



# COMPLIANCE PROGRAM AND CORPORATE BEST PRACTICES

Prevention of Corporate Liability Related to Antitrust Matters and Criminal  
Liability of Legal Entities

 **saam**  
TERMINALS

## 1. INTRODUCTION

This document, "Compliance Program and Corporate Best Practices," explains the main aspects of the system to prevent corporate liability related to antitrust matters and criminal liability of legal entities (indistinctly and hereinafter, the "Compliance Program" or the "Program"), which is part of the Comprehensive Ethics and Compliance Management System. The Program's content must be known and applied by all employees, executives and directors of SAAM Puertos S.A., SAAM Ports S.A., and their respective subsidiaries (all hereinafter jointly "SAAM Terminals" or the "Company"). In addition, the Company must ensure that third parties with whom it engages, such as strategic partners, business partners, suppliers, contractors and customers, among others, are aware of and respect the Compliance Program, to the extent it is applicable to them.

The Program calls for risk matrices prepared based on a risk assessment of the processes and activities we carry out, in terms of both criminal liability and antitrust matters, in order to provide prevention measures and mitigating controls for such risks; a program for disseminating best practices, controls, policies and procedures; and a training program based on our risk scenarios. It is also supported by other ethics and compliance management tools, such as the Corporate Code of Ethics, the Whistleblower System and its respective Complaint Management Procedure, as well as by the Ethics Committee. Likewise, the Program calls for the appointment of a Compliance Officer, who will be responsible for managing risks in criminal and antitrust matters. The Compliance Officer's duties include keeping the Program up to date and ensuring compliance with the ethical practices and measures to prevent the conduct described below.

This Compliance Program has been designed based on the applicable regulations (i.e., Law No. 20,393 ("Law No. 20,393"), on criminal liability for legal entities and its amendments incorporated by Law No. 21,121, of November 2018, Law No. 21.132, of January 31, 2019 and Law No. 21,249, of June 2020, Law No. 21,325, Law No. 21,412 and Law No. 21,459 on computer crimes; as well as from the criteria defined by the Antitrust Court ("TDLC" in Spanish) and the Supreme Court, through its jurisprudence, for the creation of an antitrust program that complies with Decree with Force of Law No. 1 of 2005 of the Ministry of Economy, Development and Tourism, which establishes the consolidated, coordinated and systematized text of Decree Law No. 211 of 1973 ("DL No. 211")).

The Program's main objective is prevention, focusing on measures to prevent the Company's organizational structure from being used to commit any of the crimes in Law No. 20,393 or the infractions set forth in DL No. 211.

SAAM TERMINALS expects everyone at the Company to behave properly and diligently and to adhere to the desirable ethical conduct and measures established in the Compliance Program, as well as in other company documents, such as the Code of Ethics, the Internal Order, Hygiene and Safety Rules, the Best Practice Guide for Relations with Public Officials and/or PEP, Community Contributions, Gifts, Invitations and Hospitality; the Best Practice Guide for Managing Antitrust Compliance; and any other complementary internal rules that may be in force. Likewise, the clauses regarding Program obligations and compliance are expressly incorporated in employment and service contracts.

## 2. OBJECTIVE

The Compliance Program's objectives are to:



Strengthen and consolidate our culture of compliance and corporate integrity, based on best practices, rejecting any conduct that is irregular and/or criminal, illicit or contrary to our principles and ethical commitments and/or in violation of current laws.



Promote an environment of effective, efficient and timely prevention, using specific mechanisms to prevent and mitigate the risks of committing crimes or regulatory violations to which the Company is exposed.



Comply with the provisions of the Law, especially the management and supervisory duties that the Company must exercise.

## 3. SCOPE

This Model applies to all controlled operations in Chile or abroad. Therefore, for foreign operations, applicable local legislation must be reviewed to adapt the scope of this document to similar laws. Jurisdictions without such legislation should consider the guidelines set forth by the parent company in this document. Similarly, the standard established here will be applied when the local standard is more lenient.

Uncontrolled companies are highly encouraged to implement control practices, structured using a systematic model to prevent irregularities, crimes and regulatory violations. This model should be based on risk exposure and led by the Board of Directors and senior management.

## 4. CORPORATE CRIMINAL LIABILITY (LAW NO. 20,393)

Chilean Law No. 20,393, which established criminal liability for legal entities for the crimes contained therein, took effect on December 2, 2009. Since then, legal entities may be criminally liable for a crime committed by individuals considered part of the Company in any way, if they have acted in the entity's direct benefit, interest or gain, and the commission of such illicit act is a result of a company failing to exercise its management and supervisory duties. In addition, under the same assumptions mentioned above, the legal entity will be criminally liable when the crimes have been committed by individuals under direct management or supervision of any of the aforementioned subjects.

