

**PREPARED BY:**  
Compliance Officer

**REVIEWED BY:**  
General Manager  
Audit and Risks Committees

**APPROVED BY:**  
Boards of Directors

Code: GL-M001  
Version: 00  
APPROVED: January 27th, 2026

**MANUAL ON THE  
PREVENTION AND  
MANAGEMENT OF  
RISKS RELATED TO  
MONEY LAUNDERING,  
TERRORIST FINANCING,  
AND PROLIFERATION  
FINANCING OF  
WEAPONS OF MASS  
DESTRUCTION**

## CONTENTS

1. SCOPE AND TARGET AUDIENCE
2. REGULATORY FRAMEWORK
  - 2.1. INTERNATIONAL REGULATORY FRAMEWORK
  - 2.2. PERUVIAN REGULATORY FRAMEWORK
3. OBJECTIVES OF THE MANUAL
4. POLICIES FOR THE PREVENTION OF MONEY LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING OF WEAPONS OF MASS DESTRUCTION
5. DEFINITIONS
6. GENERAL MECHANISMS
7. ROLES AND RESPONSIBILITIES OF DIRECTORS, MANAGERS, EMPLOYEES, AND THE COMPLIANCE OFFICER
8. COMMUNICATION
9. TRAINING PROGRAM FOR DIRECTORS AND EMPLOYEES
10. TRANSACTION RECORDING PROCEDURE
11. PROCEDURE FOR DUE DILIGENCE IN KNOWING THE CUSTOMER AND THE BENEFICIAL OWNER
12. DUE DILIGENCE PROCEDURE FOR EMPLOYEES AND DIRECTORS
13. DUE DILIGENCE PROCEDURE FOR SUPPLIERS
14. RED FLAGS FOR THE DETECTION OF UNUSUAL OR SUSPICIOUS TRANSACTIONS
15. PROCEDURE FOR UNUSUAL TRANSACTIONS AND SUSPICIOUS TRANSACTIONS REPORT
16. REVIEW OF WATCHLISTS AND PROCEDURE FOR THE ADMINISTRATIVE FREEZING OF FUNDS OR ASSETS
17. PROCEDURE FOR RECORDING, FILING, RETENTION, AND DISCLOSURE OF RECORDS, REPORTS, AND OTHER INFORMATION OR DOCUMENTATION OF THE SPLAFT
18. SEMIANNUAL REPORT BY THE COMPLIANCE OFFICER
19. COMPLIANCE OFFICER'S ROLE IN IDENTIFYING AND ASSESSING OF ML/TF AND PF RISKS
20. USE OF THIRD PARTIES OR INTERMEDIARIES
21. CONFIDENTIALITY OBLIGATION
22. APPROVAL OF THIS MANUAL
23. ANNEXES

## 1. SCOPE AND TARGET AUDIENCE

This Manual for the Prevention and Management of Risks Related to Money Laundering, Terrorist Financing, and Proliferation Financing of Weapons of Mass Destruction (hereinafter, the Manual) is intended to establish the basic mechanisms, policies, and procedures that must be observed and applied by Corporación Aceros Arequipa S.A. (hereinafter, the Company), within the framework of operations related to the production of lime for use in the company's production processes and the commercialization of surplus production, with the aim of preventing the Company from being used for illicit purposes linked to the crimes of money laundering, terrorist financing, and proliferation financing of weapons of mass destruction (ML/TF and PF).

This Manual is mandatory and must be applied by general management, shareholders, directors, control or administrative bodies, authorized representatives, the Compliance Officer, and all employees of the Company who participate directly or indirectly in such operations, who must follow the general guidelines established in the Code of Conduct of the ML/FT and PF Prevention System, the Internal Work Regulations, policies, rules, and procedures to prevent and avoid any connection with any illicit activity that could compromise the Company and the Prevention System in general.

## 2. REGULATORY FRAMEWORK

### 2.1. INTERNATIONAL REGULATORY FRAMEWORK

- The 40 Recommendations of the FATF (Financial Action Task Force).
- The 9 Recommendations of the GAFILAT (Latin American Financial Action Task Force).
- Inter-American Convention against Terrorism.
- United Nations Convention against Corruption.
- United Nations Convention against Transnational Organized Crime.
- International Convention for the Suppression of the Financing of Terrorism.
- Regulations of the Inter-American Drug Abuse Control Commission

- (CICAD/OAS).
- Resolutions of the United Nations Security Council.

## 2.2. PERUVIAN LEGAL FRAMEWORK

- Decree-Law No. 25475 and its amendments, Law establishing penalties for terrorist offenses and procedures for investigation, prosecution, and trial (05/06/1992).
- Law No. 27693 and its amendments, Law establishing the Financial Intelligence Unit of Peru (04/12/2002).
- Law No. 29038, Law incorporating the Financial Intelligence Unit of Peru (UIF-Peru) into the Superintendency of Banking, Insurance, and Private Pension Fund Administrators (06/12/2007).
- SBS Resolution No. 8930-2012, which approves the Regulations on Infractions and Sanctions regarding the Prevention of Money Laundering and Terrorist Financing (12/01/2012), as well as its amending provisions.
- Legislative Decree No. 1106, Legislative Decree on the Effective Fight against Money Laundering and Other Crimes Related to Illegal Mining and Organized Crime (04/19/2012).
- Circular SO-2-2016 on the submission of the Compliance Officer's Annual Report to the UIF-Peru via electronic means.
- Law No. 30437, Law amending Article 3 of Law 27693, Law establishing the Financial Intelligence Unit - Peru to expand its powers in the fight against terrorism.
- SBS Resolution No. 3862-2016 approves regulation governing the mechanisms and procedures for the UIF-Peru to administratively freeze the funds or other assets of persons or entities linked to terrorism and the financing of terrorism, as well as those linked to the proliferation of weapons of mass destruction and their financing, identified within the framework of United Nations Security Council Resolutions.
- SBS Resolution No. 4349-2016, Regulation on the functions and positions held by politically exposed persons (PEPs) in the area of the prevention of money laundering and the financing of terrorism, amended by SBS Resolution No. 00199-2025.
- Legislative Decree No. 1249, a legislative decree establishing measures to strengthen the prevention, detection, and punishment of money laundering

- and terrorism.
- SBS Resolution No. 2794-2019, which establishes the obligation to submit the Semi-Annual Reports of the Compliance Officer referred to in Article 10 of Law No. 27693.
- Supreme Decree No. 020-2017-JUS, Regulations of Law No. 27693.

### 3. OBJECTIVES OF THE MANUAL

#### MAIN OBJECTIVE:

- a. To comply with legal regulations and best practices regarding the Prevention of Money Laundering, Terrorist Financing, and Proliferation Financing of Weapons of Mass Destruction, through policies and procedures designed to prevent and identify such activities in a timely manner within the framework of the Company's operations as a reporting entity under the Financial Intelligence Unit of Peru (UIF-Peru).

#### SECONDARY OBJECTIVES:

- b. To organize mechanisms for the identification, recording, control, and monitoring of unusual and/or suspicious transactions detected by the Compliance Officer in the course of their duties.
- c. To establish policies that ensure the duty of confidentiality and secrecy.
- d. To reduce the likelihood that the Company may be used for illegal activities carried out by general management, shareholders, directors, control or administrative bodies, authorized representatives, the Compliance Officer, and employees in general.

#### 4. POLICIES FOR THE PREVENTION OF MONEY LAUNDERING, TERRORIST FINANCING, AND PROLIFERATION FINANCING OF WEAPONS OF MASS DESTRUCTION

- a. Collaborate in the fight against money laundering, terrorist financing, and proliferation financing of weapons of mass destruction, ensuring the proper functioning of the ML/TF and PF Prevention System.
- b. Comply with the laws and regulations applicable to the business activities it conducts and those related to the Prevention of Money Laundering, Terrorist Financing, and Proliferation Financing of Weapons of Mass Destruction, in order to reduce its exposure to the risk of being used in ML/TF and PF activities.
- c. Comply with the general guidelines established in this Manual and Code of Conduct of the ML/TF and PF Prevention System.
- d. Know and assess its employees and customers, whether regular or occasional.
- e. Verify and record the identity of the Company's employees and customers based on valid documents (e.g., National ID Card, Tax ID certificate, certified copy of the registry entry, among others).
- f. Not to establish or maintain business relationships with customers whose activities are of questionable legality or who are linked to ML/TF and PF offenses.
- g. Cooperate with the UIF-Peru, the Public Prosecutor's Office, the Peruvian National Police, and other entities linked to the Prevention System in all matters related to the provision of information and the detection of possible cases of ML/TF and PF.

#### 5. DEFINITIONS

1. **Beneficiary:** The natural person or legal entity in whose favor the transaction is carried out.
2. **Beneficial Owner:** The natural person who ultimately owns or effectively controls a company, entity, or customer, or who carries out or benefits from a transaction, even if control is exercised indirectly through other persons, companies, or intermediaries.
3. **Sound Judgment:** The Company's ability to discern or assess the risk of Money Laundering, Terrorist Financing, or Proliferation Financing in the Company's operations or transactions, based on knowledge of the customer and standard market transactions.

- 4. Customer:** Any natural person or legal entity, whether domestic or foreign, to whom CAASA sells regulated lime in exchange for financial compensation.
- 5. SPLAFT Code of Conduct:** This is the document that must contain, among other aspects, the guiding principles, values, and policies to be applied in managing the risk of exposure to Money Laundering, Terrorist Financing, and Proliferation Financing of Weapons of Mass Destruction; as well as measures to ensure the duty of confidentiality regarding information related to the ML/TF Prevention System.
- 6. Employee:** Any personnel involved in the ML/TF Prevention System related to the sale of lime who maintains an employment or contractual relationship with the reporting entity. This includes the general manager, managers, administrators, or those holding similar positions.
- 7. Identification Document:** National identity card for Peruvian citizens, and a foreigner's ID card, passport, or legally established document for the identification of foreigners, as applicable.
- 8. Executor:** The natural person who requests or physically carries out the transaction.
- 9. Legal Arrangements:** These are i) autonomous assets managed by third parties that lack legal personality or ii) contracts in which two or more persons, who temporarily associate, have a common right or interest in carrying out a specific activity, without constituting a legal entity. This category includes investment funds, mutual funds investing in securities, trust estates, and consortia, among others.
- 10. Terrorist Financing:** This is the act of providing, contributing, or collecting funds, financial or economic resources, directly or indirectly, for the purpose of using them to commit terrorist acts, or to sustain the existence, operation, or activities of a terrorist group or individuals linked to terrorism.
- 11. Proliferation Financing of Weapons of Mass Destruction:** This is understood to mean any act by which funds or financial services are provided, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer of material, disassembly, transport, transfer, storage, or use of nuclear, chemical, or biological weapons and their delivery systems and related materials.

