Crime
Prevention Manual

Antofagasta Plc

Chilean Law 20.393 and UK Bribery Act

May 2019

Risks and Compliance Department
Vice Presidency of Administration and Finance

Contents

I. Introduction

Law 20.393, which entered into force in Chile at the end of 2009, and its amendments, establishes the criminal liability of legal persons for the crimes of money laundering, financing terrorism, incompatible negotiation, bribery, bribery of public officials, commercial bribery, reception, misappropriation, unfair administration, water pollution, violation of banned products, illegal fishing of seabed resources, illegal processing and storage of scarce products and any other crime that the same legislation may contemplate. Similarly, the **UK Bribery Act**, which came into force in July 2011, establishes criminal liability for acts of bribery and corruption in the private and public sectors, as well as the failure of companies to prevent bribery. Other countries where Antofagasta plc operates also have anti-corruption laws.

Anti-corruption laws have an international application. Therefore, the actions of any employee, or third party associated to the business of Antofagasta plc, may impact our organisation for not complying with these laws. It is noted that the foregoing is without prejudice to individual responsibilities for the commission of any of the aforementioned crimes.

As part of compliance with the Laws (**UK Bribery Act, Law 20.393** and other applicable anti-corruption legislation) and their duty of supervision and management, both the Board of Directors of Antofagasta plc, as well as the Boards of the companies that are part of the Antofagasta Group, approved the implementation of a **Crime Prevention Model** (hereinafter, **CPM**) that is part of the **Compliance Model**, which, more broadly, seeks to establish an **honest, upright, ethical and sustainable environment** in the organisation, preventing, detecting and acting against potential irregularities.

This **Crime Prevention Manual** (hereinafter, **Manual**) establishes how the different activities work to prevent, detect and mitigate the potential risks of committing crimes to which the companies that form part of Antofagasta plc are exposed. These risks have been integrated into the **CPM**.

The following form part of the **CPM**:

1. Code of Ethics.
2. Compliance risk analysis.
3. Tools to prevent identified crimes.
4. Tools to detect potential irregularities.
5. Action plans to address detected potential irregularities.
6. Continuous improvement of **CPM**.

II. Objectives

The objectives of this **Manual** are:

- Define the activities and procedures required to effectively implement and operate the Crime Prevention Model (**CPM**).
- Set up a mechanism to prevent and mitigate the crime risks to which the companies that are part of Antofagasta plc are exposed.
- Identify the activities provided in the **CPM** for which the **Crime Prevention Officer** is responsible in compliance with the Model supervision requirement of his/her role.
- Fully comply with the requirements demanded by the Legislation (**UK Bribery Act, Chilean Law 20.393** and other applicable anti-corruption laws).

III. Scope

The **Manual** and the **CPM** are applicable to all those who work for or provide services to the Antofagasta plc group of companies, hereinafter all or any of them indistinctly also referred to as the "Company". The scope also includes shareholders, directors, senior management, managers, executive officers, employees, temporary staff, contractors and consultants of the Company.

The Company expects an **upright, strict and diligent behaviour from all the persons identified above in compliance with the anti-corruption related legislation**, specifically regarding the crimes included in the aforementioned laws (**Law 20.393, UK Bribery Act** or similar ones), together with the prevention and mitigation measures of these set out by the Company.

IV. General Definitions

Management of the Legal Entity: Pursuant to Article 4° of **Law 20.393**, the Management of the Legal Entity is the top management authority which, in the case of the companies that are part of the Antofagasta Group, is its Board of Directors.

Associated Persons: It means any natural or legal person with whom the Company currently has — or is in process of potentially negotiating in the future — a commercial or services relationship. This includes Contractors, Subcontractors, Advisors, Agents or any third party who, due to their role or business relationship with the Company, their behaviour or acts may possibly constitute an offence included in the Regulation.

Legislation: UK Bribery Act, Chilean Law 20.393 and other applicable anti-corruption laws.

Basic offences of Law 20.393: Offences that may result in the criminal liability of legal persons and compromise the liability of the Antofagasta Group and its associated companies, when committed in the direct and immediate interest or benefit of a company or business pertaining to the Group.

To date, the following crimes are covered:

1. **Bribery or corruption:** It is understood as offering, giving or agreeing to give any benefit (economic or otherwise) to a national or foreign public officer, due to the position held, to which this person is not entitled, or for him/her to do or not to do something, within or outside the scope of his/her position, competence and responsibilities.

2. **Commercial bribery:** All acts by which an employee or agent of a private legal entity requests or accepts an economic or other benefit for himself/herself or a third party in exchange for favouring or having favoured one bidder over another when exercising his/her duties. Also punishable is anyone who gives, offers or agrees to give such benefits to an employee or an agent, but for his/her own benefit.

3. **Misappropriation of Assets:** Appropriating or distracting, to the detriment of another, money, items or any other movable thing received in deposit, commission, administration or otherwise, that produces the obligation to deliver or return it.

4. **Disloyal administration:** It occurs when someone tasked with safeguarding or managing the estate of another person, causes harm to that person either by abusively using powers or by performing or omitting another action manifestly contrary to the owner of the estate.

5. **Incompatible negotiation:** It occurs when a person, who for a legal reason administers other persons´ assets (directors or managers, arbitrators, liquidators, experts or guardians, among others), has a vested interest in any negotiation, activity, contract, operation or management in which he/she must have been involved due to the position being held.

