Global Anti-Money Laundering Policy

Global Policy effective as of June 1st, 2020.

Proposed by:	**Raúl Sergio Salinas Tijerina** Compliance Director
Reviewed by:	**Jaime Martínez Merla** Internal Control Director
Approved by:	**Roger Saldaña Madero** SVP of Legal **José Antonio González** Chief Financial Officer

Index

1. Message from the Chief Executive Officer

At CEMEX, we are committed to conducting business in full compliance with the letter and spirit of all applicable laws, rules, and regulations and in accordance with the highest level of ethical standards. We are issuing this Global Anti-Money Laundering Policy in order to reaffirm our commitment to protect our companies and employees from being used by criminals to "launder" the proceeds of crime.

We strive to do business with transparency and integrity and to ensure that all transactions comply with all applicable anti-money laundering laws and regulations and to take all reasonable measures to prevent and detect money laundering.

Money laundering is a serious crime, often linked to violent acts such as terrorism and drug trafficking, as well as other illicit activities such as corruption. Criminal charges related to laundering or corruption brought against CEMEX by any governmental entity may damage CEMEX enormously, which may result in consequences like criminal conviction or forfeiture of funds and can lead to serious consequences for any individual involved. Even unwittingly doing business with money launderers or other criminals could damage CEMEX's reputation which could take years to recover. Therefore, at CEMEX, we have a zero-tolerance stance towards money laundering, as well as bribery or corruption of any kind.

This Policy is applicable to all of CEMEX´s operation worldwide and therefore applies to all CEMEX employees, officers, agents, board members, and directors. Each must read this Policy, and, if required, attend necessary trainings, and certify periodically that they have not and shall not engage in non-compliant behavior. This Policy also applies to Third Parties doing business with CEMEX. This Policy is available in the Policy Center and on CEMEX´s main website at www.cemex.com.

We at CEMEX prioritize anti-money laundering in all our work, and we expect each of you to join in this important effort.

Fernando A. Gonzalez Olivieri
Chief Executive Officer

2. Purpose of the Policy

The purpose of this Global Anti-Money Laundering Policy ("Policy") is to ensure CEMEX, S.A.B. de C.V. and its subsidiaries and affiliates (collectively "CEMEX"), as well as their respective members of the Board of Directors and committees, executives, directors, officers, employees and interns (collectively "CEMEX Personnel") comply with all applicable anti-money laundering and terrorism financing, including anti-money laundering laws in Mexico, the U.S. Bank Secrecy Act and PATRIOT Act, the EU Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing of 2015, amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 ("AMLD V"), and similar anti-money laundering and terrorism financing laws in effect in the countries where CEMEX does business (together "Anti-Money Laundering Laws"). Moreover, this Policy is also intended to ensure all business activities carried out with Third Parties comply with Anti-Money Laundering Laws.

CEMEX has adopted a zero-tolerance standard with respect to conduct that violates any Anti-Money Laundering Laws. As such, CEMEX seeks to do business only with Third Parties that conduct legitimate activities, share this standard and are committed to follow these standards.

This Policy sets out guidelines and mechanisms designed to ensure that all CEMEX Personnel and businesses are well informed and trained to be able to detect, mitigate, prevent and report acts and/or transactions which could involve potentially illegally obtained resources, in order to promote compliance with the applicable Anti-Money Laundering Laws and to avoid possible damages to the integrity, stability and reputation of CEMEX.

This Policy should be read along with CEMEX's Code of Ethics and Business Conduct, Global Anti-Corruption Policy, as well as any other relevant and applicable policies, guidelines, procedures and controls to which CEMEX Personnel are subject. This Policy shall control over any local or regional policy, procedure or practice inconsistent with the terms hereof. However, where local law, procedure or practice is more restrictive than this Policy, the more restrictive local requirements shall govern.

This Policy is applicable to all CEMEX Personnel, regardless of where they reside or conduct business, and Third Party relationships over which CEMEX has control, including entities where a minority position is held and any joint ventures, as well as all agents, consultants, and other Third Party representatives when they act on CEMEX's behalf. All CEMEX Personnel is expected to comply with this Policy, participate in relevant training, and communicate the principles established by this Policy to their colleagues, direct reports and Third Parties. In addition, CEMEX Personnel, exposed to money laundering situations, shall be required to provide periodic anti-money laundering training certification, as required by the Compliance Area. Before engaging in a business relationship with CEMEX, all Third Parties are required to sign the CEMEX Third Party Compliance Declaration.