- 12. ML/TF and PF Risk Management:** A set of objectives, policies, mechanisms, procedures, internal rules, and actions implemented to identify, measure, monitor, mitigate, and control the various risks associated with money laundering, terrorist financing, and proliferation financing of weapons of mass destruction to which the Company is exposed.
- 13. Money Laundering:** The process by which assets, money, or proceeds derived from illicit activities are acquired, converted, transferred, concealed, or used, with the aim of giving them the appearance of legality and incorporating them into the formal economic system, thereby making it difficult to identify their true illicit origin.
- 14. OFAC List:** A list issued by the Office of Foreign Assets Control of the U.S. Department of the Treasury (OFAC), which includes countries, individuals, and/or entities that, in the judgment of the United States, support terrorism and illicit drug trafficking.
- 15. Unusual Transactions:** Transactions carried out or attempted whose amount, characteristics, or frequency are not consistent with the customer's economic activity, deviate from normal market parameters, or lack an obvious economic or legal justification. Their detection constitutes an alert requiring further analysis by the Compliance Officer to determine whether they can be classified as suspicious.
- 16. Suspicious Transactions:** Transactions carried out or attempted that, following the corresponding analysis, have no apparent economic, legal, or commercial justification, and which, due to their nature, amount, frequency, or particular characteristics, reasonably suggest the existence of funds derived from criminal activities or intended to finance such activities.
- 17. Originator:** A natural person or legal entity in whose name the transaction is carried out.
- 18. Supervisory Body:** An entity responsible for overseeing the proper functioning of the ML/TF Prevention System. In this case, the supervisory body is the Financial Intelligence Unit of Peru (UIF-Peru).
- 19. Politically Exposed Persons (PEP):** Natural persons, whether nationals or foreigners, who hold, or have held in the last two (2) years, prominent public office or prominent positions in an international organization, whether within the national territory or abroad, and whose financial circumstances may be of public interest. Likewise, a direct report of the institution's highest authority is

considered a PEP.

- 20. Transaction Register:** A record that the reporting entity must maintain, verify, retain, and submit to the UIF-Peru, containing accurate and complete information regarding both the transaction and the customer and/or participants in each transaction conducted when the amount of the transaction equals or exceeds the threshold established in current regulations or is a type of transaction that, due to its characteristics, has no threshold or cannot be defined at the time the transaction is executed.
- 21. Regulations:** Regulations of the Law establishing the UIF-Peru, approved by Supreme Decree No. 020-2017-JUS.
- 22. ML/TF and PF Risks:** The possibility that the Company may be used for the purposes of Money Laundering, Terrorist Financing, and Proliferation Financing of Weapons of Mass Destruction. This definition excludes reputational and operational risks.
- 23. Inherent Risk:** The risk (risk event) inherent in an activity, person, or condition, without taking into account the effect of applying mitigating controls.
- 24. Residual Risk:** The risk remaining after applying mitigating controls.
- 25. STR:** Suspicious Transaction Report.
- 26. ROSEL:** Online Suspicious Transaction Reporting System.
- 27. SBS:** Superintendency of Banking, Insurance, and Private Pension Fund Administrators.
- 28. Red Flags:** Situations or transactions that deviate from the norm and serve as a tool for the reporting entity, through the compliance officer, to identify unusual or suspicious transactions.
- 29. SPLAFT:** Money Laundering and Terrorist Financing Prevention System
- 30. Reporting Entity:** A natural person conducting business or a legal entity incorporated in Peru that, due to the nature of its economic or professional activities, is required to implement a Money Laundering and Terrorist Financing Prevention System (SPLAFT). This definition also includes branches of legal entities incorporated and domiciled abroad.

## 6. GENERAL MECHANISMS

The methodology applied for the implementation of the SPLAFT has taken into account the Risk-Based Approach (RBA). In this regard, the Company has assessed and identified its risks through the ML/TF and PF risk management process, which includes the following stages:

- **Identification stage:** This consists of developing and implementing procedures to obtain the information necessary to determine the identity of the customer and, where applicable, their beneficial owner. At this stage, the counterparty must complete the form with accurate and complete information. Company employees must not fill it out on behalf of third parties, and the forms must be duly signed.
- **Verification stage:** This involves applying procedures designed to verify the accuracy and consistency of the information provided by the customer and their beneficial owner, ensuring that both have been correctly identified.
- **Monitoring stage:** The purpose of this stage is to verify that the transactions carried out by customers are consistent with their economic profile and the information previously provided. This phase helps to deepen our understanding of customers, detect unusual behavior, and update data when there are doubts about its validity or authenticity.

### 6.1. THE COMPANY'S ML/TF AND PF RISK MANAGEMENT PROCESS

Within the framework of CAASA's **Comprehensive Risk and Opportunity Management Methodology (GIRO)**, the Board of Directors has mandated the incorporation of **Money Laundering, Terrorist Financing, and Proliferation Financing (ML/TF and PF)** risks into the comprehensive risk management system, in accordance with the Corporate Policy on Internal Control and Risk Management and the Company's strategic objectives. In doing so, the Board reaffirms its commitment to the implementation and sustainability of **the SPLAFT**, while also ensuring the independence of the **Compliance Officer** and the provision of the

necessary resources for the system's proper functioning.

In accordance with applicable regulations, the Company has identified customers, suppliers, and employees as relevant stakeholders for managing these SPLAFT risks. The Compliance Officer is responsible for keeping the ML/TF and PF Risk Matrix up to date through the risk identification and assessment process, and may require the support of the heads of the various departments. This matrix must be updated at least every two (02) years, or whenever there are significant changes in risks, controls, or materialized events. The ML/TF and PF Risk Matrix is managed through the processes involved in the commercialization of lime and is available for audits conducted at the Company.

## 7. ROLES AND RESPONSIBILITIES OF DIRECTORS, MANAGERS, EMPLOYEES, AND THE COMPLIANCE OFFICER

In accordance with the Internal Work Regulations, employees, directors, and managers must comply with the provisions established in the Manual for the Prevention and Management of Risks Related to Money Laundering, Terrorist Financing, and Proliferation Financing of Weapons of Mass Destruction, the SPLAFT Code of Conduct, and any other regulations implemented by the company.

Likewise, they must promptly report any red flags they detect that affect or may affect the Company's operations. Such reports must be made immediately to the Compliance Officer at or via email to [Oficialdecumplimiento@acerosarequipa.com](mailto:Oficialdecumplimiento@acerosarequipa.com).

### 7.1. BOARD OF DIRECTORS

- Implement and monitor the SPLAFT through the Audit and Risk Committee in accordance with current regulations and foster an internal environment that facilitates its development.
- Adopt and periodically review policies for managing ML/TF and PF risks.
- Approve the SPLAFT Code of Conduct.
- Periodically review the operation of the SPLAFT based on the Company's ML/TF

- and PF risk profile.
- Appoint a Compliance Officer with the qualifications, responsibilities, and authority established by current regulations.
- Establish measures to maintain the confidentiality of the Compliance Officer and ensure that his or her identity is not disclosed to persons outside the Company.
- Provide the resources (human, technological, among others) and infrastructure necessary to ensure the proper fulfillment of the Compliance Officer's duties and responsibilities.
- Approve the Compliance Officer's Semi-Annual Report (ISOC) following review by the Board's Audit and Risk Committee.

## **7.2. GENERAL MANAGEMENT**

- Manage and supervise the allocation of the necessary resources to ensure the implementation of the SPLAFT, in accordance with current regulations.
- Comply with measures related to the control of ML/TF and PF risks, in accordance with defined policies and procedures, supporting the Compliance Officer in the performance of their duties.
- Represent the Company before the UIF-Peru.
- Notify the UIF-Peru of the appointment and/or removal of the Compliance Officer.

## **7.3. COMPLIANCE OFFICER**

- Serve as the Company's liaison with the supervisory authority on matters related to their role.
- Propose strategies to prevent and manage ML/TF and PF risks.
- Monitor the proper implementation and operation of the Company's SPLAFT, including procedures for the timely detection and reporting of suspicious transactions.
- Implement, evaluate, and verify the application of the SPLAFT's policies and procedures.
- Propose and adopt the necessary measures for training the Compliance Officer,

- employees, and directors—where applicable—as well as the reporting entity when it is a natural person, at least once a year on the prevention and detection of ML/TF and PF, including the proper management of ML/TF and PF risks.
- Verify, at the outset and throughout the business relationship with the customer, the lists of persons or entities designated by the United Nations Security Council for their links to terrorism and its financing, as well as the proliferation financing of weapons of mass destruction, in accordance with Resolutions 1267 (1999), 1718 (2006), 1737 (2006), and 2231 (2015) and any subsequent resolutions.
- Verify, at the outset and throughout the business relationship with the customer, the lists that contribute to the prevention of ML/TF: i) OFAC List: a list issued by the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury, which includes countries, individuals, and/or entities involved in terrorism and illicit drug trafficking; ii) European Union Terrorist List, iii) List of Non-Cooperative Countries and Territories, iv) List of United Nations Security Council Resolutions, other than those indicated in the preceding paragraph, v) Others designated by the Superintendency.
- Report on modifications and additions to the list of high-risk and non-cooperative countries published by the Financial Action Task Force (FATF).
- Verify, with due follow-up, the immediate implementation of national asset or fund freezing measures ordered by the SBS in cases related to ML/TF and PF offenses, in accordance with paragraph 11 of Article 3 of Law No. 27693.
- Verify, with appropriate follow-up, the immediate implementation of freezing measures ordered by the SBS, in accordance with United Nations Security Council Resolutions regarding terrorism and its financing, as well as the proliferation financing of weapons of mass destruction.
- Maintain a record of those unusual transactions that, following the respective analysis, were not determined to be suspicious.
- Notify directors, managers, and employees of changes made to current regulations regarding the fight against ML/TF and PF offenses, and in particular the regulations related to the SPLAFT, keeping a record of such notifications.
- Evaluate transactions and, where appropriate, classify them as suspicious and report them to the UIF-Peru through a Suspicious Transaction Report (STR), maintaining a written record of the analysis and evaluations conducted. This

- report is submitted within the timeframe established by current regulations.
- Prepare and submit the Compliance Officer's Semi-Annual Report (ISOC) to the UIF-Peru within the established timeframe.
- Verify the proper retention and safekeeping of documents related to the SPLAFT.
- Respond to information requests made by the competent authorities.
- Respond to information requests made by the UIF-Peru, including those requiring periodic submission.
- Participate in the evaluation of proposals for the launch of new products and entry into new markets, among other matters.
- Develop the Compliance Officer's Annual Work Plan.
- Develop the Annual Training Program.
- Perform any other duties deemed necessary or established by the SBS to monitor the operation and level of compliance of the SPLAFT.
- Establish internal mechanisms to sanction violations of regulations regarding the Prevention of ML/TF and PF, as well as the Manual and the Code, and update them as applicable.

#### **7.4. EMPLOYEES IN GENERAL**

- Protect the identity of the Compliance Officer.
- Report in a timely manner to the Compliance Officer any red flags identified in the course of their duties that may link the Company to potential ML/TF or PF risks.
- Comply with the procedures defined in this Manual to mitigate ML/TF and PF risk situations.
- Attend training sessions on the Prevention and Management of ML/TF and PF Risks.

#### **7.5. PRODUCTION AND SALE OF REGULATED LIME**

- Comply with and implement procedures for the production of regulated lime and due diligence regarding customer information.
- Request and collect all relevant information regarding the identity of the customer, whether a natural person or a legal entity.

- Be responsible for ensuring that customer knowledge sworn statements are properly completed.
- Be responsible for screening the customer against the watchlists indicated in Annex No. 05, through the platform provided by the Company.
- Report any unusual transactions, activities, or situations involving customers to the Compliance Officer for analysis.
- Verify all information submitted by customers.
- Act as intermediaries between the Company and customers in cases where the Compliance Officer requires additional information to evaluate a suspicious transaction.