Therefore, criminal liability can be attributable to a company if:



The crime is committed by individuals linked to the company;



The crime generates a benefit for the company, or for its gain;



The crime is committed as a result of the company failing to exercise its management and supervisory duties.

For the purposes of Law No. 20,393, management and supervisory duties have been exercised when, before the crime is committed, the legal entity has adopted and implemented organizational, administrative and supervisory models to prevent such crimes, as set forth in that law.

## a. Crimes Related to Law No. 20,393

The following crimes give rise to criminal liability for legal entities as described in the aforementioned law:



**Money laundering:** Concealing or disguising the illicit origin of certain assets, by engaging in transactions that hide or cover up the nature, source, location, ownership or control of illegally obtained money or goods. It involves transforming assets of illicit origin (e.g., from drug trafficking, human trafficking, arms trafficking, promotion of child prostitution, embezzlement of public funds, malicious use of privileged information, computer fraud, fraud, tax crimes and other crimes) into funds from an apparently legal source.

---

**Terrorism financing:** Requesting, raising or providing funds, by any means, for the purpose of using them to commit any terrorist crime. Therefore, terrorism financing is any economic act, assistance or measure that provides financial support to the activities of terrorist groups.

---

**Bribery of a national or foreign public official:** Offering, promising, granting or consenting to the delivery of an improper payment, valuables or economic or other types of benefits to a Chilean or foreign public official (authorities, public employees, government representatives, or someone fulfilling a public function) in exchange for improper actions or omissions particular to their position or actions as a public official, to obtain an advantage or benefit for the company.

The term 'foreign public official' includes any person holding a legislative, administrative or judicial office of a foreign country, whether appointed or elected; any person exercising a public function for a foreign country, within either a public agency or state-owned enterprise. It also includes any official or agent of a public international organization.

---

**Handling stolen goods:** Storing, transporting, buying, selling, transforming or marketing, in any form, unduly obtained, misappropriated, looted or stolen goods if their origin is known or should be known.

---

**Inappropriate business dealings:** When a director, manager or senior executive of a corporation takes an interest in any negotiation, act, contract, transaction or deal involving the company in breach of the conditions established by law. In other words, the crime is committed by taking part in a decision-making process while having an undisclosed conflict of interest.

---

**Corruption among individuals:** Accepting or receiving a benefit, whether economic or of another type, for one's own or third-party benefit, in order to favor or facilitate the choice of one bidder (supplier) over another. In other words, the decision maker in a contracting process is given a benefit to favor a certain supplier, thus affecting the principles of equal conditions, objective evaluation criteria in purchasing or bidding processes (or their participation in them) and antitrust principles.

---

**Unfair administration:** When a person in charge of safeguarding or managing third-party assets (of another individual or group of individuals), by virtue of the law, a regulatory order, an act or contract, causes damage by abusively exercising the powers of administration bestowed upon him/her, carrying out or omitting an action that is overtly contrary to the interest of the owner or holder of the affected assets.

---

**Misappropriation:** Removing or acting as the owner of money or personal property that would have been received by a third party and not returning it upon request, as well as using cash or in-kind gifts for an unintended purpose.

**Water pollution affecting hydrobiological resources:** Intentionally, maliciously or negligently dumping or ordering someone to dump chemical, biological or physical pollutants that harm hydrobiological resources into the ocean, rivers, lakes or any other body of water.

---

**Crimes related to illegal fishing<sup>1</sup>:** Marketing or selling, processing, producing, storing, transporting and over-exploiting resources from the seabed, banned products or hydrobiological resources without confirming their legal origin.

---

**Employer non-compliance with health orders:** Anyone vested with the authority to decide upon the work of their subordinates, who knowingly orders them to attend a workplace other than the worker's home or residence, while they are under quarantine or mandatory sanitary isolation decreed by the health authority.

---

**Migrant smuggling and human trafficking:** Capturing, transferring or retaining persons, whether nationals or foreigners, recruited within the country or brought from abroad (generally illegally), in order to benefit from the victim's work by taking advantage of the victim's personal circumstances, or by paying an economic or other benefit to the person with authority over the victim. In these cases, the victim has no choice but to accept, even if his/her dignity and rights are violated.

---

**Activities against the Weapons Control Law:** Possessing, carrying, marketing, having, importing and entering into the country weapons, artifacts, articles or ammunition prohibited or subject to control by the authorities.