3. Roles and Responsibilities

The Compliance Director and the Regional Compliance Officers have been designated as the AML Compliance Officers and shall oversee global compliance with this Policy and applicable Anti-Money Laundering Laws. The AML Compliance Officers are responsible for:

- Supervising the implementation of the Policy;

- Together with the Local Legal Department, monitoring any changes in applicable laws and any prevalent techniques or cases related to the Anti-Money Laundering Laws in order to ensure that the Policy remains effective and updated;
- Ensuring global compliance with the Information Retention Policy;
- Ensuring that training for CEMEX Personnel is consistent with this Policy;
- Ensuring that the Local Legal Department together with their corresponding Regional Compliance Officer elaborate a summary annual report related to local compliance with this Policy;
- Providing to CEMEX´s Audit Committee a summary report related to global compliance with this Policy at least every year; and
- Ensuring that compliance with this Policy is evaluated and audited at least every two years.

4. Definitions

For the purposes of this Policy, the following terms shall have the definitions set forth below:

"AML" refers to Anti-Money Laundering.

"Anti-Money Laundering Laws" refers to anti-money laundering laws in Mexico, the U.S. Bank Secrecy Act and PATRIOT Act, EU Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing of 2015, amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 ("AMLD V"), and similar anti-money laundering and terrorism financing laws in effect in the countries where CEMEX does business or has operations.

"BSO" refers to the Business Service Organization and the Global Service Organization, who have, among other responsibilities, the delivery of business and transactional services to CEMEX operations in the execution of controls within CEMEX.

"Cash Payment" refers to, but is not limited to, remittances of cash (including coins and bank notes), including a cashier's check, and direct cash deposits to the corresponding CEMEX bank account; not withstanding this definition, a different definition could be established in accordance with the applicable local law.

"CEMEX's Audit Committee" refers to the 1) Audit Committee of Cemex, S.A.B. de C.V., 2) Audit Committee of CEMEX LATAM Holdings, and 3) Audit Committee of CEMEX Holdings Philippines.

"CEMEX Personnel" refers to the members of the Board of Directors and committees, executives, directors, officers, employees, and interns.

"Compliance Area" refers to the team that is composed by the Compliance Director, Regional Compliance Officers, and other Regional or Local Lawyers and their respective staff, whose function is to ensure business processes and transactions are compliant with applicable international laws and regulations, internal policies, guidelines, procedures and controls.
"**CT**" refers to the Commercial Team.

"One-time customer" refers to those customers that execute a single transaction, that is that they are not recurring customers.

"SAP" is CEMEX's transactional system used to register suppliers or clients, carry out payments, accounting purposes and other transactions.

"Subsidiary" refers to any legal entity in which CEMEX: (1) participates directly or indirectly in its share capital and in which it holds the ownership of rights that directly or indirectly permits voting with respect to more than 50% of such share capital; or (2) directs, directly or indirectly, the management, strategy or principal policies of the entity, whether through the ownership of stock and securities, contract or under any other legal figure.

"Third Party(ies)" refers to any of CEMEX´s customers, including but not limited to, credit customers and/or one-time customers, joint venture partners, suppliers and any other third party making a payment to CEMEX.

"Third Party Service Provider" refers to the external supplier that conducts due diligence processes and screenings on potential credit customers and/or one-time customers.

"Ultimate Beneficiary(ies)" refers to any entity or person that ultimately owns or controls a Third Party and/or the entity or person on whose behalf a transaction is made. This includes an entity or person that has, directly or indirectly, 25% or greater ownership in the Third Party, or exercises effective control over a company, partnership, corporation, trust or other legal structure, or if the applicable local law dictates a property percentage less than 25%.

The terms mentioned above may be used in singular or plural, without it being understood that their meaning changes.

5. Mechanics of Money Laundering

Money laundering is the process of disguising the nature and source of money or other property connected with criminal activity, such as drug trafficking, terrorism, bribery, or corruption, by integrating the illicit money or property into the stream of commerce so that it appears legitimate or its true source or owner cannot be identified. Those involved in the criminal activity attempt to hide the proceeds of their crimes or make them appear legitimate by "laundering" them through legitimate businesses. Relatedly, terrorism may be financed with legitimate funds, sometimes called "reverse money laundering" because a legitimate business is used to fund a criminal activity.

The money laundering process is typically accomplished in three stages, either on separate or distinct phases, that may comprise numerous transactions. Any one of these transactions or stages could involve CEMEX or CEMEX Personnel:

A. PLACEMENT: The first stage is the placement of funds into the economy. It is a means by which material proceeds derived from illegal activity are physically disposed into the market. It is usually done through the purchase of goods, deposits in financial institutions, creation of "phantom" companies, etc.

B. LAYERING: The second stage involves separating illicit proceeds from their sources by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity. This stage will usually depend on the steps or activities carried out during the placement stage. For example, after making a deposit into a bank account during the

placement stage, a launderer could make several transfers and transactions to move the deposited funds in order to conceal the original deposit. Placement and layering are usually performed through a Third Party.