## 7.6. HUMAN RESOURCES

- Request and verify references, personal and employment history, as well as the credit history of personnel at the time of establishing the employment relationship. To this end, the applicant will be asked to complete the Sworn Statement, in coordination with the Legal Department. **(See Annex No. 01)**
- Safeguard and preserve the Sworn Statement of Receipt, Acknowledgment, and Commitment to Compliance with the SPLAFT Manual and Code of Conduct. **(See Annex No. 02)**
- Screen the employee against the watchlists indicated in **Annex No. 05** prior to hiring, using the system provided by the Company.
- Support the Compliance Officer in conducting training related to the prevention of ML/TF and PF for all personnel, including training for Directors and the Compliance Department.
- Report any unusual situation involving an employee to the Compliance Officer for analysis, so that appropriate actions can be taken.

## 7.7. SUPPLIERS RELATED TO REGULATED LIME OPERATIONS

- Be responsible for gathering and verifying all information necessary for an adequate due diligence process regarding suppliers.
- Be responsible for screening the supplier against the watchlists indicated in Annex No. 05, prior to contracting them, through the system provided by the Company.

- Report to the Compliance Officer any red flags identified during the supplier's hiring process or term of engagement.

## 7.8. INTERNAL AUDIT

- Evaluate the design and implementation of the SPLAFT through an annual audit, presenting observations and recommendations aimed at improving the Prevention System.
- The conclusions of the report must be submitted to the UIF-Peru as an annex to the Compliance Officer's Annual Report.
- In coordination with the Board's Audit and Risk Committee, engage the external auditor responsible for the annual independent evaluation of the SPLAFT model, and submit observations and recommendations aimed at improving the Prevention System. The external auditor shall submit the results of this evaluation directly to the UIF-Peru.

## 8. COMUNICACIÓN

The communication channel for the purposes related to the SPLAFT is as follows:

- The employee should send an email to [Oficialdecumplimiento@acerosarequipa.com](mailto:Oficialdecumplimiento@acerosarequipa.com) with the customer's name in the subject line, providing a brief summary of the sale and explaining why it is considered a red flag. Scanned copies of all documents requested in the customer's file must be attached to this email.
- It is strictly prohibited to disclose, by any means, information related to identified unusual or suspicious transactions.

**Guidelines for communication between the Compliance Officer and all Company departments:**

- The Compliance Officer will address all employee inquiries related to the SPLAFT.
- The management of each department is responsible for ensuring compliance

- with all SPLAFT procedures, standards, and policies.
- The Compliance Officer is responsible for forwarding any information related to unusual or suspicious transactions.
- Management in each area will coordinate various preventive measures with the Company's Compliance Officer.

## 9. TRAINING PROGRAM FOR DIRECTORS AND EMPLOYEES

The Company is committed to ensuring that all directors and employees are properly trained in ML/TF and PF prevention. To this end, it will develop periodic training programs for all directors and employees to instruct them on current regulations, as well as on the policies, rules, and procedures established by the Company regarding the Prevention of Money Laundering, Terrorist Financing, and Proliferation Financing of Weapons of Mass Destruction.

### 9.1. General guidelines regarding training:

- All managers and employees must receive at least one training session per year related to the SPLAFT.
- The Compliance Officer is responsible for developing the Annual Training Program on ML/TF and PF, in coordination with Human Resources Management.
- Training may be conducted through any physical or electronic means deemed appropriate, provided that a record of such training is maintained in the employee's personal file, whether in physical and/or electronic form. For this purpose, the Company may implement electronic records of individual training for each employee, in which the aforementioned records are maintained, and which shall have the same validity as physical records.
- If the training was conducted by the Compliance Officer, the Officer must issue a certificate in the form of a sworn statement to be included in the records for each director or employee. This sworn statement must specify the date, location, duration, format, and topics of the training, as well as the full names and job titles of the individuals trained. A training certificate issued by the Compliance Officer on his or her own behalf is not permitted.
- New employees and directors joining the Company must receive training (orientation) on the scope of the Company's SPLAFT, in accordance with their respective duties, no later than thirty (30) days following their start date.

- The appropriate disciplinary measure must be applied to those directors or employees who have not participated in the training or taken the assessment without a valid justification. If they have a valid justification, they will participate in the next respective orientation.
- As part of their duties, the Compliance Officer will be responsible for communicating changes to the Company's internal SPLAFT regulations to all directors and employees.

## **9.2. In accordance with the duties performed, annual training sessions shall cover at least the following topics:**

- Definition of the Money Laundering and Terrorist Financing offenses.
- Company policies and procedures regarding the Prevention and Management System for ML/TF and PF risks.
- ML/TF and PF risks to which the Company is exposed.
- Current regulations on ML/TF and PF Prevention.
- ML/TF and PF typologies detected in the business.
- The Company's internal policies.
- Red flags for detecting unusual and suspicious transactions.
- Procedure for reporting unusual transactions.
- Information on the lists that contribute to ML/TF and PF Prevention.
- Regarding the freezing of funds or assets in cases related to ML/TF and PF offenses ordered by the SBS, pursuant to paragraph 11 of Article 3 of Law No. 27693 and/or the freezing of funds or assets pursuant to United Nations Security Council Resolutions regarding terrorism, terrorist financing, and the proliferation financing of weapons of mass destruction, pursuant to paragraph 12 of the aforementioned article.
- Responsibilities of directors and employees regarding the ML/TF and PF Prevention, in accordance with their area of expertise and the duties they perform.

## **9.3. Training for the Compliance Officer and team:**

- The Compliance Officer and support personnel must receive at least one (1) annual training session, separate from those provided to Company employees, in order to be instructed on the management of ML/TF and PF risks.

## 10. PROCEDURE FOR RECORDING TRANSACTIONS

The Company must maintain and keep up to date a transaction register (RO) in accordance with the provisions of Article 24 of the Regulations of Law No. 27693. The RO is confidential.

The OR must record the transactions carried out by our customers on the day they were invoiced. This OR is retained for a minimum of ten (10) years from the date the transaction was carried out and is maintained in a chronological, accurate, and complete manner, and the Company shall maintain a backup copy on backup media implemented for that purpose.

The record for each commercial transaction must contain, at a minimum, the following:

a) Information regarding the identification of the individuals involved in the transaction, in the roles of originators, executors, and/or beneficiaries of the transaction:

- In the case of a natural person, their full name, type and number of identification document, nationality (if a foreigner), address, profession or occupation, marital status, and name of spouse or cohabiting partner (if applicable), as well as details of the power of attorney, must be recorded.
- In the case of a legal entity, the corporate name, the Unique Taxpayer Identification Number or its equivalent, the SUNARP Registry Entry number, the tax and legal addresses, and the name of the legal representative, for whom the data corresponding to a natural person must be recorded.
- The identification of the person physically carrying out the transaction (executor), as well as the person on whose behalf the transaction is carried out (originator), and the person in whose favor the transaction is carried out (beneficiary), must be recorded in the RO, as applicable.

For these purposes, the customer must be required to present an identity document (National ID Card, Passport, Foreigner's ID Card) at the time of establishing the business relationship and, particularly, when conducting a

transaction.

Data related to the transaction: modality (single or multiple), type, date, type of asset involved in the transaction, description of the goods or services, transaction amount, currency in which the transaction is conducted, exchange rate (if applicable), means of payment used, account(s) involved (where applicable), locations where the transaction took place, date and method of payment, type and amount of the guarantee, origin of the funds or assets involved, period (if applicable).

The Company must record transactions whose amounts exceed the established threshold, as detailed below:

<b>Companies that produce and market chemical inputs and regulated goods</b>	<b>Single transaction (amount equal to or greater than USD)</b>	<b>Multiple transaction (amount equal to or greater than USD)</b>
<b>Lime Commercialization</b>	<b>\$10,000.00</b>	<b>\$50,000.00</b>

## 11. DUE DILIGENCE PROCEDURE FOR KNOWING THE CUSTOMER AND THE BENEFICIAL OWNER

### 11.1. OBJECTIVES OF KNOW YOUR CUSTOMER

The primary objective of customer due diligence is to reduce the risk that, through action or omission, the Company may become involved in potential Money Laundering, Terrorist Financing, and Proliferation Financing of Weapons of Mass Destruction. In other words, it prevents the goods, products, or services offered by the Company from being used to legitimize funds derived from illicit activities. Through due diligence, the Company seeks to promote sound business practices, compliance with the law, and the protection of its reputation.

### 11.2. CUSTOMER DUE DILIGENCE

This procedure applies to all customers involved in lime commercialization, and the following forms are used to comply with it: Sworn Statement of Know Your

Customer for Natural Persons (Annex No. 03) and Sworn Statement of Know Your Customer for Legal Entities and Legal Arrangements (Annex No. 04).

The Company shall identify the customer and the beneficial owner for each transaction at the time of establishing business relations and throughout the course of the business relationship, regardless of the transaction's specific details, characteristics, and/or frequency, and shall take reasonable measures to verify their identity to the extent permitted by due diligence, so as to be satisfied that the beneficial owner is known. In the case of natural persons and legal arrangements, for the purpose of determining the beneficial owner, the provisions of Article 4 of Legislative Decree No. 1372 and its amending regulations must be taken into account.

In this regard, a natural person shall be considered a beneficial owner if they: (i) directly or indirectly hold at least 10% of the share capital; (ii) exercise effective control through the ability to influence financial, operational, or governance decisions; or, (iii) failing that, hold the highest administrative position.

With respect to legal arrangements, natural persons who are settlors, trustees, beneficiaries, participants, or investors, or who exercise ultimate effective control over the assets, results, or profits, shall be considered beneficial owners. In the case of other legal arrangements or similar structures, such as foreign law trusts, the natural person holding an equivalent position shall be identified as the beneficial owner, including the protector or administrator, where applicable.

#### A. GENERAL REGIME:

The general due diligence process for identifying the customer and beneficial owner consists of three stages:

- **Identification:** This involves applying procedures to obtain minimum information necessary to establish the identity of the customer and the beneficial owner.
- **Verification:** This involves applying verification procedures regarding the information provided by the customer or the beneficial owner to ensure that they have been properly identified.

- **Monitoring:** Its purpose is to ensure that the transactions carried out by customers are consistent with the information declared by the customers (profile). Monitoring allows regulated entities to reinforce and reaffirm their knowledge of their customers, as well as to obtain further information when there are doubts regarding the accuracy or validity of the data provided by customers. Reporting entities must determine the frequency with which they perform this stage, taking into account the ML/TF and PF risks they face, where applicable.