6. **Money Laundering:** Any act intended to hide or conceal the unlawful origin of goods, or to acquire, hold or use the assets, knowing that they stem from committing an illegal act involving drug trafficking, terrorism, weapons sales, promotion of child prostitution, kidnapping, bribery, misappropriation, unfair administration, stock market, bank financing and others, with the intention to profit from, sell, contribute to a company or any other purpose, and knowing their illicit or illegal origin at the time of receiving the good.

7. **Terrorism Financing:** When a natural or legal person by any means, whether direct or indirect, requests, collects and/or delivers any kind of contribution with the purpose of using it to expedite any act of terrorism, either with a contribution in kind or cash or collaborating in any other way with activities that qualify as terrorist ones.

8. **Possession of stolen goods:** When a person who, knowingly or negligently, possesses, sells or trades any stolen or misappropriated goods or products, even when such items have already been sold.

9. **Water pollution:** When a person discharges or causes to be discharged (without authorisation or in contravention of its conditions or in breach of applicable law) chemical, biological or physical pollutants into the sea, rivers, lakes or any other body of water, negatively impacting hydro-biological resources.

10. **Violation of product bans:** It refers to the processing, stockpiling, transforming, transporting, commercialising and/or storing banned hydro-biological resources, as well as to developing, trading and storing products derived therefrom.

11. **Illegal fishing of seabed resources:** It occurs when fishing is conducted in areas of management and exploitation of benthic resources without being the holder of the rights required by law.

12. **Illegal processing and storage of scarce products:** Processing, elaborating or storing hydrobiological resources in a state of collapse or overexploitation or products derived from these, without proof of their legal origin.

13. **Failure to comply with preventive measures taken by the sanitary authority in case of an epidemic or pandemic:** Whoever, knowingly and having authority to command the work of a subordinate, orders this worker to go to a work performance place different from the address or home of this person, who is in quarantine or compulsory sanitary isolation decreed by the health authority.

14. **Arms control offences:** All the offences contained in Title II of Law N° 17.798 on Arms Control may generate the criminal liability of a legal person. Among them, by way of example, are those crimes that punish those who organise, belong to, finance, provide, assist, instruct, or incite the creation and operation of private militias, combat groups or militarily organised groups; the carrying, possession or holding of firearms or explosives without the appropriate authorisations or registrations; etc.

15. **Human trafficking:** Recruiting, transferring, harbouring or receiving people to be subject to any form of sexual exploitation, forced labour, servitude or slavery or organ removal (Article 411 *quater* of the Criminal Code).

16. **Cybercrime** (Law 21.459): It includes eight forms, namely:

a) Attack on the integrity of a computer system (Article 1°): An offence punishing anyone who prevents or obstructs the normal operation of a computer system.

b) Illegal access (Article 2°): An offence punishing anyone who unlawfully accesses a computer system.

c) Illegal interception (Article 3°): An offence punishing anyone who intercepts, interrupts or interferes with the non-public transmission of information in a computer system and anyone who, without authorisation, collects data contained in computer systems.

d) Attack on the integrity of computer data (Article 4°): An offence punishing anyone who unduly alters, damages or deletes computer data, provided that this causes serious damage to the holder of such data.

e) Computer-related forgery (Article 5°): An offence punishing anyone who unduly introduces, alters, damages or deletes computer data with the intention that they be taken as authentic or used to produce authentic documents.

f) Receiving illegally obtained computer data (Article 6°): An offence punishing anyone who trades in illegally obtained databases.

g) Computer-related fraud (Article 7°): An offence punishing anyone who manipulates a computer system to obtain benefit or that causes harm to another person.

h) Abuse of devices (Article 8°): An offence punishing anyone who facilitates the fraudulent use of credit or debit cards through programmes, devices or other elements produced or adapted primarily for the commission of such offences.

17. Robbery or theft of timber (Article 448 *septies* of the Criminal Code): An offence penalising anyone who steals or takes without permission logs or pieces of wood.

18. Possession of timber without proving its legal origin. (Article 448 *octies* of the Criminal Code): An offence punishing as a perpetrator of theft anyone who is found with logs or pieces of wood and cannot justify their acquisition, tenure or work in tasks related to felling trees, and anyone who is found in other people's property in identical tasks or activities, without the consent of its owner or logging authorisation, and also anyone who forges or maliciously uses documents to obtain guides or forms to illegally transport or trade in wood.

All references to Law N°20.393 made in this Manual include the above offences, as well as all future amendments to the law, including but not limited to modifying current criminal offences, establishing new criminal offences, modifying the level of charges to restrict or expand criminal liability, among others.

V. Crime Prevention Model (CPM)

The Company's Crime Prevention Manual consists of a set of measures to prevent, detect and remedy the Crimes of **Law 20.393**, which are applied through the various activities of the **CPM** and that are included herein. These activities are intended to comply with the requirements of a **"Crime prevention system"** and to implement **"Policies and procedures",** as required by the Regulations. This Manual also establishes the risk identification activities, risk controls and suitable monitoring and reportability mechanisms for preventing, detecting and mitigating the risks associated with the above offences.

All the executive officers, employees and external staff of the Company are committed to complying with the laws and regulations in force in the countries where it operates. Therefore, the Company will not tolerate any kind of corruption, and it is expressly prohibited to commit any illegal act, such as the offences included in the abovementioned legislation (**Law 20.393, UK Bribery Act** or other similar law). Consequently, the Company shall:

1.Ensure the fulfilment of its duty to manage and oversee by properly operating the **CPM**.

2. Appoint a **Crime Prevention Officer**, who will hold the position for three years and may be re-elected for equal periods while holding this position.