C. REINTEGRATION: The third stage involves attempting to make the proceeds of illegal activities appear completely legitimate. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they appear to the financial system to be legitimate funds. For example, criminal proceeds could be used to buy a third party business, which carefully follows regulations, and the profits of the business are then transferred back to the criminal enterprise in a manner that appears legitimate.

6. Legal and Regulatory Framework

CEMEX operates in different countries and is therefore subject to Anti-Money Laundering Laws in several jurisdictions. Violations of these laws could result in severe consequences for CEMEX, including expensive investigations, reputational damage, and disqualification from serving as a government business partner or supplier. They could also lead to significant economic sanctions and potential imprisonment of individuals. Consequently, compliance with Anti-Money Laundering Laws is mandatory and a high priority at CEMEX. CEMEX Personnel shall endeavor to understand what laws or regulations govern his or her conduct, and to comply with those governing laws and regulations. If a local regulation impedes the implementation of any obligations under this Policy, CEMEX Personnel must notify the Compliance Director, Regional Compliance Officer and the Local Legal Department. Additionally, where local law is more restrictive than this Policy, the more restrictive local law will control.

a. MEXICO

The Federal Law for the Prevention and Identification of Operations with Resources of Illegal Origin *(Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita*) sets forth the parameters by which an activity will be considered vulnerable to money laundering. It also provides guidance on proscribed activities as well as situations where respective notices must be presented.

The sanctions set forth by this law include monetary sanctions that can reach up to $4,556,500.00 Mexican pesos and/or criminal conviction in case of a federal crime, such as perjury and money laundering.

b. UNITED STATES

U.S. prosecutors, including the U.S. Department of Justice ("DOJ"), have the authority to impose significant penalties against corporations and, in some circumstances, against individual employees. Even inadvertent violations of U.S. anti-money laundering laws may result in civil penalties. Any person (including a non-U.S. Person) who aids or abets or causes a U.S. person to violate these laws may also be subject to civil and criminal penalties. Among the main laws applicable to anti-money laundering in the U.S., the following are of note:

(i) The Money Laundering Control Act of 1986, 18 U.S.C. §§ 1956-1957, which makes money laundering a federal crime;
(ii) The Intelligence Reform and Terrorism Prevention Act of 2004, which, among other things, seeks to prevent the financing of terrorism and money laundering;

(iii) The USA PATRIOT Act of 2001, which establishes, among other things, the governmental powers for the prevention of terrorism and authorizes the U.S. State Department to designate terrorist organizations under the Terrorist Exclusion List; and

(iv) The economic sanctions programs administered by OFAC (collectively, the "OFAC Laws"; OFAC stands for Office of Foreign Assets Control) that limit or, in some cases, prohibit altogether transacting with certain entities and individuals.

(a) The OFAC sanctions programs are generally divided between (i) comprehensive sanctions that target entire countries or jurisdictions, their governments, and any persons located in those countries (i.e. Cuba, Crimea, Iran, North Korea, Syria); (ii) partial sanctions programs that target specific sectors in a country's economy (e.g., Somalia, Venezuela and Ukraine/Russia), (iii) list-based programs (e.g., Iraq, Lebanon, and Zimbabwe); and (iv) activity-based programs (e.g., the sanctions placed on terrorists, proliferators of weapons of mass destruction, and drug traffickers). Persons sanctioned under the list-based and activity-based sanctions are included in OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List").

(b) Failure to comply with the OFAC Laws can involve severe civil and criminal penalties for CEMEX Personnel. Criminal penalties may include up to 20 years imprisonment and criminal fines of up to USD 1,000,000 per violation. Civil penalties may include significant monetary penalties, freezing or blocking of assets, and reputational harm.

c. EUROPEAN UNION

The EU Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing of 2015, amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 ("AMLD V"), sets out guidelines for anti-money laundering, suspicious activity reports, specific transactions reports, legal auditing of clients, identification of the Ultimate Beneficiary of the business, registration of certain information, and other related obligations.

The adoption of this legislation by the European Union seeks to bring further transparency in the financial system of the region as well as to the countries that are part of it. It is necessary for CEMEX employees to comply with AMLD V requirements. It is important to note that the consequences of non-compliance can amount to € 5 million in fines or 10% of the company's annual profit, in some cases.

7. The Concept of "Knowledge" in Money Laundering

Generally, many Anti-Money Laundering Laws criminalize the act of knowingly conducting a transaction with the proceeds of a crime. In some countries, the government may prove "knowledge" by proving that the defendant is engaged in "willful blindness." Willful blindness is a deliberate failure to make a reasonable inquiry of wrongdoing despite suspicion or an awareness of the high probability of its existence. This could mean that even if a CEMEX employee does not have direct knowledge of the illegal nature of the proceeds involved in a transaction, CEMEX may still be liable for money laundering offenses

if circumstances raised enough suspicions of money laundering activities, but no actions were taken by CEMEX to follow up on the suspicions.