These stages will be carried out as follows:



## a) Identification Stage

Employee responsible for this stage	Activities to be performed in this stage	
Person responsible for the sale	<b>Step 1: Information must be requested from the customer</b>	
	<p><b>If the customer is a natural person, the minimum information required is as follows:</b></p> <ul style="list-style-type: none"> <li>- First and last names.</li> <li>- Type and number of identification document.</li> <li>- Nationality.</li> <li>- Address.</li> <li>- Occupation.</li> <li>- Employment status or place of work.</li> <li>- Marital status.</li> <li>- Name of spouse if married or cohabiting.</li> <li>- Date of birth.</li> <li>- Phone number, if applicable.</li> <li>- Purpose of the relationship to be established with the reporting entity, provided that this is not directly apparent from the subject matter of the contract.</li> <li>- Source of the funds/assets involved in the transaction.</li> <li>- Whether the customer is or has been a PEP.</li> <li>- If the customer indicates that they are a PEP, enhanced due diligence measures must be applied.</li> </ul>	<p><b>If the customer is a legal entity, the minimum information required is as follows:</b></p> <ul style="list-style-type: none"> <li>- Corporate name.</li> <li>- Date of incorporation of the company.</li> <li>- Unique Taxpayer Identification Number (RUC) or equivalent registration number for non-residents.</li> <li>- Corporate purpose, principal economic activity, or purpose of incorporation of the legal entity, as applicable.</li> <li>- Identification of its ultimate beneficial owners, in accordance with Article 4 of Legislative Decree No. 1372 and its amendments.</li> <li>- Purpose of the relationship to be established with the reporting entity, provided that this is not directly apparent from the subject matter of the contract.</li> <li>- Identification of the representative (executor).</li> <li>- Specify whether the executor is acting under a power of attorney or mandate, indicating the details of the notarized public instrument and the SUNARP Registry Entry number, category, entry, and Registry Zone.</li> <li>- Address and telephone number of the main office or premises where the activities specific to the business line are carried out.</li> <li>- Source of the funds/assets involved in the transaction.</li> </ul>
<p>The information shall be collected through the following forms:</p> <ul style="list-style-type: none"> <li>• Sworn Statement of Due Diligence on Customers for Natural Persons. <b>(Annex No. 03)</b></li> <li>• Sworn Statement of Due Diligence on Customers for Legal Entities and Legal Arrangements. <b>(Annex No. 04)</b></li> </ul> <p>These sworn statements allow us to identify the beneficial owner of the transaction. If it is determined that the beneficial owner is different from the natural person or legal entity that conducted the transaction, we must collect the following information:</p> <p>If the transaction is conducted on behalf of a third party, a natural person, the following is required:</p> <ol style="list-style-type: none"> <li>a) First and last names of the natural person.</li> <li>b) Type and number of identification document.</li> <li>c) Details of the representation (if acting under power of attorney and if this is by public deed) or mandate.</li> <li>d) Indicate whether the individual is or has been a PEP, specifying, if applicable, the position and the name of the institution (public body or international organization), and</li> <li>e) The origin of the funds involved in the transaction, when it is conducted in cash and equals or exceeds the threshold for purposes of the RO.</li> </ol> <p>If the transaction is conducted on behalf of a legal entity:</p> <ol style="list-style-type: none"> <li>a) Its corporate name.</li> <li>b) Tax ID No. (RUC), if applicable.</li> <li>c) Details of the representation (whether acting under power of attorney and whether such power of attorney is by public deed) or mandate.</li> <li>d) Origin of the funds/assets involved in the transaction, when it is conducted in cash and meets or exceeds the threshold for purposes of the RO.</li> <li>e) Identification of the beneficial owner of the transaction beneficiary, in accordance with Article 4 of Legislative Decree No. 1372 and its amendments, as applicable.</li> </ol>		

## b) Verification stage

Employee responsible for this stage	Activities to be performed in this stage
<p><b>Person responsible for the sale</b></p>	<p><b>Step 2: The information provided by the customer must be verified</b></p>
	<p>The information provided by the customer and their legal representative (in the case of a legal entity) is verified:</p> <ul style="list-style-type: none"> <li>• Requesting the presentation of a physical ID for natural persons and a Tax ID certificate for legal entities.</li> <li>• Verifying the address using copies of utility bills.</li> <li>• Verifying against watchlists that contribute to the prevention of Money Laundering, Terrorist Financing, and Proliferation Financing of Weapons of Mass Destruction (PEP List, OFAC List, UN List, etc.) through the system provided by the Company.</li> <li>• Verifying the validity of the power of attorney (SUNARP) provided by the customer.</li> <li>• Other actions or searches deemed necessary depending on the specific case.</li> </ul>
<p><b>Compliance Officer</b></p>	<p>For customers considered <b>high-risk</b> and/or subject to enhanced due diligence regime, in addition to the information verified in the previous point, the <b>Compliance Officer</b> must verify the following information:</p> <ul style="list-style-type: none"> <li>• Verify the authenticity of the identity document on public source websites. Example: SUNAT, ESSALUD, GOOGLE.</li> <li>• Verify the legal entity's status with SUNAT.</li> <li>• Verify with credit bureaus.</li> <li>• Verify the customer's occupation on the ESSALUD and SUNAT websites.</li> <li>• Take any other actions deemed necessary depending on the specific case.</li> <li>• Verify whether the transaction exhibits red flags that would classify it as unusual and/or suspicious, as applicable.</li> </ul>

c) **Monitoring stage**

Employee responsible for this stage	Activities to be performed in this stage
<p><b>Compliance Officer</b></p>	<p><b>Step 3: Transactions between the customer and the Company must be monitored</b></p>
	<p>Once the relationship with the customer has been established, transactions must be monitored:</p> <ul style="list-style-type: none"> <li>• The Compliance Officer shall review customers in the Transaction Register to verify whether they have been added to the watchlists specified in <b>Annex No. 05</b> on an annual basis.</li> </ul>

**B. ENHANCED REGIME:**

The application of this regime requires the reporting entity to develop and implement enhanced customer due diligence procedures, in addition to those of the general regime. To this end, it identifies and registers under this regime those customers who exhibit a pattern inconsistent with their ML/TF and PF risk profile, as well as those customers who could be highly exposed to ML/TF and PF risks.

This regime applies to the following customers:

**ACEROS  
AREQUIPA**

To whom does it apply?	What additional due diligence measures have been implemented?
<ul style="list-style-type: none"> <li>• Domestic or foreign non-residents.</li> <li>• Non-domiciled legal entities.</li> <li>• Trusts.</li> <li>• PEPs and identified as:               <ul style="list-style-type: none"> <li>i) relatives of the PEP up to the second degree of consanguinity and second degree of affinity,</li> <li>ii) spouse or cohabiting partner of a PEP; and,</li> <li>iii) natural persons or legal arrangements in which a PEP is the beneficial owner, in accordance with Article 4 of Legislative Decree No. 1372 and its amendments.</li> </ul>               This applies to the customer when they become a PEP after having established a business relationship.             </li> <li>• Natural persons, legal entities, or legal arrangements known to be under investigation by the competent authorities for money laundering and predicate offenses, and/or terrorist financing.</li> <li>• Customers associated with natural persons or legal entities subject to investigation or legal proceedings related to money laundering, predicate offenses, and/or terrorist financing. Furthermore, a direct report of the institution's highest authority is considered a PEP.</li> </ul>	<p>The following measures must be applied:</p> <ul style="list-style-type: none"> <li>• In the case of PEPs, the names of their relatives up to the second degree of consanguinity and second degree of affinity, as well as their spouse or cohabiting partner, must be requested, along with a list of natural persons or legal arrangements in which they are the beneficial owner, in accordance with Article 4 of Legislative Decree No. 1372 and its amendments.</li> <li>• Verification of the customer's purchase transaction volume and assessment of whether it is consistent with their income or presents any red flags.</li> </ul> <p>Likewise, the Company, through the Compliance Officer, will conduct the appropriate inquiries and apply additional identification and verification measures, such as:</p> <ul style="list-style-type: none"> <li>• Collecting information from publicly available sources.</li> <li>• Verifying through credit bureaus the positive or negative payment history of the Customer, whether an natural person and/or a legal entity, in relation to obligations incurred in the financial, commercial, and service sectors.</li> <li>• If necessary, additional customer information will be requested through a specific report provided by the external firm engaged to provide support services.</li> </ul>

## 12. DUE DILIGENCE PROCEDURE FOR EMPLOYEES AND DIRECTORS

### 12.1. DUE DILIGENCE PROCEDURE FOR EMPLOYEES

Employees are all natural persons who have an employment relationship with the Company and are involved in lime commercialization; this includes senior management, consisting of the General Manager, managers or administrators holding similar positions, and the Compliance Officer.

The Human Resources Department is responsible for requesting the Sworn Statement from employees; furthermore, at the time of hiring, the Company verifies the watchlists indicated in Annex No. 05 to determine whether employees are included on them. After employment begins, at least once a year, the Company verifies again whether they appear on these lists.

In the event of a match, a Suspicious Transaction Report (STR) is filed and the General Manager is notified so that the SPLAFT Code of Conduct and the Internal Work Regulations may be applied. If the Company decides to hire the employee, it must retain the applicant's file in physical or electronic form, as well as the Compliance Officer's opinion, if one was requested.

It should be noted that under no circumstances will the Company engage the services of the following individuals:

- a. Natural persons known to be under investigation by the competent authorities for money laundering, predicate offenses, and/or terrorist financing, and/or who are linked to activities related to the proliferation financing of weapons of mass destruction.
- b. Natural persons linked to natural persons or legal entities subject to investigation or legal proceedings related to money laundering, predicate offenses, terrorist financing, and/or proliferation financing of weapons of mass destruction.

#### **Documents to be requested after employee selection:**

- i. i. Employees are required to report any changes to the information provided to the Company within a period not exceeding fifteen (15) business days from the date the change occurs.
- ii. Notwithstanding the foregoing, the Company shall verify, at least once a year, that the information provided by its employees is updated as appropriate. To achieve this objective, it may use online update campaigns.
- iii. If the information provided by employees is unclear or insufficient, the Company may request additional information within a period not exceeding 7 business days.
- iv. After obtaining complete information from its employees, the Company must file these documents in each employee's personnel file.

#### **12.2. DUE DILIGENCE PROCEDURE FOR DIRECTORS**

The Legal Affairs Department will be responsible for collecting and safeguarding the directors' sworn statements, which will be made available upon request by the UIF-Peru.

In addition, at the time of selecting a Director, the Company must verify the watchlists indicated in Annex No. 05 to determine whether they are included on them. After the appointment, at least once a year, the Company will verify again whether the Directors are on those lists.

If any aspect of the information provided by the director candidate remains unclear, the Company may request additional information within a period not exceeding 7 business days.

After reviewing the information provided by the candidate and finding no adverse records, the Company may proceed with the appointment of the director. If this is not the case, the Company, through the Compliance Officer, must report to the General Shareholders' Meeting regarding the candidate's status so that the Meeting may issue a determination on the appropriateness of the appointment.

#### **Documents to be submitted after the director's appointment:**

- I. Directors are required to report any changes to the information provided to the Company within fifteen (15) business days of the change occurring.
- II. Notwithstanding the foregoing, the Company must verify, at least once a year, that the information provided by its directors is updated when necessary. To achieve this objective, the Company may use online update campaigns.
- III. If the information provided by the directors is unclear or insufficient, the Company may request additional information within a period not exceeding 7 business days.
- IV. After obtaining the complete information from its directors, the Company must file these documents in each director's file.

### 13. DUE DILIGENCE PROCEDURE FOR SUPPLIERS

The Supply Chain Management Department is responsible for collecting and evaluating supplier information, considering as suppliers those natural persons or legal entities contracted to provide goods or services directly related to the conduct of activities subject to supervision by the UIF-Peru. To this end, during the selection process, the Company must request and verify the following minimum information:

- Full name or corporate name, in the case of a legal entity.
- Tax ID certificate.
- Address of the main office or premises.
- Years of experience in the market.
- Business sectors in which the supplier provides its products or services.
- Identification of the beneficial owner, in accordance with Article 4 of Legislative Decree No. 1372 and its amendments.
- First and last names of the legal representative, including the information required for individuals.
- Sworn Statement stating that the supplier is a natural person with no criminal record. In the case of a supplier that is a legal entity, a sworn statement signed by the legal representative stating that no penalty has been imposed pursuant to Article 105 of the Penal Code, Law No. 30424, or the applicable special criminal law.