The implementation and fulfilment of the activities provided in this **CPM** shall be the responsibility of each Company of the Antofagasta Group, and their effectiveness will be reported to each of their Board of Directors by the **Crime Prevention Officer.**

The Company's **CPM** is developed through a series of activities included in the Compliance Model as shown in the chart below:

A. Crime Prevention Officer

Law 20.393 requires the appointment of a **Crime Prevention Officer** (hereinafter, **CPO**). The Board of Directors has full powers to appoint the **CPO** for a three-year term, and must record its decisions in the respective minutes of the Board of Directors of Antofagasta plc.

The Boards of Directors of Antofagasta plc and of the Companies have appointed their respective **Crime Prevention Officers**, whose names and date of last appointment are included in the document entitled "Crime Prevention Officers" available on the Company's intranet.

The **CPO** is responsible for setting up a crime prevention system through a **CPM**, together with the Company's top management, that is to say, its Board of Directors.

Role of the Crime Prevention Officer:

Through his/her performance, the **CPO** represents the Company's values. In addition, the **CPO** has full knowledge of:

- The roles and individuals responsible for each area of the Company.
- The legislation and regulations in place by the legitimate and competent regulatory authorities.
- The Code of Ethics, Procedure Manuals, Regulations and other internal instructions of the Company.

Means and Powers of the CPO:

1. When performing his/her role, the **CPO** has autonomy in relation to the management team of the Company to which he/she was appointed, its shareholders and controllers, and has direct access to the respective Board of Directors.

2. The **CPO** has available an annual budget (means provided by the Chief Executive Officer or General Manager and approved by the Board of Directors) and has a support staff to implement, operate and review the **CPM** in compliance with the Law.

3. The **CPO** has the basic and necessary tools to properly perform the role and responsibilities pertaining to this position.

The **CPO** has direct and unrestricted access to the various areas of the organisation, in order to carry out the following activities:

i) Conduct specific investigations.

ii) Facilitate the monitoring of the crime prevention system.

iii) Request and review information for performing his/her duties.

Responsibilities of the CPO:

1. Ensure the proper development, implementation and operation of the **CPM** in the Company.

2. Coordinate compliance by the various areas and management of the Companies with the laws and regulations to prevent the crimes mentioned herein.

3. Ensure that all persons belonging to the Companies receive and comply with the **Code of Ethics** to prevent any misconduct in the daily activities of the employees and service providers. This may be checked by ascertaining the training the Company must regularly provide to its employees on these matters and by reviewing the reports of complaints regarding irregularities or breaches of the **Code of Ethics**.

4. Report to the respective Board of Directors on the status of the **CPM** and matters within the **CPO's** competence and management, on a biannual basis. In addition, opportunely report to the Board of Directors on any situation it should be aware of, and which could be classified as an offence, so that the latter may adopt the necessary measures.

5. Promote, together with the Board of Directors, the design and necessary updates to the policies, procedures, instructions and guidelines, including this **Manual**, so that the **CPM** can be operated effectively and/or whenever necessary, pursuant to any changes made to the country's laws and regulations.

6. Ensure knowledge of and compliance with the established protocols, policies, procedures, instructions and guidelines as elements of crime prevention in the daily actions of the employees and associates of the organisation.

7. Lead investigations when there is a valid complaint or a suspicious situation that warrants it, collecting and analysing any necessary evidence.

8. Define specific reviews to check compliance with the activities of the **CPM**. In addition, define their scope and extent. The results of the completed reviews must be reported to the applicable Board of Directors or Board Committee.

9. Check the design and implement the **CPM** training programmes focusing on the members of the organisation.

10. In conjunction with the Board of Directors, be responsible for identifying and analysing the risks of offences in relation to the implementation of control activities for preventing and mitigating such risks and properly operating the **CPM**.

11. Keep an updated list of the activities that may represent, by the way they are carried out or their own characteristics, a risk of committing the offences envisaged in the aforementioned regulations (**Law 20.393, UK Bribery Act** or other similar law). The list identifying such activities is contained in the "Risk Matrix", which is an integral part of the Model.

12. Encourage effective crime risk prevention controls over the Companies' internal processes and activities and keep adequate records of evidence of compliance and enforcement of these controls.

13. Document and safeguard evidence related to crime prevention activities.

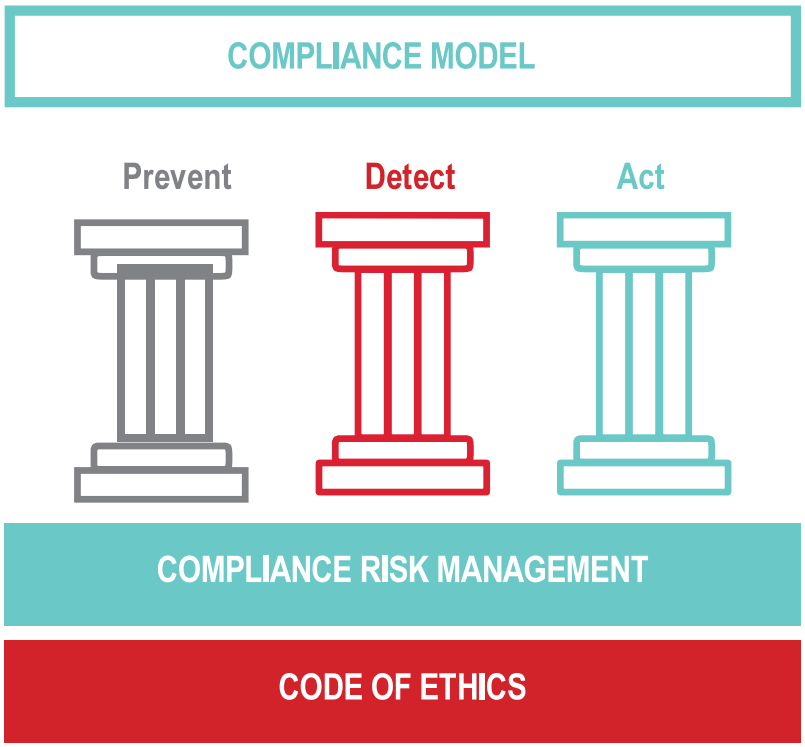
14. Receive any complaint filed for failure to comply with the **CPM** or because an unlawful act has been committed, filed by any of its owners, individuals in charge, directors, senior management, executive officers, employees, dependents, contractors and business-related third parties.