The following is a non-exhaustive list of examples of activities that could fall within the definition of money laundering or that might constitute evidence of money laundering under Anti-Money Laundering Laws:

(i) Engaging in a transaction with knowledge that the transaction is facilitating criminal activity or with knowledge that the funds being used are derived from the proceeds of criminal activity;
(ii) Concealing the source of criminally obtained funds by subsequent transfers to disguise the origin of the funds; or
(iii) Facilitating a transaction while willfully or recklessly disregarding the source of an investor's assets or the nature of the investor's transactions or business operations.

8. Due Diligence

The Compliance Area shall conduct due diligence checks ("Due Diligence" or "DD Checks") on Third Parties with which CEMEX does business with based on the risk assessment mentioned below. The DD Checks shall be conducted on a risk basis taking into account point 12 below.

On a risk basis, the following steps shall also be taken:

(i) Verifying the Third Party's identity. For individuals, this can include requesting a copy of their passport or the national identity document containing the name, date of birth, tax identification number and valid government identification, consistent with local laws, and also request their physical address. For a legal entity, this can include requesting incorporation documents or certificates of good standing from a relevant governmental agency, as well as their legal representatives, owners, or Board Members´ data;
(ii) Collecting from the Third Party the signed Third Party Compliance Declaration;
(iii) Identifying the Third Party's Ultimate Beneficiaries and verifying the Ultimate Beneficiaries against official documentation;
(iv) Confirming the Third Party's legal status by checking official and/or authenticated documents (such as copies of business licenses, tax registrations, articles of incorporation, bank references, credit agency reports, or any other equivalents deemed reasonable);
(v) Collecting, in the case of a Third Party entity such as a company, partnership, trust, etc., its place(s) of operations and identity and nationality of its shareholders, administrators, and directors, as well as its bylaws, articles of incorporation, or equivalent in each country it operates;
(vi) Obtaining any other Third Party information which is collected as a part of ordinary business practice, such as financial statements, credit agency reports, bank references, and bank account information, ownership and control structure;
(vii) Screening the Third Party against relevant AML and sanctions lists. These include, but are not limited to, the OFAC SDN List, the U.S. State Department's Terrorist Exclusion List, other relevant sanctions lists in the jurisdictions in which CEMEX operates, and commercially available AML lists (e.g., LexisNexis, World-Check or Factiva); and
(viii) Notifying the Third Party in writing of this Policy and the Third Party's obligation to comply with all applicable Anti-Money Laundering Laws. Once the DD information has been collected, the Regional Compliance Officer, in consultation with the BSO or the Commercial Team as applicable according to Annex I, shall determine whether the transaction or commercial relationship should proceed based on the information provided.

Records of Due Diligence determinations and associated documentation shall be updated, on a risk basis, if appropriate, every two (2) years or whenever CEMEX Personnel detects a red flag. (See "9. Spotting Red Flags" below.) BSO or the Commercial Team, in the countries where BSO is not responsible for managing the information regarding customers, is responsible for administering and managing Third Parties' information on SAP and requesting additional information, if necessary. For more information on which For more information on which area is responsible for the customer matters please consult Annex I.

The BSO or CT shall, on a quarterly basis, provide the Compliance Area a digital copy of the report of all the approved or rejected transactions during that period, which shall include the reasons of said approval or rejection.

The Compliance Area shall maintain a record of all approved and rejected transactions. The record must include the reasons behind such approval or rejection.

9. Spotting Red Flags

CEMEX Personnel should be alert to suspicious behavior or "red flags" when doing business with, conducting DD checks on, and/or monitoring continued engagement with Third Parties. Annex II contains a non-exhaustive list of red flags that, if observed, should be reported to the Compliance Area and/or the Local Legal Departments.

If a red flag is spotted, the Compliance Area and/or Local Legal Department must be notified and will investigate the red flag, in coordination amongst themselves and with the Regional Counsel, and take further action consistent with this Policy and relevant Anti-Money Laundering Laws. The Local Legal Departments will have access to the Compliance for Entities Tool.

Such an investigation may entail a thorough review of the business relationship with the Third Party and any previous transactions with the Third Party to ensure that such transactions were consistent with this Policy and CEMEX's knowledge of the Third Party, its commercial activity and risk profile, and, when necessary, the source of its funds.

10. Payments

CEMEX should undertake payment acceptance due diligence measures to reduce the risk of receiving monies involved in money laundering activities. Third parties should be notified that acceptable forms of payments should be limited to the following:

(a) Wire transfer from a bank account in the Third Party's name;
(b) Credit or debit card; or
(c) Check drawn on a bank account in Third Party's name.

