's AML Programme. In addition, regular reporting and management level dialogue with the AML/CFT Compliance Officer will assist in keeping senior management and the Directors up to date with AML legal developments.

New staff / Change in roles

When new staff (employees or contractors) are engaged by the Company, role-based AML/CFT training appropriate to their role will be provided as soon as practicable after the commencement of employment or engagement with the Company. If these staff members move from one role to another they may need further AML/CFT training for their new role.

The AML/CFT Compliance Officer will ensure that new members of staff will receive all necessary training within three months after joining the Company and at least every two years thereafter. Staff members who have not yet been trained can carry out roles that involve dealing with clients or any Company's AML checking, verification or monitoring process only under supervision of fully trained staff members.

Training records, and overall control and responsibility

The Company will retain training records including dates and types of training and testing results (if applicable).

The AML/CFT Compliance Officer is responsible for developing the Company's AML/CFT training programme, and for ensuring proper keeping of records of training undertaken. The AML/CFT Compliance Officer will have and maintain a higher level of training on AML/CFT matters, including where appropriate attendance at external industry or regulator courses or seminars and liaison with external experts.

Senior managers and directors

Senior managers and directors are responsible for overseeing this policy or the AML/CFT program and AML/CFT Compliance Officer.

Senior management and directors of the Company will support and assist the AML/CFT Compliance Officer to meet those responsibilities, and take spec care to ensure that communications lines are always open and effective.

4. CLIENT DUE DILIGENCE

Effective Client Due Diligence ("CDD") measures are essential to the management of money laundering and terrorist financing risk. CDD means identifying the clients and verifying their true identity on the basis of documents, data or information obtained from a reliable and independent source both at the moment of starting a business relationship and on an ongoing basis.

Identification of a client is coming to know a client's identifying details, such as their name and address, his financial status and the capacity in which he is entering into the business relationship with the Company.

Verification is obtaining evidence satisfactory to the Company which supports this claim of identity.

The Company will:

a) Collect certain identification information from each client;
b) Utilize risk based measures to verify the identity of each client;
c) Record client identification information and the verification methods and results.

For individual clients the Company will collect the following CDD information:

a) Client's full name;
b) Client's date of birth;
c) Passport number/identification card number;
d) Country of residence/location of client;
e) Address;
f) Mobile telephone number and e-mail.

For corporate clients the Company will collect the following CDD information:

a) Full company name;
b) Registration number and date;
c) Country of registration;
d) Corporate documents;
e) Registered address;
f) Mobile telephone number and e-mail.

Where the underlying principles are not individuals, the Company shall investigate further to establish the identity of the natural persons ultimately owning or controlling the business.

Verifying information

Based on the risk, and to the extent reasonable and practicable, the Company will ensure that it has a reasonable belief that it knows the true identity of its clients by using risk based procedures to verify and document the accuracy of the information received about the clients. In verifying client identity, the Company will analyze any logical inconsistencies in the information obtained.

Client's identity must be verified when:

a) Establishing a business relationship with a new client;
b) The Company suspects money laundering or terrorist financing;
c) The Company has doubts about the veracity or adequacy of documents, data or information previously obtained for the purpose of CDD.

In respect of the existing client, the review and update of the CDD information shall be performed on a risk-sensitive basis and at least once in each 1 (one) year period, in respect of normal and low risk clients.

Where verification of identity is conducted after the establishment of the business relationship, verification will be completed as soon as is practicable after the business relationship has been established.

Methods of verification

The Company will verify client identity through documentary evidence and non-documentary evidence via SumSub as a certified service-provider (electronic verification).

The Company will use documents to verify client identity when appropriate documents are available. In light of the increased instances of identity fraud, the Company will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. It may also use such non-documentary means, after using documentary evidence, if still uncertain about whether the true identity of the client is known.

In analyzing the verification information, the Company will consider whether there is a logical consistency among the identifying information provided, such as the client's name, date of birth, street address and telephone number.

Appropriate documents for verifying the identity of clients include, but are not limited to, the following:

a) For an individual: a high-resolution copy of passport or a national identity card issued for the purpose of identification that contains the name, date of birth, a photograph and the signature or other biometric measure (e.g. eye scan, fingerprint data) of the person in whose name the document is issued;

b) For a person other than individuals: a high-resolution copy of documents showing the existence of the entity, such as Certificate of Incorporation, Certificate of Good standing/Incumbency/Extract from register, Articles of Association/analogue document, Shareholders and directors register, Passport or ID of each shareholder, Utility bill of each shareholder not older than 6 (six) months, Passport or ID of each director, Utility bill of each director not older than 6 (six) months, etc.

To verify proof of address of the client the Company requires one of the following to be provided, in the same correct name of the client:

a) A high-resolution copy of a utility bill (fixed-line phone, water, electricity) issued within the last 3 months;
b) A copy of a tax or rates bill from a local authority;
c) A copy of a bank statement (for a current account, deposit account or credit card account);
d) A copy of a bank reference letter.