The Corporate Procurement and Transportation departments are responsible for verifying the supplier to be contracted against the watchlists indicated in Annex No. 05, in order to determine whether or not the supplier is included on them. This search will be updated at least once a year. If any matches are found, the Compliance Officer must be notified via email at [Oficialdecumplimiento@acerosarequipa.com](mailto:Oficialdecumplimiento@acerosarequipa.com) so that the information can be submitted as a Suspicious Transaction Report (STR).

## 14. RED FLAGS FOR THE DETECTION OF UNUSUAL OR SUSPICIOUS TRANSACTIONS

Red flags are control mechanisms that enable the identification of behavioral patterns—such as specific customer behaviors or procedures, and atypical situations—used by individuals or companies to conceal Money Laundering, Terrorist Financing, or Proliferation Financing of Weapons of Mass Destruction. They serve as a tool for the Company, through the Compliance Officer, to identify unusual or suspicious transactions.

All Company employees are responsible for being alert to red flags from customers, directors, employees, or suppliers that could indicate ML/TF and PF.

### 14.1. RED FLAGS APPLICABLE TO THE COMPANY'S ACTIVITIES TO DETERMINE UNUSUAL CUSTOMER BEHAVIOR.

- a. Sudden appearance of companies or natural persons with no history in the market whose source of capital cannot be verified.
- b. The customer refuses to provide the requested information or submits information that is inconsistent, unusual, or of dubious origin, making verification by the Company difficult.
- c. It comes to light through public media, such as print or digital newspapers, social media, or internet search engines, that a customer is being investigated or prosecuted for the crime of Money Laundering, predicate offenses, the crime of terrorist financing and related offenses, or that they are involved in situations related to establishments, agents, or acts of illegal or informal trade.
- d. The customer displays an unusual lack of concern regarding the risks they are assuming and/or the fees and costs associated with the transaction.
- e. The customer makes payment, either as a down payment or for the total sale amount, using installment payments (smurfing), with the number of transactions exceeding four (04).
- f. The customer conducts complex or unusual transactions, such as involving third parties with no apparent connection to the purchase transaction.
- g. The customer uses cash deposits as the sole means of payment for the purchase of the product.

- h. The customer insists on meeting with Company personnel at a location other than the office or premises to conduct a commercial or financial activity.
- i. The customer provides the same address and/or phone number as other individuals with whom they have no apparent relationship.
- j. The customer pays for part or all of the product with a transfer from abroad, without being able to reliably prove the origin of the funds.
- k. The customer makes cash deposits into the Company's account and subsequently requests a refund of their money for no apparent reason.
- l. The customer makes payments or prepayments of sums of money that are not consistent with the occupation they claim to have.
- m. Transactions in which the customer does not disclose having the financial means to carry out the transaction, raising the possibility that they are not acting on their own behalf but as an agent for a third party, and refusing to provide information regarding said person or entity.
- n. Disproportionate growth in the customer's business transactions.
- o. Sale of the product to legal entities established less than one year ago (shell companies).

#### **14.2. RED FLAGS TO IDENTIFY UNUSUAL EMPLOYEE BEHAVIOR**

- a. The employee's lifestyle does not correspond to their income, or there is a notable and unexpected change in their financial situation.
- b. The employee consistently avoids or refuses to take vacation time.
- c. The employee has frequent and unexcused absences.
- d. The employee frequently stays in the office outside of working hours without a valid reason.
- e. The employee uses their own home to receive customer documents.
- f. The employee holds or insists on holding meetings with customers at a location other than the Company's offices or outside of working hours, without any justification, to conduct a commercial or financial transaction.
- g. The employee is involved in nonprofit organizations, such as foundations, associations, committees, NGOs, among others, that are linked to the ideology, claims, or demands of a domestic and/or foreign terrorist organization; provided that this is duly demonstrated.
- h. There is an unusual or sudden increase in the number of transactions handled

by the employee.

- i. It is verified that the employee has failed to report or has concealed from the Compliance Officer information regarding a change in the behavior of a customer or supplier.
- j. The employee is involved in businesses in the same business sector or that compete with the Company's activities.

### 14.3. RED FLAGS TO IDENTIFY UNUSUAL SUPPLIER BEHAVIOR

- a. Suppliers with an inactive Tax ID No. (RUC), or one that does not exist or cannot be found.
- b. Suppliers or contractors who offer to pay significant commissions without legal or logical justification.
- c. Suppliers with no experience in the business sector.
- d. Suppliers classified as prohibited from contracting with the government.
- e. Suppliers offering bids with prices below market value.
- f. Front companies.
- g. Companies whose shareholders, legal representatives, or authorized agents are under investigation for ML/TF and PF or predicate or related offenses.
- h. Companies whose shareholders, legal representatives, or authorized agents are Politically Exposed Persons (PEPs).
- i. Companies incorporated in tax havens.
- j. Offshore companies.
- k. The supplier refuses to provide the information requested by the Company (valid Power of Attorney documentation, National ID Card of the representative)
- l. The shareholders, legal representatives, and/or the company are listed on watchlists or lists of interest.

If any of the scenarios described above occur, the Compliance Officer must be notified immediately via email at [Oficialdecumplimiento@acerosarequipa.com](mailto:Oficialdecumplimiento@acerosarequipa.com), including the following information: Description of the identified red flags, and relevant information and/or documentation that allows for the identification of the customer, supplier, or employee.

#### 14.4. PERIODIC REVIEW AND UPDATE OF RED FLAGS

##### Considerations:

1. The Compliance Officer is responsible for periodically reviewing whether or not the red flags implemented by the Company need to be updated.
2. If an update is necessary, the new red flag will be brought to the attention of the ML/TF and PF Risk Committee.
3. Each time a red flag is updated, it will be approved at a board meeting and disseminated to all personnel through physical or virtual means, as determined.
4. Whenever a red flag is updated, this change will be incorporated into the Compliance Officer's training program for employees and/or directors.

#### 15. PROCEDIMIENTO DE OPERACIONES INUSUALES Y REPORTE DE OPERACIONES SOSPECHOSAS

##### Considerations:

1. In the context of customer relations, it must be verified whether any of the scenarios described in the previous section (RED FLAGS) have been triggered.
2. The Compliance Officer is responsible for assessing whether or not the transaction should be considered an unusual transaction. To do so, the Compliance Officer will have a maximum of 30 days for evaluation and classification, starting from the receipt or identification of the red flag.
3. If a transaction is deemed unusual, the Compliance Officer will evaluate it to determine whether the unusual transaction should be classified as a suspicious transaction and reported to the Peruvian Financial Intelligence Unit (UIF-Peru) via a Suspicious Transaction Report (STR). If, after analysis, the transaction is not deemed a suspicious transaction, it must be properly documented and stored and will remain classified as an unusual transaction.

##### The following procedure must be followed for the analysis of an unusual transaction:

- The Compliance Officer will request the customer's file to verify whether the identified red flags warrant classification as an unusual transaction.
- If necessary, a due diligence report is requested from the external provider

- contracted for these cases.
- If, after verifying the unusual transaction, it is found to be justified, it will be filed. Conversely, if the unusual transaction is NOT justified, the Company's Compliance Officer will assess the need to file a Suspicious Transaction Report (STR) to the UIF-Peru.
- If the transaction is classified as suspicious, it must be reported immediately to the UIF-Peru, within a period not exceeding 24 hours. The STR is confidential and restricted in nature, regardless of the amount involved in the transaction. Only the Compliance Officer may be aware of the submission of the STR.

### **15.1. FILING AND RETENTION OF DOCUMENTATION SUPPORTING THE ANALYSIS OF UNUSUAL AND SUSPICIOUS TRANSACTIONS**

The Compliance Officer is responsible for backing up and retaining the documentation supporting the proper analysis of unusual and suspicious transactions. This may be stored in a physical file or digitally. The Compliance Officer must retain the information for a minimum period of ten (10) years.

The minimum information contained in the file for an unusual and suspicious transaction is as follows:

- i. Identification details of the unusual transaction:
  - Date the transaction was conducted;
  - Type of transaction;
  - Amount of the transaction;
  - Currency in which the transaction was conducted;
  - Payment method used for the transaction;
  - Method of payment;
  - Source of the funds, goods, or other assets;
  - Payment receipt number, if applicable;
  - Description of the transaction, indicating the reasons that led to its classification as unusual;
  - If the transaction was classified as suspicious, specify the STR number used to report it to the UIF-Peru.

- If the unusual transaction was not classified as suspicious, the analysis and evaluation of the transaction and the reasons for that determination must be provided.
- ii. Identification details of the persons involved in the transaction, whether natural persons or legal entities, domestic or foreign, and acting on their own behalf, for their own benefit, or through a representative or agent (originator/owner, beneficiary/purchaser, executor); including at least the following:

In the case of a natural person:

- Full name;
- Type and number of the identity document;
- Nationality, in the case of a foreign national;
- Address;
- Marital status, including the first and last names of the spouse or cohabiting partner, if applicable;
- Role in the transaction, regardless of title: buyer, guarantor, surety, representative, or agent (specify on whose behalf they are acting), principal (specify on whose behalf they are acting);

In the case of a legal entity:

- Corporate name;
- Unique Taxpayer Identification Number (RUC) or equivalent registry for non-residents, if applicable;
- Address;
- First and last names of the legal representative, including the information required for an individual;
- Identification of the beneficial owner, in accordance with Article 4 of Legislative Decree 1372 and its amendments;
- Identified red flags;
- Description of the red flag;
- Source of the red flag.

In addition, the following documents must be retained:

1. Copy of the sworn statement of due diligence on customer and beneficial owner for natural persons and legal entities.
2. Copy of identification document (National ID Card, Foreigner's ID Card, Passport) for natural persons.
3. Copy of the Tax ID certificate for legal entities.
4. Copy of the legal representative's identification document.
5. Copy of the spouse's identification document, if applicable.
6. Due diligence report, if applicable.
7. Copy of the invoices or receipts involved in the commercial transaction. Copy of the payment methods used, such as deposit slips, bank transfer receipts, credit approval letters, among others.
8. Report on the assessment to determine whether the transaction is unusual and/or suspicious.

## 16. REVIEW OF WATCHLISTS AND PROCEDURE FOR THE ADMINISTRATIVE FREEZING OF FUNDS OR ASSETS

In addition to ML/TF risks, the proliferation financing risk of weapons of mass destruction, in accordance with FATF Recommendation 1, includes potential non-compliance, failure to implement, or circumvention of obligations related to targeted financial sanctions as referred to in FATF Recommendation 7.

In this regard, the Company, in its capacity as a Reporting Entity, is responsible for continuously monitoring the publication of relevant international lists via the UNSC or SBS website and cross-referencing them with its transaction records and databases of customers, directors, employees, and suppliers, in order to identify any funds or other assets, or any transaction involving persons or entities designated by the United Nations Security Council, in which case the Company must report such findings without delay to the UIF-Peru through the established channels.