15. Be a standing member of the **Ethics Committee** of the respective Company and have access to all complaints made regarding Anti-Corruption Rules.

Notwithstanding the foregoing, the **CPO** may act directly or through the staff under his/her charge or through any assigned person to delegate part of his/her activities.

B. Components of the Crime Prevention Model

The Company's **CPM** is implemented through the activities provided for in the Group's **Compliance Model.** This model, in turn, is based on the **Code of Ethics** and compliance risk analysis. It consists of three key pillars: **Prevent, Detect and Act.**



I. THE CODE OF ETHICS IS OUR FOUNDATION

The **Code of Ethics** sets out a behavioural framework for the business's daily challenges **based on transparency, integrity, compliance with applicable laws and good business decisions**. In this respect, it provides a control environment for the activities that could expose the Company to legal or criminal liability.

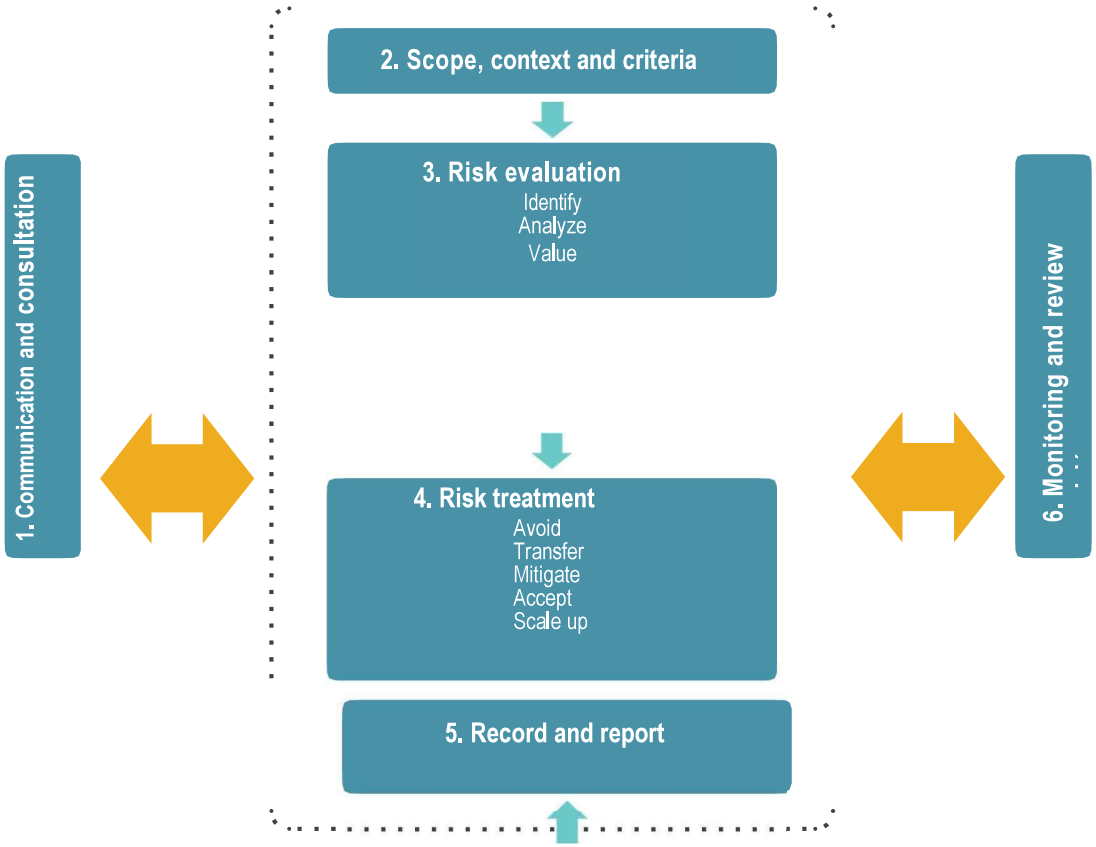
The Company demands from all its executive officers, supervisors, employees and contractors **an upright, strict and diligent behaviour** in compliance with the Prevention Model, with all of them having to commit to the strictest adherence to it.

The **Code of Ethics** is the basis for defining and implementing the main activities of the **CPM.**

II. COMPLIANCE RISK MANAGEMENT

In conjunction with the Board of Directors, the **CPO** is responsible for the process of identifying and assessing the potential crime risks to which the Company is exposed. As a result of this process, risk identification, controls and action plans related to crimes must be developed and reviewed annually or when significant changes occur in business conditions.

To carry out this activity, and in accordance with the Risk Management Manual in force in the Company, the activities shown below must be considered:



1. Communication and consultation

Communication seeks to promote risk awareness and understanding, while consultation involves obtaining feedback and information. Both activities facilitate the timely exchange of information required for a robust analysis, as well as the involvement of key **stakeholders** at each stage.