The Company will not be required to take steps to determine whether the document that the client has provided for identity verification has been validly issued and it may rely on government issued identification as verification of a client's identity. If, however, it appears that the document shows some obvious form of fraud, the Company will consider that factor in determining whether it can form a reasonable belief that it knows Anti-Money Laundering and Counter-Terrorism Financing Policy the client's true identity.

The Company will use the following non-documentary methods of verifying identity:

a) Contacting a client;
b) Independently verifying the client's identity through the comparison of information provided by the client with information obtained from Internet and/or other source;
c) Checking references with other financial institutions;
d) Obtaining a financial statement.

Non-documentary methods of verification will be used in the following situations:

a) When the Company is unfamiliar with the documents the client presents for identification verification;
b) When there are other circumstances that increase the risk that the Company will be unable to verify the true identity of the client through documentary means.

Lack of verification

Should the Company reasonably believe that the true identity of a client cannot be established or suspect the client has provided misleading information it will do any or a combination of the following:

a) Not proceed with or terminate any business with the client;
b) File a SAR in accordance with applicable law and regulations.

Enhanced client due diligence procedures (EDD)

The regulatory measures require further research and identification of clients who may pose a high risk of money laundering to better assess the risks they pose.

If the Company has assessed that the business relationship is a high risk relationship, based on the client's individual risk status, that is, the nature of the client, the business relationship, its location, or any other specificity of the business relationship, it will apply EDD measures.

By way of non-exhaustive examples, circumstances when EDD will be applied are:

a) If the Company establishes a business relationship with a client connected with a country that does not apply, or insufficiently applies the FATF Recommendations;
b) If the Company establishes a business relationship with a politically exposed person or a family member or closed associate of a politically exposed person;
c) If a client seeks to conduct a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose;
d) In any other circumstances which by its nature can pose a higher risk of money laundering or as specified in Anti-Money Laundering regulations.

The Company may in all circumstances consider that the level of risk involved is such that enhanced due diligence should apply to a particular situation.

In addition to CDD, the following enhanced requirements under EDD will apply:

a) Obtaining the information relating to the source of the funds or the wealth of the client will be required;
b) Carrying out more frequent and more extensive ongoing monitoring on the client;
c) Any additional information prescribed by regulations.

When obtaining information to verify the client's statements about source of funds or wealth, the staff member will most often ask for and scrutinize details of the person's employment status or business/ occupation, as shown in the client application form.

If suspicious information is found indicating possible money laundering or terrorist financing activity, the AML Compliance Officer shall file a Suspicious Activity Report in accordance with applicable law and regulations.

Politically Exposed Person (PEP)

Politically exposed person are individuals who are or who have been entrusted with prominent public function, including heads of state/government, senior government, judicial or military officials, members of boards of central banks, ambassadors, senior executives of state owned corporations, important political party officials, including their family members or close associates of the politically exposed person.

The Company will, as soon as practicable after establishing a business relationship, take reasonable steps to determine whether the client or any beneficial owner is a politically exposed person.

If the Company determines a person to be PEP, it will:

a) Conduct enhanced due diligence as described above;
b) Obtain information about the source of wealth or funds of the individual and take reasonable steps to verify that this information is correct;
c) Require senior management approval for continuing the business relationship with the individual in question.

Agent to conduct client due diligence

Subject to any conditions that may be prescribed in regulations, the Company may authorize another company or person to be its agent and rely on that agent to conduct the CDD procedures.

5. SUSPICIOUS TRANSACTIONS

If the Company suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it shall as soon as practicable, and in any event, within fourteen days, report its suspicions to the Unidad de Análisis Financiero de Panamá (UAF).

Factors such as business relations and transactions with clients from jurisdictions that do not have adequate systems in place to prevent or deter money laundering or terrorist financing; or any of the "red flags" identified below.

"Red flags"
By way of example only, the following situations/indicators ("red flags") have been considered by the Company. They may give reasonable grounds for suspicion, when presented individually or in conjunction with other circumstances or information involving the same client:

• Clients who give conflicting information to different Company employees; or attempt to mislead or offer corrupt inducements to any employee or contractor to bypass the Company's controls;
• Other circumstances or public news/information implying that the operations are related to criminal activity, money laundering or financing of terrorism;
• Any hint of identity fraud, credit card theft or misleading identity details;
• Clients who exhibit an unusual level of concern for secrecy, particularly with regard to their identity, type of business or source of wealth/assets;
• Clients who refuse to provide appropriate identification data or use misleading identification data, or make it difficult to verify information.

Controls within the Company's systems may mean that some of these red flags will be very unlikely to arise, but it will remain vigilant to any new or unexpected client's attempts to evade controls in any of the ways mentioned above.

Country risk

Country risk, in conjunction with other "red flags", provides useful information as to potential money laundering or terrorism risks. There is no universally agreed definition by either governments or financial institutions of which countries pose a higher risk. Factors that may result in a determination that a country poses a higher risk include:

a) Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations;
b) Countries identified by the Financial Action Task Force ("FATF") as non-cooperative in the fight against money laundering or identified by credible sources as lacking appropriate money laundering laws and regulations.