**The procedure to follow is as follows:**

1. At the start of the contract or relationship (Customer, Supplier, Director, or Employee), the watchlist published by the SBS must be reviewed.
2. **During the term of the relationship (Customer, Supplier, Director, or Employee),** the international watchlists published by the SBS on its website **must also be reviewed** at and cross-referencing them with the company's transaction records and database of customers, suppliers, directors, and employees; if any matches are found, they must be reported immediately to the Compliance Officer.
3. **If it is detected that a customer, supplier, director, or employee is included on any of the watchlists, the following steps must be taken:**
  - 3.1. The information obtained shall be documented by the reporting entity, detailing the following:
    - Date of verification .
    - Names of the individuals verified .
    - Lists consulted .
    - Result found .
    - Signature of the Compliance Officer .
  - 3.2. If a customer is identified as being on the watchlists, the Compliance Officer must be notified immediately.
  - 3.3. The Compliance Officer will report the case to the UIF-Peru and, if applicable, will submit the report within a maximum of twenty-four (24) hours of detection.
  - 3.4. Upon receiving the report from the Compliance Officer, the UIF-Peru, if applicable, will order the administrative freezing of the funds or other assets detected belonging to the persons or entities designated on international watchlists; and will communicate the decision via official letter, ordering that the freezing be carried out, without prejudice to the initiation of the corresponding financial analysis and investigation. Said official letter shall be sent to the email address of the Compliance Officer registered with the UIF-Peru and by physical mail.
  - 3.5 The Compliance Officer, with the support of the legal department, must immediately proceed to administratively freeze the funds or other assets upon receipt of the official notice from the UIF-Peru; and, likewise, must notify the UIF-Peru of the execution of the ordered freeze via email and by

physical mail. This measure remains in effect until it is validated or revoked by a judicial authority. To implement the freeze, the Compliance Officer must coordinate with the Treasury Department, which will be responsible for blocking payments to the identified person or entity.

3.6. Only the UIF-Peru, through an official letter or other means as provided, shall inform the Company of the termination of the administrative freeze on funds or other assets.

3.7. The Compliance Officer shall coordinate with the Treasury Department to lift the freeze, when applicable.

3.8. Supporting documentation shall be archived for a minimum period of ten (10) years, either in physical or digital form.

## 17. PROCEDURE FOR RECORDING, FILING, RETENTION, AND COMMUNICATION OF RECORDS, REPORTS, AND OTHER INFORMATION OR DOCUMENTATION OF THE SPLAFT

- 1. Recording and Filing:** Transactions entered into the RO, transactions classified as unusual, suspicious transactions, semi-annual reports, ML/TF and FP risk management, relationships and transactions involving customers and suppliers, analyses, and other documents are backed up in folders created for the Legal Department in the cloud (SharePoint). This information backup is online and restricted in access.
- 2. Retention:** The information comprising the ML/TF Prevention System will be retained for a minimum of 10 years. For this purpose, computer systems or similar means will be used to allow for easy retrieval of the information for consultation and internal or external reporting to the competent authorities in accordance with the law.
- 3. Communication:** All communication regarding the ML/TF Prevention System shall be via email addressed to the Compliance Officer.

## 18. SEMIANNUAL REPORT OF THE COMPLIANCE OFFICER

The Compliance Officer must submit a report every six months on compliance with the policies and procedures comprising the SPLAFT implemented by the Company each semester, known as the Compliance Officer's Semiannual Report (ISOC). The Board of Directors shall approve this report within thirty (30) days following the end of the respective annual period.

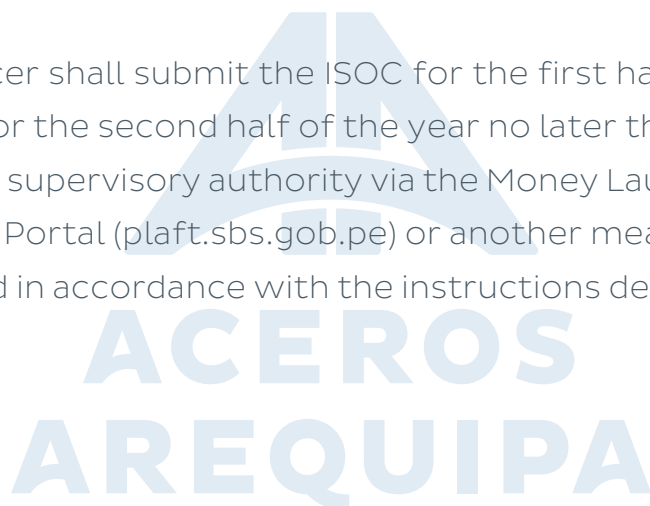
### 1. The report must contain at least the following information:

- The Compliance Officer's address, phone number, and email address.
- An indication of whether the Compliance Officer acts in a corporate capacity or not.
- The names of the partners, shareholders, or associates and their percentage of ownership, if applicable.
- The names of the managers or other employees responsible for managing the business, if applicable.
- Annual statistics from the RO, indicating the number of transactions recorded and the amounts involved, with the information broken down by month.
- Annual statistics on detected unusual transactions, indicating the number of transactions detected, the amounts involved, or other aspects considered significant, with the information broken down by month.
- Annual statistics on suspicious transactions reported to the UIF-Peru, indicating the number of reported transactions, the amounts involved, or other aspects considered significant, with the information broken down by month.
- Description of new red flags of unusual transactions established and typologies of suspicious transactions that have been detected and reported, if any.
- Procedures for identifying and assessing ML/TF and PF risks; due diligence procedures for customers, directors, employees, and, where applicable, suppliers and counterparties; procedures for identifying unusual and/or suspicious transactions
- Number of employees, number of training sessions on topics related to ML/TF Prevention, the number of people who have been trained; number of

- people who were trained more than once a year, as well as details of the training topics according to the recipient's profile and role, and the ML/TF and PF risks they face.
- Date of the last update to the SPLAFT Manual and Code of Conduct, as well as the level of compliance with these by directors and employees, noting any instances of non-compliance, the sanctions imposed, and the corrective measures adopted.
- Corrective actions taken in response to observations and/or recommendations made by the supervisory authority and internal or external auditors, as applicable.
- Geographic location of offices, branches, and agencies.
- Other information as determined by the SBS.

## **2. Deadline for submission to the UIF-PERU:**

The Compliance Officer shall submit the ISOC for the first half of the year no later than August 15, and for the second half of the year no later than February 15 of the following year, to the supervisory authority via the Money Laundering and Terrorist Financing Prevention Portal ([plaft.sbs.gob.pe](http://plaft.sbs.gob.pe)) or another means established by the SBS, in the format and in accordance with the instructions determined through the same means.



## 19. COMPLIANCE OFFICER'S ROLE IN IDENTIFYING AND ASSESSING ML/TF AND PF RISKS

- **Launch of new products and/or services:**

The Compliance Officer shall issue a report containing an assessment of the level of ML/TF and PF risk exposure to which the new products offered by the Company would be subject.

- **New technologies:**

The Compliance Officer shall issue a report containing an assessment of the level of exposure to ML/TF and PF risks to which the Company would be exposed if it incorporates new technologies into its processes.

- **Expansion into new geographic areas:**

The Compliance Officer shall issue a report containing an assessment of the level of exposure to ML/TF and PF risks to which the Company would face if it were to expand into new geographic areas. This assessment shall take into account the evaluation of the “geographic area” risk factor.

## 20. USE OF THIRD PARTIES OR INTERMEDIARIES

The Company, if it deems it necessary, may use third parties or intermediaries to perform services related to the identification and/or verification of information regarding customers, directors, employees, and suppliers, as applicable.

Should the Company engage a third party or intermediary, it shall collect their identification data and supporting documentation, as well as a sworn statement in which the third party or intermediary affirms that they have taken the necessary measures to comply with the due diligence provisions regarding the identification of customers, directors, employees, and suppliers, as applicable, as set forth in this Manual.

## 21. DUTY OF CONFIDENTIALITY

The Suspicious Transaction Report (STR), the Transaction Register (RO), the information and documentation contained therein, and all communications regarding this matter sent by the Company to the UIF-Peru are confidential by law; therefore, under their own responsibility, the Company—including its shareholders, directors, CEO, managers, employees, personnel, or third parties with a professional relationship—and in particular the Compliance Officer, are prohibited from disclosing to any person, except a court of law or other competent authority in accordance with applicable legal provisions, that such information has been requested and/or provided to the UIF-Peru.

## 22. APPROVAL OF THIS MANUAL

This Manual has been approved by the Company's Board of Directors. The Board of Directors entrusts General Management with its dissemination, implementation, and periodic updating. The last update was made on January 27, 2026. Updates will be available on the Company's social media and will be disseminated to all directors and employees.


ACEROS  
AREQUIPA

## 23. ANNEXES


No.	Document Name	Type	Code
1	Sworn Statement of Due Diligence on Directors and Employees	Annex	01
2	Sworn Statement of Receipt, Acknowledgment, and Commitment to Comply with the SPLAFT Manual and Code of Conduct	Annex	02
3	Sworn Statement of Due Diligence on Customers (Natural Person)	Annex	03
4	Sworn Statement of Due Diligence on Customers (Legal Entity and Legal Arrangements)	Annex	04
5	International Watchlists Contributing to the ML/TF and PF Prevention	Annex	05