2. Scope, context and criteria

For a robust risk analysis and its updates, it is critical that there is a common view about the operating context of the Company or specific departments, the criteria considered for the assessment and the scope of the analysis.

3. Risk assessment

This stage consists of three main steps: **Identify, Analyse and Value.** Risk assessment should involve key people who have knowledge of or are related to the risks to be discussed and who have the authority to make decisions on risk management strategies.

i) **Identify:** This should be done using a "top-down" approach through working meetings with the involvement of all key people. A list is developed of the main risk scenarios for the commission of offences within the scope of the Law, committed in the interest or direct and immediate benefit of the Company and carried out by the owners, directors, individuals in charge, main executive officers or those engaged in management and supervisory activities, as well as by workers under the direct management or supervision of any of the aforementioned individuals.

ii) **Analyse:** The current state of risk must be defined, considering the organisation's preventive and mitigating controls and considering their implementation and effectiveness. This makes it possible to determine the residual risk level according to the Probability and Impact tables defined in the Comprehensive Risk Management Manual. Controls identified at this stage should be currently in place and effectively reduce the probability or impact of a risk.

iii) **Value:** Based on the outcome of the analysis stage, that is, the current state of risks and their existing controls, risks are prioritised in order to identify the most exposed areas or operating processes. This enables focusing the **CPO's** resources and efforts to identify which risks require additional action plans, so that their level remains within tolerable limits for the organisation.

4. Risk treatment

For prioritised risks or those that present exposure outside the tolerance limits defined by the organisation, action plans must be developed aimed at reducing the likelihood or impact of risk. Each action plan must have an assessment of the risk level reduction once the plan is implemented and, should it be approved, a person in charge, a schedule and a budget for its execution.

5. Record and report

The entire compliance risk management process must be documented to support decisions and assist in their management.

6. Monitoring and review

The purpose of the monitoring and review stage is to:

- Ensure the quality and effectiveness of the defined critical controls, allowing to conclude whether the control:
- Reasonably prevents or mitigates the risk of crime.
- Does not reasonably prevent nor mitigate the risk of crime.
- Monitor progress of the execution of action plans.
- Investigate materialised or "near-materialised" risks.

III. THE THREE MANAGEMENT PILLARS OF THE CRIME PREVENTION MODEL

Pillar 1: Prevent

Prevention is one of the main focuses of the CPO and the Company has a series of regulations, tools and activities that support the prevention of crimes in the organisation. Among these are:

1. Policies and procedures

All policies and procedures that establish definitions, regulations, and controls for the Company's activities must be duly documented, disseminated, and available to all personnel involved in these processes.

2. Internal Instruction on Order, Hygiene and Safety

In compliance with the Legislation, the Company's Internal Instruction on Order, Hygiene and Safety must incorporate the internal obligations, prohibitions and sanctions in case of non-compliance with the terms of this **Manual**.

3. Anti-corruption legislation

All persons acting on behalf of the Company must refrain from offering, promising or agreeing to give a public or private employee, whether Chilean or foreign, an economic or other benefit under any pretext or circumstance and by any means. Likewise, workers must always take care that the money or property of the Company or the celebration of acts and contracts are used in no case for illegal purposes or constituting a crime contemplated in the Legislation.

Workers must always be alert to any situation that seems suspicious and which could lead to or facilitate the commission of any of the crimes indicated above, and report it immediately through the Company's whistleblowing channel:

- **Internet/Intranet**: https://tuvoz.aminerals.cl
- **Telephone: 800-362- 672 (Chile)**
- **Email: tuvoz@aminerals.cl**

4. Due Diligence

Relationship with third-parties

The Due Diligence process carried out on the Company's potential business partners, whether for the purposes of a strategic alliance, joint venture or co-branding, not only considers commercial and financial aspects, but also analyses all the information necessary to detect the external company's possible connection with any of the crimes established in **Law 20.393** and the **UK Bribery Act**.

Relationship with contractors and suppliers/associates

The selection of contractors/suppliers (hereinafter, "Associates") of the Company must incorporate a Due Diligence process that contemplates the following matters whenever applicable: background check on the partners or owners of the company; verification of suspicious situations in relation to the Associate, such as prices of products or services well below the market price; if a foreign company, obtaining information on the risk of corruption of the Associate's country of origin; checking possible conflicts of interest of Company employees with the contractor or supplier due to commercial or kinship ties; incorporation of the Due Diligence form into the necessary papers for tenders; and maintaining a database of Associates whose evaluation has been rejected.

5. Contract clauses

In compliance with the Laws, all work contracts for employees and associates must have clauses, obligations and prohibitions relating to this legislation.

Compliance with this requirement is the responsibility of the Human Resources and Contracts areas, as appropriate, and must be periodically reviewed by the **CPO**.

Exceptionally, modifications to the clauses may be made as long as they have the approval of the Corporate Risk and Compliance Area.

6. Conflict of interest declaration

When joining the Company as a worker, people must sign a **conflict of interest declaration** and specify if they have any Conflict in accordance with the provisions of the Company's **Code of Ethics** and the **Conflict of Interest Guideline.** This must be reviewed and updated each time a conflict is identified after the original Declaration is made. The Company has arranged a system to make and update the **conflict of interest declaration**, which is available on the Company's Intranet and website.