CEMEX may accept a wire transfer which does not specify any bank account owner, if it is legally acceptable in the country where the transaction is taking place. The Local BSO or CT must keep a record of the Third Party's report of such wire transfer, including confirmation of the Third Party's bank account details (i.e. bank name, and account name).

a. Cash Payments

The making or receiving of Cash Payments in excess of the applicable local thresholds set forth in this Policy is prohibited (consult the Related Documents Section in the Policy Center to view the applicable thresholds for each country). CEMEX may make or accept a Cash Payment above the applicable threshold subject to prior written approval of the Compliance Director or Regional Compliance Officer or the Regional Counsel, only when allowed by the applicable local law. The Compliance Director, Regional Compliance Officers or the Regional Counsel, as applicable, may only approve the making or accepting of a Cash Payment if all the following conditions are met:

(i) The Cash Payment is legal and commercially reasonable in consideration of local business practices and with respect to the Third Party, and such reasons are documented;
(ii) CEMEX obtains ownership information of the Third Party, except for Third Parties who are publicly traded companies, government owned companies, or officially accredited educational institutions, notwithstanding those exceptions, CEMEX shall intend to obtain ownership, ultimate beneficiary information or certificate by the board of directors´ secretary or similar entity;
(iii) The Cash Payment is made in compliance with the notification and record keeping requirements of applicable local laws and regulations and the Cash Payment is not made in such a way that it appears intended to circumvent such requirements; and
(iv) Controls are in place to detect any AML red flags involving the Cash Payment (see Annex II).

The Compliance Director and the Local Legal Department, in coordination with the Regional Compliance Officers, may establish one or more thresholds for small Cash Payments, to be applied to transactions with specified Third Parties in specific geographic regions, for which CEMEX employees need not seek prior written authorization for each transaction. In additional to the requirements (i) through (iv), above, a decision to establish such thresholds should consider:

(v) Whether, in the country in which they are made, such Cash Payments are common and commercially reasonable considering the business line, Third Parties and transactions at issue; and
(vi) Whether non-Cash Payment options are available for such transactions.

The BSO or CT must document and maintain records related to any rejection or approval of any Cash Payment, with reasons supporting the decision.

The Compliance Area and Local Legal Department must document and maintain records related to any decision to establish any value thresholds for small Cash Payments as described above.

Notwithstanding the above, no Cash Payments above the thresholds, set forth in the Related Documents Section in the Policy Center, shall be permitted when made by one-time customers.

11. Training

Anti-money laundering training shall be provided at least once to CEMEX´s employees in money laundering sensitive areas (such as BSO, sales department, finance, treasury, accounting or credit departments). The Compliance Director, together with the Regional Compliance Officers and Local Legal

Departments, shall provide a periodic refresher training at least every two (2) years to employees of the sensitive areas.

The Compliance Director, with the assistance of the Regional Compliance Officers and Local Legal Departments, shall maintain a record of those CEMEX employees who attend such trainings and shall maintain a copy of the materials used for such training.

12. Risk Assessment

Each regional and local Enterprise Risk Management area shall conduct an assessment to be updated every two (2) years, of CEMEX's anti-money laundering risks as its business evolves and expands. The results of the risk assessment shall be shared with the Regional Compliance Officers and Local Legal Departments to evaluate any necessary enhancements to this Policy.

13. Internal Review and Audit

The Compliance Area shall perform a formal internal review of CEMEX's compliance with this Policy at least once every 2 years. The review will include an annual written report, which will be sent to the Audit Committee and retained by the Compliance Director in accordance with CEMEX's information retention policies. Any deficiencies identified during the independent review will be accompanied by written plans to address the deficiencies in a manner consistent with CEMEX Policy.

The internal review will cover the following:

- any updates on the laws and techniques or cases related to AML and economic sanctions,
- any investigations and the reasons behind moving forward with a transaction or deciding to stop it;
- the summary of the annual AML risk assessment;
- the implementation of any training activities; and
- the results of any internal review and audits and the measures to address any internal review and audit findings.

14. Record Keeping and Data Retention

CEMEX shall record and maintain, subject to CEMEX´s Global Information Retention Policy, all information required or gathered as part of its:

(i) Due diligence checks as well as documents relating to Third Parties' local and international transactions with CEMEX, in compliance with CEMEX's Global Information Retention Policy, for a maximum period of ten (10) years after the business relationship with the Third Party has ended;

(ii) Anti-money laundering training issued to CEMEX employees and Third Parties, in compliance with CEMEX's Global Information Retention Policy, for a maximum period of ten (10) years after the date of the training;

(iii) Internal reviews or audits into relevant Third Parties, in compliance with CEMEX's Global Information Retention Policy, for a maximum period of five (5) years after the date of the review or audit; and

(iv) Any decision rejecting or approving the making or receiving of one or more Cash Payments as described in Section 10, for a maximum period of five (5) years.