## ANNEX No. 01: Sworn Statement of Due Diligence on Director and Employee

		SWORN STATEMENT OF DUE DILIGENCE ON DIRECTORS AND EMPLOYEES				Macroprocess Legal Management	
		GL-E001				Version: 01	
<b>I. GENERAL IDENTIFICATION INFORMATION</b>							
First and Last Names:							
Type of ID:	National ID Card ( )	Passport ( )	Foreigner's ID Card ( )	Document No.:	Nationally:		
Place of Birth:	Other (Specify):			Phone Number(s):	Email:		
Home Address:	Street - Avenue - Road - Alley / Block - Lot				No.	Apartment / Interior	
	Neighborhood / Complex / Area / Sector			District	Province	Department	
						Country	
Marital Status:	Single ( )	Divorced ( )	Married ( )	Cohabiting ( )	First and last names of spouse or cohabiting partner:	Occupation / Profession:	Current position and name of the company or institution:
<b>II. EDUCATION AND TRAINING</b>							
	Level of education	Educational Institution / Institute / University	If you have completed a specialization, please indicate it:	City / Country	Start Date	End Date	
a)	Primary Education						
b)	Secondary Education						
c)	Technical Studies						
d)	Bachelor's Degree / Degree						
e)	Professional Degree / Degree Certificate						
f)	Master's Degree						
g)	Doctorate						
h)	Training / Course						
i)	Certificate Program						
<b>III. EMPLOYMENT HISTORY (WORK EXPERIENCE DURING THE LAST TWO YEARS)</b>							
	Name of Company or Institution:	Position Held	Place of Employment	Start Date	End Date		
a)							
b)							
<b>IV. FINANCIAL HISTORY</b>							
1. Monthly income received in addition to that from Corporación Aceros Arequipa S.A.							
	Type	Source (origin of the income)	Amount	Method of Payment			
a)							
b)							
2. Real estate (houses, apartments, land, etc.) in Peru or abroad							
	Country	Address / Location	Ownership Regime	Value			
a)							
b)							
3. Personal property (cars, motorcycles, etc.) in Peru or abroad							
	Vehicle Type	Model - Brand - Year	License Plate No.	Value			
a)							
b)							
4. Accounts in the Banking and/or Financial System							
	Bank / Financial Institution	Account Type	Opening Date	Value			
a)							
b)							
5. Debts							
	Details of the debt	Specify whether the debt was incurred with (Financial Institution, Individual, or Other):		Debt Status	Amount		
a)							
b)							
<b>V. IDENTIFICATION OF POLITICALLY EXPOSED PERSONS (PEP)</b>							
Are you a Politically Exposed Person (PEP), a relative up to the second degree of consanguinity or second degree of affinity of a Politically Exposed Person (PEP), or have you been a direct employee of a PEP?				Yes, I have been a PEP ( ) I am currently a PEP ( ) I am a relative of a PEP ( ) Yes, I have been a direct employee of a PEP ( ) I am not and have never been any of the above ( )			
Note: PEPs are natural persons, whether nationals or foreigners, who currently hold or have held, within the last two (2) years, prominent public office or prominent positions in an international organization, whether within the national territory or abroad, and whose financial circumstances may be of public interest. Likewise, a direct associate of the institution's highest authority is considered a PEP. Scope of PEP family relationship: This may include parents, children, siblings, grandparents, grandchildren, spouse, cohabiting partner, parents-in-law, siblings-in-law, children of the spouse, and grandparents of the spouse. (*) See PEP positions on the back of the page.							
If you checked "Yes, I have been a PEP" or "I am currently a PEP," please complete the following:							
A)	Position held or previously held:	Entity or institution:	Start date:	End date:			
If you checked "I am a relative of a PEP," please complete the following:							
A)	Relationship to the PEP:	First and last names of the PEP relative:	Position held or previously held by the PEP relative:	Start date:	End date:		
If you checked "Yes, I have been a direct employee of a PEP," please complete the following:							
A)	First and last names of the PEP:	Entity or institution:	Position currently held or previously held by the PEP:	Start date:	End date:		
<b>VI. BACKGROUND CHECK</b>							
Have you been or are you currently under investigation by police, prosecutors, or the courts, or have you been convicted of crimes such as money laundering, terrorist financing, illegal mining, drug trafficking, terrorism, crimes against the public administration, kidnapping, procuring, human trafficking, illicit arms or migrant trafficking, tax crimes, extortion, fraud, corruption, customs fraud, or other crimes generating illicit profits?			Yes, I have been investigated/prosecuted ( ) I am currently under investigation/prosecution ( ) Yes, I have been sanctioned/convicted ( ) No, I have not been and am not currently under investigation/prosecution ( )				
If you answered "Yes, I have been investigated/prosecuted," please complete the following section:							
A)	Crime(s) for which you were investigated/prosecuted:	Reason for the investigation/prosecution:	Prosecutor's Case No. / Court Case No.:	Prosecutorial Authority / Judicial Authority:			
If you answered "I am currently under investigation/prosecution," please complete the following section:							
A)	Crime(s) for which you are being investigated / prosecuted:	Reason for being investigated / prosecuted:	Prosecutor's Case No. / Court Case No.:	Prosecutorial Authority / Judicial Authority:			
If you answered "Yes, I have been sanctioned/convicted," please fill out the following section:							
A)	Crime(s) for which you were sanctioned/convicted:	Date of the sanction / conviction:	Sanction / penalties imposed:	Court Case No.:	Judicial Authority:		
<b>VII. IDENTIFICATION OF CONFLICTS OF INTEREST</b>							
Do you have any family relationship (up to the second degree of consanguinity and the second degree of affinity) or personal relationship (friendship) with any member of Corporación Aceros Arequipa S.A. that represent a potential conflict of interest?			Yes ( ) No ( )				
If you answered "Yes," please complete the following section:							
A)	Degree of family or personal relationship with the CAASA employee:	Position held by the CAASA employee:	First and last names of the CAASA employee:				
Have you been a General Manager, Director, Line Manager, employee, and/or shareholder of any supplier or client of Corporación Aceros Arequipa S.A.?							
			Yes ( ) No ( )				
If you answered "Yes," please complete the following section:							
A)	Type of company:	Supplier company ( ) Customer company ( )	Company name:	Position held at the CAASA supplier or client company:			
<b>DECLARATION OF TRUTHFULNESS OF THE INFORMATION</b>							
I hereby declare under oath that the information contained in this document is true, complete, and accurate. Accordingly, I release Corporación Aceros Arequipa S.A. (CAASA) from any and all legal liability—whether administrative, civil, and/or criminal—that may arise from any falsehood, omission, inaccuracy, or error in the information provided herein. Furthermore, I agree to notify my employer of any changes to the information provided within a maximum of fifteen (15) calendar days from the date such change occurs.							
Signed in:		City / Country	Date (mm/dd/yyyy)				
		Signature of the declarant (Sign as on National ID Card):					
		Name: National ID Card No.:					


## ANNEX No. 02: Sworn Statement of Receipt, Acknowledgment, and Commitment to Comply with the SPLAFT Manual and Code of Conduct

	<b>SWORN STATEMENT OF RECEIPT, ACKNOWLEDGMENT, AND COMMITMENT TO COMPLY WITH THE SPLAFT MANUAL AND CODE OF CONDUCT</b>	Macroprocess Legal Management
	GL-E002	Version: 01
By means of this document, I hereby declare under oath the following:		
That my current personal information is as follows:		
1	<b>Identified with:</b> National ID Card <input type="checkbox"/> Passport <input type="checkbox"/> Foreigner's ID Card <input type="checkbox"/> Other: <input type="checkbox"/>	<b>Last Name:</b> _____ <b>Document No.:</b> _____
	<b>First Name:</b> _____	<b>City of origin:</b> _____
	<b>Nationality:</b> _____	<b>Company (Employer):</b> CORPORACIÓN ACEROS AREQUIPA
	<b>Department and Position:</b> _____	
That, upon signing this document, I <b>DECLARE</b> that I have received a copy of the following documents:		
2	1. Manual for the Prevention and Management of ML/TF and PF Risks 2. Code of Conduct for the ML/TF and PF Prevention System.	
3	That, I have become <b>aware of</b> and <b>understood</b> the contents of the Manual for the Prevention and Management of ML/TF and PF Risks, as well as the Code of Conduct of the ML/TF and PF Prevention System; both of which are mandatory.	
4	That, I am aware that if I violate the provisions of the Manual for the Prevention and Management of ML/TF and PF Risks or the Code of Conduct of the ML/TF and PF Prevention System, I am subject to disciplinary action as appropriate by my employer.	
5	That, I will immediately report to the Compliance Officer or my direct supervisor any incident that, in good faith, leads me to suspect a violation of the Code of Conduct, the Manual, or any other internal policy and/or procedure associated with the SPLAFT of Corporación Aceros Arequipa S.A.	
6	By signing this document and in accordance with the provisions of the applicable legal regulations, I <b>HEREBY COMMIT</b> to faithfully complying with the provisions of the documents described above and all other applicable legal provisions on the matter in the performance of my duties within Corporación Aceros Arequipa S.A.	
I affirm and ratify all statements made in this sworn statement, in witness whereof I sign it at the place and date indicated below:		
DATE	SIGNATURE	
<b>SPLAFT:</b> Money Laundering, Terrorist Financing, and Proliferation Financing Prevention System. <b>ML/TF and PF:</b> Money Laundering, Terrorist Financing, and Proliferation Financing		

# ANNEX No. 03: Sworn Statement of Due Diligence on Customers (Natural Person)

		SWORN STATEMENT OF DUE DILIGENCE ON CUSTOMERS - NATURAL PERSON				Macroprocess Legal Management	
		GL-E003				Version: 01	
<b>I. GENERAL IDENTIFICATION INFORMATION (CUSTOMER)</b>							
First and Last Names:							
Type of ID:	National ID Card ( )    Passport ( )    Foreigner's ID Card ( )			Document No.:		Nationality:	
Place of Birth:	Other (Specify):			Phone number(s):		Email:	
Home Address:		Street - Avenue - Road - Alley / Block - Lot				No.	Apartment / Interior
		Housing Development / Complex / Area / Sector		District	State	Department	Country
Marital Status:	Single ( )    Divorced ( ) Married ( )    Cohabiting ( )	First and last names of spouse or cohabiting partner:		Occupation / Profession:	Purpose of the relationship with Corporación Aceros Arequipa S.A.:		
<b>II. IDENTIFICATION OF POLITICALLY EXPOSED PERSONS (PEP)</b>							
Are you a Politically Exposed Person (PEP), a relative up to the second degree of consanguinity or second degree of affinity of a Politically Exposed Person (PEP), or have you been a direct employee of a PEP?						Yes, I have been a PEP ( )    I am currently a PEP ( ) I am a relative of a PEP ( )    Yes, I have been a direct employee of a PEP ( ) I am not and have never been any of the above ( )	
Note: PEPs are individuals, whether nationals or foreigners, who currently hold or have held, within the last two (2) years, high-level public office or prominent positions in an international organization, whether within the country or abroad, and whose financial circumstances may be of public interest. Additionally, a direct report of the institution's highest authority is considered a PEP. Scope of PEP family relationship: This may include parents, children, siblings, grandparents, grandchildren, spouse, cohabiting partner, parents-in-law, siblings-in-law, children of the spouse, and grandparents of the spouse. (*) See PEP positions on the back of the page.							
If you checked "Yes, I have been a PEP" or "I am currently a PEP," please complete the following:							
A)	Position held or previously held: Start date:			Entity or Institution: End date:			
If you checked "I am a relative of the PEP," please complete the following:							
A)	Relationship to the PEP: Entity or institution where the PEP relative works or worked:			First and last names of the PEP relative: Start date:		Position held or previously held by the PEP relative: End date:	
If you checked "Yes, I have been a direct employee of the PEP," please complete the following:							
A)	First and last names of the PEP: Position held as a direct employee of the PEP:			Entity or Institution: Start date:		Position currently held or previously held by the PEP: End date:	
<b>IV. BENEFICIARY OF THE TRANSACTION (BENEFICIARY)</b>							
The transaction has been or will be carried out on behalf of:							
1. Myself ( )    2. A third-party natural person ( )    3. A third-party legal entity ( )    4. A third-party legal arrangement ( )							
1. If you answered "Myself," please complete the following box, if applicable:							
A)	Source of the funds or assets involved in the transaction when it is conducted in cash and equals or exceeds the threshold for purposes of the RO:						
2. If you answered "A third-party natural person," please complete the following section, if applicable:							
A)	First and last names:		Identification document: Document No.:		National ID Card ( )    Passport ( )    Foreigner's ID Card ( )    Other (Specify):		
Representation details:							
1) Power of Attorney by Public Deed ( )    2) Power of Attorney ( )    3) Other (specify):							
B)	Information regarding the representation document:			Notary's first and last names:			
Date of the deed:			Date of the certified copy:		Date of the Deed:		
Other (specify):			Date of the document:				
Indicate whether the third-party natural person is or has been, within the last two (2) years, a Politically Exposed Person (PEP):							
						Yes ( )    No ( )	
Indicate whether the third-party natural person has a spouse, cohabiting partner, or relative up to the second degree of consanguinity or second degree of affinity to a Politically Exposed Person (PEP):							
						Yes ( )    No ( )	
If you answered "Yes" to any of the questions, please provide the following information:							
C)	First and last names of the PEP (if the third-party natural person is related to the PEP):			Entity or institution where they worked:		Position or title held:	
Identification document:			National ID Card ( )    Passport ( )    Foreigner's ID Card ( )    Other (Specify):		Document No.:		Period during which they held that position or role:
First and last names of the PEP (if the third-party natural person is related to the PEP):			Entity or institution where they worked:		Position or title held:		
Identification document:			National ID Card ( )    Passport ( )    Foreigner's ID Card ( )    Other (Specify):		Document No.:		Period during which they held that position or role:
D)	Source of the funds or assets involved in the transaction when it is conducted in cash and equals or exceeds the threshold for purposes of the RO:						
3. If you answered "A third-party legal entity" or "A third-party legal arrangement," please complete the following section:							
A)	Name / Corporate Name		Tax ID No. or Equivalent Registration				
Representation details:							
1) Power of Attorney by Notarial Deed ( )    2) Power of Attorney ( )    3) Other (specify):							
B)	Information regarding the representation document:			Notary's first and last names:			
Date of the deed:			Date of the certified copy:		Date of the Deed:		
Other (specify):			Date of the document:				
C)	Source of the funds or assets involved in the transaction when it is conducted in cash and equals or exceeds the threshold for purposes of the RO:						
D)	Identification of the beneficial owner of the transaction (first and last names)						
<b>DECLARATION OF TRUTHFULNESS OF THE INFORMATION</b>							
I hereby declare under oath that the information provided in this document is accurate and true, and I therefore release Corporación Aceros Arequipa S.A. (hereinafter, CAASA) from any legal liability (administrative, civil, and/or criminal) that may arise from any falsehood, omission, inaccuracy, or error contained herein or that may arise if the illicits origin or destination of my funds is proven. Likewise, should CAASA be involved in an investigation or legal proceeding for the crimes mentioned in this sworn statement, due to causes attributable to me, and should the financial penalties and fines provided for in applicable laws be imposed, I shall reimburse CAASA for all expenses incurred and compensate it for any damages caused.							
Signed in:		City / Country		Date (mm/dd/yyyy)			
				Signature of the declarant (Sign as on National ID Card)			
				Name:			
				National ID Card:			