Likewise, every director, executive officer, supervisor, employee and associate of the Company who - for business reasons or not - is related to **Politically Exposed Persons (PEP)**; or who, in their relationship with public employees or private sector companies, national or foreign, has or believes they have a conflict of interest, is obliged to report conflict situations, through the same **conflict of interest declaration**, available in the individualised System, or through the form provided for associates.

In the case of associates, every time a contract is renewed or tendered, all contractors or suppliers must sign the **conflict of interest declaration** in accordance with the provisions of the **Conflict of Interest Guideline** and the Declaration of Non-Granting of Undue Benefits to directors, executive officers or employees of the Company.

7. Guidelines for gifts, invitations and other benefits

Company employees may not offer, give or receive gifts, invitations or benefits when:

- The amount is over $150.
- Are established regularly or periodically with the same person or institution.
- The invitations are obviously "disproportionate" (whether in time, cost or other).
- The Company is in a process of negotiation/bidding, obtaining a permit or authorisation of a key right or licence.
- They constitute benefits or advantages that cannot be evaluated in money but may compromise the independence or impartiality of the person who receives them.
- **It is strictly prohibited to offer, give or receive money.**

For more information, see the Guidelines for Gifts and Invitations.

8. Communication and training

The Company is responsible for informing all its employees and associates of the existence and content of the Model and the scope of the Laws.

In addition, and for this policy to be integrated into the daily work of each member of the Company, regular training must be carried out for its members to transmit the minimum necessary knowledge on the subject and the application of its procedures.

The training must include, as a minimum, the following contents:

- Definition of the crimes considered in the Laws.
- Company policies on the Prevention Model.
- Brief presentation on the content of the Prevention Manual.
- Tools and mechanisms used to implement the Model and the **Code of Ethics**.
- Examples of risk situations for the commission of these crimes.
- Established whistleblowing channels.
- Internal rules and instructions.
- Obligation to report.
- Disciplinary consequences, as well as legal (civil, criminal, administrative) of non-compliance with internal and external regulations, in matters of crimes contemplated in the aforementioned Laws.
- Responsibility of each employee regarding this matter.

All Company employees must participate in the training provided by the Company for these purposes.

Pillar 2: Detect

The **CPO** has tools to **detect** any irregularity in relation to the crimes contained in the Laws. It is the responsibility of all employees and associates of the Group to support the detection process, reporting all the relevant information, and in a timely manner, on irregularities witnessed or of which they were aware.

1. Whistleblowing channel and investigation

The whistleblowing channel is a system implemented in the organisation, available through the Intranet, Internet, email and telephone (800 line), which is intended to be a mechanism for the submission of any complaint related to an irregularity or breach of internal policies, irregular conduct, transgression of the **Code of Ethics**, breach of the **CPM** or the possible commission of any illegal act indicated in the Laws. The **CPO** must carry out an analysis of the complaints received, through the different channels provided by the organisation, to identify those that have implications on the **CPM** or that are associated with the crimes covered by the Laws.

The **CPO** must oversee the coordination of the investigations derived from the complaints that have implications for the **CPM** or that are associated with crimes covered by the Laws.

The treatment of the complaints and the coordination of the investigation of the complaints are carried out in accordance with the provisions of the Methodology for the Review and Communication of Complaints.

2. Analysis of information and reviews

The **CPO** coordinates, directly, or through his/her personnel in charge, with the organisation's different areas and departments, the review of sensitive data and the updating of information from third parties, including suppliers and contractors, that allow any irregularity in relation to the **CPM** and the Laws to be detected.

The internal control and internal audit areas must act in the event that any irregularity is detected in relation to the Laws or the **CPM**.

Pillar 3: Act

1. Response activities

The objective is to carry out the investigation, establish resolutions, corrective actions, disciplinary measures or sanctions for those who fail to comply with the **CPM**, or when indicators of the crimes covered by the Laws are detected. As part of the response activities, the review of breached control activities should be considered, in order to strengthen control activities or replace them with new ones.

In the event that a crime that violates the Laws is verified, the response activities of the **CPM** are the following:

- Communicate sanctions and control improvements.
- Coordinate disciplinary sanctions.
- Record and monitor cases and sanctions.
- Report to criminal justice system, as appropriate.

C. Monitoring and review of the CPM

Through monitoring, the **CPO** (or whoever he/she designates) must periodically verify that the **CPM** operates as designed.

To carry out monitoring activities, the **CPO** can request support from other areas of the organisation, such as Internal Audit (or outsource this activity), Accounting, among others, as long as said areas are not involved in the activity to be reviewed.

The **CPO** may perform the following monitoring activities:

- Review the supporting documentation of the tests carried out by the support areas.
- Verify control activities (through sampling).
- Analyse the reasonableness of transactions.
- Verify compliance with the restrictions established in the procedures.
- Other activities.

In those monitoring activities where it is required to determine a sample, the **CPO** must determine and document the criteria to be used.

Review Plan

The **CPO** must establish a Review Plan, which considers the verification of the effective operation of the implemented controls, mitigation of the risk of committing the established crimes and effective operation of the **CPM** in accordance with the provisions of the applicable regulations. This Plan must define the number of necessary revisions, matters that are going to be verified, and frequency and controls of these, etc.

All operations that have given rise to an investigation for the possible commission of some of the crimes identified in this Manual must be registered. This record must be kept for a minimum period of five (5) years.

According to **Art. 4, literal (b) of Law 20.393**, the Company can certify the **Crime Prevention Model**, according to the requirements established in the same regulations and in relation to the situation, size, business, revenue level and complexity of the Company.