15. Consequences of Non-Compliance

Violations of any applicable Anti-Money Laundering Laws or this Policy may result in criminal prosecution and/or the imposition of civil sanctions, not to mention potential long-term harm to CEMEX's reputation. Under no circumstances shall a CEMEX employee facilitate or participate in any money laundering activity. CEMEX will not pay any fine imposed on any CEMEX employees or Third Party nor any attorney´s fees as a result of a breach of any Anti-Money Laundering Laws or this Policy.

In addition, any breach of this Policy may result in disciplinary action, including possible termination of employment, or such other remedial or disciplinary action as shall be appropriate under the circumstances, in accordance with the applicable labor law. Conversely, CEMEX will fully support any CEMEX employees or Third Parties who decline to engage in conduct that would place CEMEX's ethical principles and reputation at risk.

16. Reporting Requirements

If a CEMEX employee knows of or suspects a violation of applicable Anti-Money Laundering Laws or this Policy, they **must** report the facts promptly through the Process Assessment Department, Compliance Director, Regional Compliance Officers, Local Legal Department, or ETHOSLine, which is an independent and anonymous avenue through which CEMEX employees can communicate their concerns or report any suspected or actual instances of misconduct without fear of retaliation or reprisal.

CEMEX strictly prohibits retaliation against any individual who raises concerns in good faith regarding actual or suspected misconducted related to this Policy or any Anti-Money Laundering Laws. Such retaliation would be grounds for discipline, against whoever intends to exercise it, including potential termination of employment.

Consistent with its obligations under the law, and the enforcement processes established in CEMEX's internal policies, CEMEX will keep confidential the identity of anyone reporting in good faith a possible violation to the extent reasonably possible. No one will be terminated, demoted, suspended, harassed, or discriminated against solely because they reported in good faith a possible violation.

17. Contact Information

The Compliance Director, Regional Compliance Officers and the Process Assessment Department will monitor the compliance of this Policy.

18. Internal Controls

Control 1: Validation of third parties' legal documentation before its registration in SAP

To register a Third Party in SAP, CEMEX users shall submit a request for the creation of a Third Party with general data and upload the required documentation. (1) BSO or Commercial Team ("CT") is responsible of verifying that the CEMEX user has submitted the complete required documentation (2) to SAP and that the information captured (3) is complete and accurate. If needed, BSO or CT shall request corrections or additional documents to ensure the accuracy of the records. Additionally, BSO or CT shall capture in the respective SAP fields if the Third Party is a government entity (092) and/or will act on Cemex's behalf as an agent or representative.

When the documentation is complete and the information has been validated, the Third Party should be registered in SAP unless it falls under a high-risk category.

BSO or CT shall send the request of these high-risk Third Parties to the Compliance Area in order to be validated. In every case, there must be written approval or rejection of the Compliance Area sent to the BSO or CT. This shall be documented by the BSO or CT. Once BSO or CT has received the written approval, the Third Party will be registered in SAP.

This control aims to mitigate the risk of registration of Third Parties that do not comply with the legal documentation and the lack of visualization of high risk Third Parties.

Audit support evidence
• The email sent by BSO or CT including the complete required documentation to the Compliance Area for its evaluation. • The written approval, rejection or evaluation sent by the Compliance Area.

Control 2: Sanction screening and evaluation of third parties

When the Compliance Area receives an email from BSO or CT to verify a high risk potential third party (a third party acting as a Cemex agent or representative, as specified in their signed Third Party Compliance Declaration, or a government entity), they should verify that the documentation received from BSO or CT is precise and complete; carry out the compliance screening to verify if the third party is invalidated (by falling in one or more of the following categories: Politically Exposed Person, Corruption, Government Entities (or government owned entities) and/or money laundering.) to be retained by Cemex under the principles set out in the relevant policies.

One of the following scenarios will proceed from the Compliance Area review:

- If the third party shows no relevant results that indicate that the third party is invalidated to be retained by CEMEX, the Compliance Director, Regional Compliance Officers or the Third Party Service Provider will inform via email their approval of the Third Party´s registry to BSO or CT.
- On the other hand, if the third party shows relevant results that indicate that the third party is invalidated to be retained by CEMEX, the Compliance Director or Regional Compliance Officers will carry out additional investigations together with the Local Legal Department in order to evaluate how to proceed.

This control aims to mitigate the risk of retaining third parties that do not comply with the standards set out in the relevant policies and other applicable regulations.

Audit support evidence
• The email sent by BSO or CT including the complete documentation to the Compliance Area for its evaluation. • The email sent by the Compliance Director, Regional Compliance Officers or the Third Party Service Provider to BSO or CT including the screening results detailing that **no relevant results** were found and an explicit written approval to register the Third Party in SAP. • The email from the Compliance Director or Regional Compliance Officers to the Local Legal Department including the screening results informing that **relevant results** were found, and additional investigation needs to be carried out.