The Country categorisation lists, updated FATF jurisdiction lists, and Company's own internal black list shall be reviewed at least quarterly by staff from the Financial Monitoring department, and any suggested changes or risk revisions reported to the AML/CFT Compliance Officer for consideration and approval.

Responding to red flags and suspicious activity

All potential suspicious transactions must be reported internally to the AML/CFT Compliance Officer. They will include the following minimum information:

• Details of the client: name, address, date of birth and any other details
held on Company's files;
• Details of the information which has given rise to the suspicion;
• The time and date on which the employee first became suspicious;
• The time and date of the report that the employee is making. When an employee detects a "red flag", they must file an incident report without delay to the AML/CFT Compliance Officer. The AML/CFT Compliance Officer, or its designee, will conduct an appropriate investigation to determine whether there are reasonable grounds for suspicion.

The AML/CFT Compliance Officer will consider each internal potentially suspicious transaction and determine whether it gives rise to ground of suspicion such that a SAR obligation is triggered. The AML/CFT Compliance Officer will discuss with Company's senior management to evaluate the information provided. This must be evaluated promptly.

Care must be taken by the AML/CFT Compliance Officer and the Company's employees/contractors not to alert the client to the fact that a potentially suspicious transaction is being investigated so as not to breach the offense of unlawful disclosure of an SAR (known as "Tipping Off"). Initial enquiries to verify the identity of a client and ascertain the source of funds or other relevant information to understand the nature of a transaction do not constitute tipping off.

Submitting a Suspicious Activity Report ("SAR")

Once it is determined that there are reasonable grounds for suspicion, the Company (through the AML/CFT Compliance Officer, a duly appointed designee, senior management, or an auditor, as applicable) must promptly file a Suspicious Transaction Report, known in Panama as a Reporte de Operación Sospechosa (ROS), with the Unidad de Análisis Financiero de Panamá (UAF).

The ROS should be submitted through the UAF's official electronic reporting platform ("UAF en Línea") using the applicable UAF ROS forms and instructions published by the UAF (including the UAF-SOS/ROS forms, as applicable). If urgent attention is required or guidance is needed, the Company should contact the UAF immediately and submit the ROS through the official reporting channel without delay.

UAF contact details:
Unidad de Análisis Financiero (UAF), Corozal, Calle Mackinley Este, Panamá
Telephone: +507 514-0100
Email: contactcenter@uaf.gob.pa

Confidentiality

The existence or consideration of a SAR may only be disclosed to certain people who are authorized to receive such information including law enforcement authorities or other authorities authorized by the regulations. The Company will not inform anyone outside of these authorities.

The person making a SAR is protected from civil, criminal or disciplinary action in respect of any information contained in the report, unless the information was disclosed in bad faith. The identity of that person will not be revealed except for law enforcement purposes or on the order of a court.

The AML/CFT Compliance Officer, or its designee, will be responsible to ensure that SARs are filed as required.

6. RECORD KEEPING

Regulations require the Company to keep records in a form that enables them to be available on a timely basis, when lawfully required, to the UAF or law enforcement authorities.

As a general policy, the Company will retain all records relevant to its AML/CFT Programme including those related to client due diligence measures, carried transactions and all business correspondence relating to business relationships with clients, for a period of not less than seven years.

At a minimum, records relating to transactions which must be kept will include the following information:
• The name, address, occupation of the beneficial owner,
• The nature of the business;
• The date on which the transaction was conducted;
• The form of instruction and authority;
• Details of the parties to the transaction;
• Where applicable, the facility through which the transaction was conducted and any other facilities directly involved in the transaction.

The Company will maintain records related to unusual and suspicious transaction reports, including the following:

• All reports made by staff to the AML Compliance Officer;
• The internal written findings of transactions investigated. This applies irrespective of whether a suspicious report was made;
• Consideration of those reports and of any action taken;
• Reports by the AML Compliance Officer to senior management and the board of directors.

7. UPDATING THE POLICY

Money launderers and financers of terrorism develop and modify their ML/FT methods to avoid detection and overcome Company's measures put in place to disrupt them. As a result, the Company must continue to manage and mitigate the ML/FT risks on an ongoing basis, by:

a) Checking any new products and services that we may offer for the possibility to ML/FT;
b) Following legal updates, guidance, financial crime news, or emerging ML/FT methods.

The Company has approved this policy as reasonably designed to achieve and monitor its ongoing compliance with the current and future requirements under the applicable AML/CFT Regulations.

ML and TF risks, methods and typologies can change all the time. Country risks can move up or down as their level of

AML/CFT systems and laws improves or degrades. Accordingly, the Company must ensure it keeps its written Compliance Programme up to date and under review. Any differences or deficiencies must be noted and changes made accordingly.

The Company's AML/CFT Policy will be reviewed at least every 12 months.