VI. Higher Risk Business Activities

1. DONATIONS

The following obligations are an integral part of the procedure that regulates donations in the Company:

- Establish the chain of authorisation to make donations.
- Ensure that the entity receiving the donation has the proper accreditations (legal validity, constitution, legal representatives, etc.)
- Verify the entity in the "**Registry of Institutions Receiving Donations**" - Law 19.885.
- Identify the work carried out in society by the institution receiving the donation.
- Establish the objective and use of the resources donated by the Company.
- Monetary donations must be reported to the **Crime Prevention Officers** of each company for registration and approval before being made.

2. SPONSORSHIPS

A record must be kept with the physical evidence of the contributions made to sponsor events, which must include an identification of the recipient or beneficiary of said sponsorship and the purpose of the benefit. Additionally, the authorisation process must be registered of the company that applies for the sponsorship, including detailed information regarding the application for the sponsorship (if there is one).

3. EXPENSE ACCOUNTS, REIMBURSEMENT OF EXPENSES AND CREDIT CARD USE

In order to aid compliance with the duties of executive officers and some employees, the Company advances funds, reimburses expenses already incurred and provides credit cards.

The procedure considers completing forms associated with expense accounts, indicating the detail of expenses, with the respective associated endorsements. The forms must have the signature of the applicant and the approval of the direct supervisor. Finally, they must be sent to the accounting area.

These funds cannot be used to make invitations to public officials, representation expenses, or for other purposes other than those indicated in the preceding paragraph. More details can be found in the procedure "Expense accounts, **reimbursing expenses and credit card expenses**".

4. EMPLOYEE AND THIRD-PARTY TRAVEL

Only travel expenses related to: transport, accommodation, food, transfers, use of laundry, use of telephone, vehicle rental expenses, representation expenses, that are actually paid and have original supporting documents or invoices, will be reimbursed.

In very exceptional cases, and in jurisdictions with very informal economies ("cash only"), in which it is not possible to obtain a document that supports the transaction, it must be described in detail and discussed with the respective VP, Area Manager or General Manager, who must evaluate its approval.

The Company will not be responsible for disbursements that are not directly related to the purpose of the business trip. These disbursements will be the responsibility of the worker.

The Group will not reimburse expenses that go against its values. Likewise, it is prohibited to accept trips paid for by current or potential customers, suppliers or contractors of the Company.

5. MERGERS OR ACQUISITIONS

The Mergers or Acquisitions process must necessarily contemplate Due Diligence with the analysis of all the information that it is possible to collect on the participation of the company that it is intended to acquire, or with which there is an interest in merging, in the crimes covered by the Laws.

6. PERMITTING PROCESS AND MEETINGS WITH THE AUTHORITIES

As part of the Company's ordinary operations, it is necessary to obtain a series of sectorial or other permits for the purposes that the business requires. It is also necessary to have meetings with authorities or public officials. Communications with authorities or public officials through emails must be made using the institutional email addresses of both our Company and the institution to which the official or authority belongs. Face-to-face meetings with authorities or officials must be scheduled in advance and subject to an established agenda.

In case of any perceived anomaly in this process, or of non-compliance with it, the **Crime Prevention Officer** must be notified.

7. PROCUREMENT OF SERVICES AND SUPPLY OF GOODS

The Company is governed by the highest ethical standards. Thus, it requires its suppliers of goods or services to strictly comply with all laws and regulations that apply to their business processes. For this purpose, its analysis covers the review of the background of participants, the application of the Due Diligence questionnaire, the **Conflict of Interest** form (internal and external) and the screening of suppliers, among others. When contracting services and the supply of goods, there is greater exposure to the crimes of incompatible negotiation and bribery between private parties, so it is the obligation of each Group worker to actively manage their potential **Conflicts of Interest**, keep their declaration updated and strictly follow the guidelines of the supply area.

8. SURPLUS DISPOSAL

The disposal of surpluses is generated from equipment, tools, materials, supplies and other items that a company declares expendable, because they are no longer necessary or are no longer useful for the main activity of the business. These surpluses are classified as: derecognised fixed assets, obsolete stock materials, project surpluses and other surpluses (scrap or obsolete materials from the production process).

Generally, this surplus is valued with a provision for obsolescence or write-off which must be reversed at the time of disposal.

For the disposal of surpluses, the Company must comply with the following activities: declaration of non-essential assets by the business area; disposal process, and accounting of the activity, in accordance with the Group's accounting policies.

9. PURCHASES AND LEASES OF ASSETS

In the purchase and lease of assets, the exposure to the crime of "reception" is greater, understood as carrying out a transaction or the trading of stolen assets.

Thus, it is required to ensure the origin of the asset to be purchased or leased.

As a basic rule, it is suggested to take the following into account when purchasing or leasing assets:

- Do not buy or lease products with an unknown or suspicious origin.
- When buying or leasing an asset, always demand the product's Declaration of Origin, Certificate of Origin or another document that supports the legitimate origin of the assets.
- **Always demand a receipt or invoice when buying or leasing. In the case of purchases, demand the guarantee of the product.**

(*) This list is not exhaustive and is not expected to cover all higher-risk business activities.

VII. Non-Compliance Reporting Procedure

1. General framework

The Company expects that, in the performance of their duties, employees and associates always act in accordance with the principle of **good faith**, which requires, among other aspects, **constantly maintaining a positive attitude of collaboration towards the organisation.** These principles of conduct and values are consistent with those established in our **Code of Ethics.** As part of a tool for compliance with the aforementioned, the Company has designed and implemented a whistleblowing channel so that employees and associates of the organisation can manifest, communicate or denounce the irregularities that they detect in the performance of their work.