Control 3: Control: Validation of relevant results found – Due diligence

Whenever relevant results are found in the initial screening process, the Compliance Area will carry out additional investigations supported by the Local Legal Departments or Regional Counsel who will provide an investigation and supporting evidence to help the Compliance Director or Regional Compliance Officers on their decision of approving or rejecting a third party.

The Compliance Area will instruct BSO or CT to capture in the respective SAP field and classify the Third Party as a Government Entity (092) if there are results in the investigation that confirm that the Third Party is a Government Entity, Government Official or somehow there is a government participation.
This control aims to mitigate the risk of registering third parties based on incomplete information that should be supported by further investigation.

Audit support evidence
• Email from the Compliance Director or Regional Compliance Officers to the Local Legal Departments requesting support with the investigation of relevant results. • Email from the Local Legal Departments to the Compliance Director or Regional Compliance Officers detailing their investigation results and supporting evidence. • Email from the Compliance Director or Regional Compliance Officers to BSO or CT including the screening results, an explicit approval or rejection of the Third Party registration on SAP and other instructions, as applicable.

Control 4: Periodic monitoring and blocking of Third Parties

The Compliance for Entities Tool performs an automated monthly review of the Third Parties master data file, which includes all Third Parties registered on SAP, in order to make sure that no recent activity has been carried out by Third Party that could invalidate them to be retained by Cemex under the applicable internal policies.

Once it is known that the Third Party appears on any database or sanction list in the Compliance for Entities Tool, the Compliance Area will notify BSO or CT.

Based on the confirmation by BSO or CT, the Compliance Area will execute one of the following actions:

- **Inactive Third Parties**. Third Parties will be blocked in SAP through the Compliance for Entities Tool.

- **Active Third Parties**. If it is the case, will request the Local Legal Departments to conduct an investigation and supporting evidence to help the Compliance Director or Regional Compliance Officers on its final decision of approving or rejecting a Third Party.
  Note: Regarding any doubt of blocked third parties executed by the Compliance Area contact the Compliance Director and/or the Compliance Area.

  The Compliance Area will instruct BSO to capture in the respecitve SAP field and classify the Third Party as a Government Entity (092) if there are results in the investigation that confirm that the Third Party is a Government Entity, Government official or somehow there is a government participation.

This control aims to mitigate the risk of retaining third parties that have recently engaged in activities that could invalidate them or have been sanctioned by relevant countries and lists after their registry in SAP.

Audit support evidence
• Email from the Compliance Area to the Local Legal Departments requesting support investigating relevant results. Email sent to BSO or CT by the Compliance Area including the monthly report of cases identified in the Compliance for Entities Tool to notify them of the matches. • Email confirmation from the BSO or CT detailing the explicit status of active/inactive Third Parties. **For active third parties**: • Email sent to the Local Legal Departments by the Compliance Director or Regional Compliance Officers requesting support investigating relevant results of Third parties. • Email including the investigation results and supporting evidence by the Local Legal Department to the Compliance Director or Regional Compliance Officers, if applicable. • Monthly report of cases identified including the Third Parties´ active/inactive and approval/block status. • Email from the Compliance Director or Regional Compliance Officers to BSO or CT including the screening results and an explicit approval/rejection of the Third Party registry in SAP.

Control 5: Payments making and reception control

Making or receiving Cash Payments in excess of the thresholds set forth in the document titled Thresholds by Country, available in the Related Documents Section in the Policy Center is prohibitted. For any exception, the BSO or CT, should seek for the authorization of the Compliance Director or Regional Compliance Officers prior to the execution of the transaction.

This control aims to mitigate the risk of receiving monies involved in money laundering activities.

Audit support evidence
• Evidence of written authorization of all exceptions.

Control 6: Anti-Money Laundering Training

Ensure that an anti-money laundering training is conducted by the Compliance Area to the sensitive areas at least every two (2) years.

This control aims to mitigate the risk of non-compliance with applicable Anti-Money Laundering Laws in CEMEX business.

Audit support evidence
• Evidence of training material used for the training sessions • Evidence of the employee attendance at the training sessions

Control 7: Enterprise Risk Management Assessment

Validate that the regional or local ERM performs an anti-money laundering risk assessment at least every two years and informs the Compliance Area about the results of this risk assessment. ERM results should be considered for the enhancements and update of this Policy.

This control aims to mitigate the risk of non-awareness of possible risks associated with the expansion and evolution of our business.

Audit support evidence
• Evidence that the ERM risk assessment results report was shared with the Compliance Area. • Summary of ERM identified risks and its impact on this Policy for its update.