# ANNEX No. 04: Sworn Statement of Due Diligence on Customers (Legal Entity and Legal Arrangement)

		SWORN STATEMENT OF DUE DILIGENCE ON CUSTOMERS - LEGAL ENTITY AND LEGAL ARRANGEMENT			Macroprocess Legal Management
		GL-E004			Version: 01
<b>I. GENERAL INFORMATION ABOUT THE COMPANY (CUSTOMER)</b>					
Name or Business Name:		Tax ID No. or Equivalent Registration No.:			
Email:		Phone number of the main office or premises:			
Address of the main office or premises:		Street - Avenue - Road - Alley		No.	Apartment / Unit
		Neighborhood / Complex / Area / Sector		District	Province
				Department	Country
Corporate purpose, primary economic activity, or purpose of incorporation of the legal entity, as applicable:		Business sector in which it operates:		Approximate time in the market:	
<b>II. INFORMATION ABOUT THE PERSON CONDUCTING THE TRANSACTION ON BEHALF OF THE CUSTOMER (EXECUTOR)</b>					
First and Last Names:					
Type of ID document:		National ID Card ( ) Passport ( ) Foreigner's ID Card ( ) Other (Specify):		Document No.:	Nationality:
Position held at the company or type of relationship with the company:		Phone:			
Specify if you are acting on behalf of:		1) Power of Attorney ( )		2) Mandate ( ) 3) Other (specify):	
Details of the Public Instrument of Representation:		If by Public Deed, please provide the following information:			
		Date of the deed:		First and last names of the Notary:	
		Date of the certified copy:		If by Certified Copy of Minutes, complete the following information:	
				Date of the certificate:	
		If requesting another document, specify it in the box below:			
Registration Details:		Entry No.:		Registry Zone and Office No.:	
<b>III. IDENTIFICATION OF THE BENEFICIAL OWNER IN ACCORDANCE WITH ART. 4.1 OF LEGISLATIVE DECREE NO. 1372 (BENEFICIAL OWNER)</b>					
Identify the shareholders (Legal Entities) with a direct or indirect equity interest of 10% or more in the company's capital (only if 10% or more):					
A)	Name/Corporate Name			Percentage of Shares/Ownership:	
B)	Name/Corporate Name			Percentage of Shares/Ownership:	
C)	Name/Corporate Name			Percentage of Shares/Ownership:	
Identify the shareholders (Natural Persons) with a direct or indirect equity interest of 10% or more in the company's capital (only if 10% or more):					
A)	First and last names:	National ID Card ( ) Passport ( ) Foreigner's ID Card ( ) Other (Specify):		Document No.:	
B)	First and last names:	National ID Card ( ) Passport ( ) Foreigner's ID Card ( ) Other (Specify):		Document No.:	
C)	First and last names:	National ID Card ( ) Passport ( ) Foreigner's ID Card ( ) Other (Specify):		Document No.:	
<b>IV. IDENTIFICATION OF POLITICALLY EXPOSED PERSONS (PEP)</b>					
Is or has any of the shareholders with a stake equal to or greater than 10% of the share capital, partners, directors, and/or legal representatives of the company been a Politically Exposed Person (PEP) in the last two (2) years?				Yes ( ) No ( )	
Are you a shareholder, partner, director, and/or legal representative of the company, or the spouse, cohabiting partner, or relative up to the second degree of consanguinity or second degree of affinity of a Politically Exposed Person (PEP)?				Yes ( ) No ( )	
<p>Note: PEPs are natural persons, whether nationals or foreigners, who currently hold or have held in the past two (2) years prominent public office or prominent positions in an international organization, whether within the national territory or abroad, and whose financial circumstances may be of public interest. Likewise, a direct collaborator of the institution's highest authority is considered a PEP.</p> <p>Scope of PEP family relationship: This may include parents, children, siblings, grandparents, grandchildren, spouse, cohabiting partner, parents-in-law, siblings-in-law, children of the spouse, and grandparents of the spouse.</p> <p>(*) See PEP positions on the back of the page.</p>					
If you answered "Yes" to any of the questions, please provide the following information:					
A)	First and last names of the PEP:	National ID Card ( ) Passport ( ) Foreigner's ID Card ( ) Other (Specify):		Entity or institution and position held:	Relationship to the company or the shareholder, partner, director, and/or legal representative:
B)	First and last names of the PEP:	National ID Card ( ) Passport ( ) Foreigner's ID Card ( ) Other (Specify):		Entity or institution and position held:	Relationship to the company or the shareholder, partner, director, and/or legal representative:
<b>V. BENEFICIARY OF THE TRANSACTION</b>					
The transaction has been or will be carried out in favor of:					
1. Myself ( ) 2. A third-party natural person ( ) 3. A third-party legal entity ( ) 4. A third-party legal arrangement ( )					
If you answered "Myself," please complete the following box, if applicable:					
A)	Source of the funds or assets involved in the transaction when it is conducted in cash and equals or exceeds the threshold for purposes of the RO.				
If you answered "A third-party natural person," where applicable, complete the following box:					
A)	First and last names:	National ID Card ( ) Passport ( ) Foreigner's ID Card ( ) Other (Specify):		Document No.:	
Representation details:					
1) Power of Attorney by Public Deed ( ) 2) Power of Attorney ( ) 3) Other (specify):					
Representation Document Information:					
Date of the deed:		First and last names of the Notary:			
Date of the certified copy:		Date of the certificate:			
Other (specify):		Date of document:			
Indicate whether you are or have been, within the last two (2) years, a Politically Exposed Person (PEP):				Yes ( ) No ( )	
Indicate whether you have a spouse, cohabiting partner, or relative up to the second degree of consanguinity or second degree of affinity to a Politically Exposed Person (PEP):				Yes ( ) No ( )	
If you answered "Yes" to any of the questions, please provide the following information:					
C)	First and last names of the PEP:	National ID Card ( ) Passport ( ) Foreigner's ID Card ( ) Other (Specify):		Entity or institution and position held:	Relationship to the company or the shareholder, partner, director, and/or legal representative:
D)	First and last names of the PEP:	National ID Card ( ) Passport ( ) Foreigner's ID Card ( ) Other (Specify):		Entity or institution and position held:	Relationship to the company or the shareholder, partner, director, and/or legal representative:
Source of the funds or assets involved in the transaction when it is conducted in cash and equals or exceeds the threshold for purposes of the RO.					
If you answered "A third-party legal entity" or "A third-party legal arrangement," complete the following box:					
A)	Name / Corporate Name	Tax ID No. or Equivalent Registration			
Representation details:					
1) Power of Attorney by Public Deed ( ) 2) Power of Attorney ( ) 3) Other (specify):					
Representation Document Information:					
Date of the deed:		First and last names of the Notary:			
Date of the certified copy:		Date of the certificate:			
Other (specify):		Date of document:			
C)	Source of the funds or assets involved in the transaction when it is conducted in cash and equals or exceeds the threshold for purposes of the RO.				
D)	Identification of the beneficial owner of the transaction (first and last names)				
The company attaches to this form: (i) the identity document of its legal representative, (ii) the original Power of Attorney of its legal representative issued by SUNARP, dated no more than thirty (30) days prior to submission, and (iii) the public documents proving its existence and containing its name or corporate name. In the case of legal entities, the articles of incorporation attached.					
<b>DECLARATION OF TRUTHFULNESS OF THE INFORMATION</b>					
I hereby declare under oath that the information provided in this document is accurate and true, and I hereby release Corporación Aceros Arequipa S.A. (CAASA) from any legal liability (administrative, civil, and/or criminal) that may arise from any falsehood, omission, inaccuracy, or misrepresentation contained herein or that may arise if the illicit origin or destination of my funds is proven. Likewise, in the event if company becomes involved in an investigation or legal proceeding for the crimes mentioned in this sworn statement, due to causes attributable to my client, and the financial penalties and fines provided for in applicable laws are imposed, my client shall reimburse all expenses incurred and compensate CAASA for any damages caused.					
Signed in:		City / Country		Date (mm/dd/yyyy)	
		Name:		Signature of the Company's Legal Representative	
		National ID Card No.:			

## ANNEX No. 05: International Watchlists for ML/TF and PF Prevention

- OFAC List: a list issued by the Office of Foreign Assets Control of the U.S. Department of the Treasury, which includes countries, individuals, and/or entities that support terrorism and illicit drug trafficking.
- United Nations Security Council Terrorist List, specifically the lists of individuals or entities involved in terrorist activities and their financing, as well as the financing of the proliferation of weapons of mass destruction, in accordance with Resolutions 1267 (1999), 1718 (2006), 1737 (2006), and 2231 (2015) and any successor resolutions.
- European Union Terrorist List.
- Lists related to the Proliferation Financing of Weapons of Mass Destruction: lists issued by the UN Security Council, including the Consolidated List under UN Resolution 1718 on the Democratic People's Republic of Korea and the Consolidated List under UN Resolution 1737 on Iran.
- List of Non-Cooperative Countries and Territories.
- List of United Nations Security Council Resolutions.
- Any others designated by the Superintendency.

ACEROS  
AREQUIPA