In the same way, the organisation expects its employees and associates to take responsible measures to prevent a breach of the Crime Prevention Model, in order to seek guidance and raise situations in time to prevent them from becoming problems.

If any doubts or suspicions are held regarding a possible violation of laws, this policy or other company policies, any employee or associate of the Company can communicate this situation through the formal channel to make this kind of report, available on the Intranet or the Internet.

2. Whistleblowing or irregularities reporting channels

The Company has the following channels to make complaints or report irregularities:

- **Intranet/Internet:** https://tuvoz.aminerals.cl
- **Telephone: 800-362-672 (Chile)**
- **Email:** tuvoz@aminerals.cl

3. Whistleblowing

Company employees and associates can raise in a preventive manner, and through the indicated channels, those situations that could involve a possible violation of laws, of this policy or other company policies. However, they must report in said system, suspected violations of laws in Chile or the country in which the company operates, or violations of the Company's policies, rules and procedures, and that consider knowledge or suspicion of the involvement or connection of any Group Company, employee, supplier, associate or third party in any of the crimes indicated in the Laws.

Those complaints that are related to the crimes stipulated in the Laws must be referred to the **Crime Prevention Officer**.

4. Management of complaints or reports

The **CPO** is responsible for the proper and timely handling of the complaints or reports received and that are related to the crimes stipulated in the Laws, and ensures that the necessary measures are taken in response to such complaints or reports.

Complaints made about non-compliance with the **CPM** must consider the following:

- The complainant must describe in the most detail possible the situation in which the transaction or operation that gave rise to the complaint was known. It must include the grounds on which the indications of this possible operation or unusual or suspicious situation are based.
- In the case of a beneficiary of the transaction, indicate their personal information.
- The communication should contain as much information as possible about the suspect or those involved.
- The **CPO** keeps a confidential file with all the information received and which can only be accessed by those persons who, due to their position, must intervene in some way in the investigation of the complaint and only with respect to the information essential for said intervention.

5. Confidentiality of the complaint

All complaints are kept strictly confidential and, therefore, should only be known by the recipient of the complaint and by the **Crime Prevention Officer**, or by the persons who must intervene in the investigation process.

6. Guaranteed anonymity and non-retaliation policy

The Group's whistleblowing channel allows anonymous reporting, in line with the best international reporting practices, which show that most whistleblowers prefer to remain anonymous.

Similarly, the Group ensures a policy of **non-retaliation** against people who make complaints in good faith. Any action contrary to this guideline must be reported to the **CPO**.

7. Reporting to the criminal justice system

Upon detection of an act with characteristics of a crime, the CPO must evaluate, in conjunction with the Company's Legal Advisor and the Board of Directors, whether to report such acts before the Courts of Justice, the Public Ministry or the Police. This action is specified as a mitigating circumstance of criminal liability for the legal entity in **Article 6 of Law 20.393**, which details:

"It shall be understood, in particular, that the legal entity collaborates substantially when, at any stage of the investigation or judicial proceeding, its legal representatives, prior to knowing of the judicial proceeding directed against it, have brought the punishable act to the attention of the authorities or provided background information to establish the facts investigated."

VIII. Administrative sanctions

All Company employees must know the content of the **Crime Prevention Model** and must abide by its guidelines at all times. The **CPO** monitors compliance with this **Manual** and implements verification programmes.

Failure to comply with the terms of this Manual by employees will be penalised in accordance with the provisions of the Company's respective Internal Regulation of Hygiene, Order and Safety of the Company.

In the case of advisors, contractors or suppliers, failure to comply with the terms of this Manual is considered a serious breach of contract and will give the Company the rights established in the contracts in force.

Employees must report violations observed in the **Crime Prevention Model** to their supervisors or the **CPO**, or through the established reporting mechanisms.

Company employees should be aware that they could be subject to internal investigations if there is any indication, or a complaint is received that relates to a breach of any law or internal regulation of the company within the Law. Employees must provide their full collaboration in internal investigation procedures carried out within the framework of the **CPM**.

The policies and procedures indicated in this **Manual**, in the **Code of Ethics** and in the other documents that support the Model are mandatory and are incorporated into the functions and responsibilities assigned to each employee.

The same obligation of collaboration is required of the advisors, contractors and suppliers of the Company, which is recorded in the respective contracts or agreements that are signed in this regard.

RECEPTION CONFIRMATION

I do hereby declare that I have received a copy of the Crime Prevention Manual that defines the various prevention, detection, and mitigation activities of the potential risks of committing crimes to which the companies that are part of Antofagasta Plc are exposed. I assume the duty to comply with the obligation to read and know in detail the content of this Manual and apply it in the performance of all my work functions. Additionally, I understand that it is my duty to report any irregularity in relation to the conduct and obligations contained in this Crime Prevention Manual.

By virtue of the foregoing, I put on record that the Group has informed me about the scope of the regulations contained therein and the effects derived from its eventual non-compliance.

Name
ID number
Position
Department
Company
Date
Signature

Whistleblowing channels

The Company has the following channels to report irregularities:

- **Intranet/Internet:** https://tuvoz.aminerals.cl
- **Telephone: 800-362-672 (Chile)**
- **Email:** tuvoz@aminerals.cl

This Crime Prevention Manual was approved in 2019.
In 2021, types of penalties and information on the whistleblowing channel were updated.
In 2023, the scope of crimes will be updated.

Crime
Prevention Manual

Antofagasta Plc
Ley 20.393 and **UK Bribery Act**
May 2019

Risks and Compliance Department
Vice Presidency of Administration and Finance

ANTOFAGASTA PLC