19. Annex I: Identification of the responsible areas for managing Third Parties' information on SAP

Country	Responsible for recording and updating the system's data regarding customers
Mexico	Commercial Team (Experiencia del Cliente)
Colombia	BSO Team (CSR Colombia)
Bahamas	Commercial Team
Costa Rica	BSO Team (CSR Colombia)
Dominican Republic	BSO Team (CSR Colombia)
Nicaragua	BSO Team (CSR Colombia)
Panama	BSO Team (CSR Colombia)
Jamaica	BSO (Commercial Administration)
Puerto Rico	BSO Team (CSR Colombia)
Guatemala	BSO Team (CSR Colombia)
Haiti	Commercial Team
Peru	BSO Team (by Local Service Center)
Belize	BSO Team (Sales Rep. services Area in Monterrey/Mexico)
El Salvador	BSO Team (CSR Colombia)
TCL Group	BSO (Commercial Administration)
USA	BSO Team (Transactional Services/IBM or other third parties)
UK	BSO Team
Poland	Commercial Team (third party)
Germany	BSO Team
France	BSO Team Customers / Commercial Team Job sites
Croatia	Commercial Team (Commercial support - Logistics)
Bosnia	Commercial Team (Commercial support - Logistics)
Serbia	Commercial Team (Commercial support - Logistics)
Montenegro	Commercial Team (Commercial support - Logistics)
Spain	Commercial Team (Commercial Agents)
Italy	BSO (Account Receivable Team)
Czech Republic	BSO Team
Egypt	BSO Team for Ready Mix and Commercial Team for Cement
Israel	BSO Team (Sales Administration)
UAE	BSO Team
Philippines	BSO Credit

20. Annex II: Non-Exhaustive List of AML Red Flags

1. The Third Party shows unwillingness to provide identification documents or any other data requested during the DD check or such information is incomplete, wrong or misleading;

2. The Third Party uses a false address;

3. The Third Party displays expired identification;

4. The Third Party provides inconsistent information;

5. The Third Party has complex shareholding structures which are not reasonably justified;

6. The Third Party's operations drastically change over time in volume or amount;

7. The Third Party shows unusual concerns related to the disclosure of any such data requested, particularly regarding its identity and type of business;

8. The Third Party unreasonably questions the requirements of documentation and handling of information;

9. The Third Party's financial information reflects asset concentration in subsidiaries or affiliates where there is an absence of audited financial statements;

10. The Third Party refuses to provide information regarding its subsidiaries and affiliates, if and when requested;

11. The Third Party has multiple accounts under the same name for no apparent purpose;

12. The Third Party or an individual or any of its subsidiaries or affiliates has a negative background, such as criminal records, civil penalties of any kind, or investigations regarding tax fraud, money laundering activities, and/or organized crime;

13. The Third Party, or one of its owners or board members, is on OFAC's List of Specially Designated Nations and Blocked Persons;

14. The Third Party, or one of its owners or board members, is on the U.S. State Department's Terrorist Exclusion List;

15. The Third Party refuses to or is unable to identify a legitimate source of its funds;

16. The Third Party transacts with important public figures, such as public officials or other politically exposed persons;

17. The Third-Party attempts to send or receive a payment in cash, or cash equivalents, in excess of EURO 10,000, or its equivalent in local currency, for Europe, the Middle East and Asia or USD 10,000, or its equivalent in applicable local currency, for North America, South America or the Caribbean Region, or any other threshold, as set forth in the Policy.

18. The Third Party makes payments through the accounts of different individuals or entities rather than through its own accounts;

19. The Third Party's payments are done through a credit institution of different nationality than that of the Third Party;

20. The Third Party frequently engages in transactions where payments equal the maximum amount allowed for withdrawals at financial institutions;

21. The Third Party seeks to bribe, threaten or persuade CEMEX employees to avoid any obligation related to this Policy or Anti-Money Laundering Laws;

22. There are deposits in foreign currency made by multiple individuals for the same transaction;

23. The Third Party requests unjustifiably high or low prices for products or services which are not within market standards;

24. The Third Party requests or ensures that goods are transported through more than one jurisdiction for no apparent reason;

25. The Third Party frequently changes its payment instructions;

26. The Third Party requests or proposes excessive modifications to letters of credit or similar documents;

27. The Third Party provides false invoices or invoices with miscellaneous charges that have not been previously approved by CEMEX;

28. The Third Party makes an unusually large amount of overpayment or requests a refund to be sent to an unknown Third Party as a result of cancelled purchase order;

29. The Third Party's representative seems not to know basic facts about the Third Party's business, which raises suspicion as to whether he or she is actually employed by the Third Party;

30. The Third Party requests CEMEX to issue an invoice which does not accurately reflect an invoiced price or other material terms of the transaction;

31. The Third Party structures a transaction to circumvent the notification requirements of authorities or governments, for example by paying one invoice with numerous money orders or cashiers' checks in amounts under the notification requirements; or

32. The Third Party has a broker, attorney, or other agent to facilitate the transactions which is unusual for the type of business, and CEMEX has no proper information or documentation regarding such agent or such agent's authority.