---

**Timber theft:** theft or robbery of logs or timber. This crime is also committed by anyone in possession of logs or timber when they cannot justify their acquisition, their legitimate possession or their work in such tasks or related activities aimed at felling trees, and, likewise, anyone who is found on another's property performing the same tasks or activities, without the consent of the owner or authorization for felling. The same applies to anyone falsifying or maliciously making use of false documents to obtain guides or forms to illegally transport or sell timber.

---

**Computer crimes:** Executing a series of acts to attack the integrity of a computer system (e.g., illicit access, illicit interception of information, falsification, handling stolen data, fraud and abuse of computer devices).

---

1) For this group of offenses, no risks have been identified in the activities we carry out as a Company or the industry in which we operate.

## Sentences, Penalties and Fines for Violations of Law No. 20,993:

### For Individuals:

Individuals (individually) who commit these crimes may be exposed to a variety of penalties.

In Chile, the law establishes penalties, depending on the crime committed, which in some cases can reach up to 10 years in prison, fines in some crimes of up to 5,000 UTM (monthly tax units), and a prohibition from holding public office or working in companies that are state-owned or have contracts with the state.

Therefore, individuals are primarily responsible for complying with the guidelines in this document; and for avoiding any conduct that may constitute a crime, especially in exercising or performing their work for the Company, or the work performed by personnel under their charge.

The foregoing is notwithstanding the corresponding disciplinary measures, in accordance with the Company's internal rules.

### For Legal Entities:

Legal entities are exposed to the penalties of:

- a. Dissolution of the legal entity or cancellation of its legal personality;
- b. Fine payable to the state (400 to 300,000 UTA);
- c. Temporary or lifelong prohibition from entering into acts and contracts with the State and prohibition from being awarded (or renewing) concessions;
- d. Partial or total loss of tax benefits or absolute prohibition from receiving such benefits for a determined period; and
- e. Accessory penalties (publication of an extract of the judgment, confiscation, payment into tax coffers of an amount equivalent to the investment made in committing the crime if it exceeds the revenue generated by the company).



## 5. Liability for Violating Antitrust Regulations

Generally speaking, DL 211 defines an attack on free competition as “any act or convention that impedes, restricts or hinders free competition or tends to produce such effects(…)”

### a. Anti-competitive practices

- Conduct linked to horizontal agreements (i.e., developed jointly or in coordination with competitors and affecting any competitively relevant variable).
- **Collusive agreements:** Direct or indirect coordination between two or more competing companies to coordinate their behavior in the market with respect to a competitively sensitive variable (e.g., price fixing, cutting production, allocating market areas or quotas, affecting the outcome of public or private bidding processes, sales/marketing conditions or others).
- **Concerted practices:** Direct or indirect coordination between competitors, who, without entering into an agreement as such, knowingly substitute the risks of competition for practical cooperation between them. Typically, it takes place through an exchange of sensitive commercial information between competitors.
- **Exchanges of sensitive commercial information:** Direct or indirect exchanges between competitors of strategic information that, if known by a competitor, would influence its behavior in the market, enabling non-individual decision making (e.g., pricing policies, sales and purchase conditions, discount policies, payment terms and conditions, costs, profit margins, production volumes, business strategies, techniques for the design and content of future bidding offers, development of new products or services, among others).
- **Conduct related to abuse of dominant position:** Unilateral, abusive conduct by one or more companies with a dominant position in the market that inflicts harm on their suppliers, competitors, customers or consumers (directly or indirectly). For example, predatory pricing, refusal to sell, margin squeeze, arbitrary discrimination, abusive pricing, tied sales, among others.
- **Anti-competitive practices:** In general terms, any behavior contrary to honest industrial or commercial conduct constitutes an anti-competitive practice. Illicit practices include but are not limited to: (a) acts capable of creating confusion in the customer, by any means, with respect to the company itself, the products offered by the company, or a competitor's industrial or commercial activity; (b) false assertions, in the course of trade, capable of discrediting a competitor's products, industrial or commercial activity; and (c) indications or assertions whose use, in the course of trade, could be misleading as to the nature, mode of manufacture, characteristics, suitability for use or quantity of the products.
- **Interlocking:** A link between two competing companies that occurs when they directly or indirectly share people in relevant executive or board positions. The most paradigmatic case, called direct interlocking, is when the same person simultaneously fulfills the roles of director or relevant executive in two competing companies.

## b. Penalties for Violating DL No. 211

Antitrust law establishes severe consequences for offenders. The following penalties can be applied by the Antitrust Court or Supreme Court:

- **Fines:** up to 30% of the offender's sales of the line of products or services associated with the violation during the period for which the violation was occurring or up to twice the economic benefit reported from the violation. If the sales or economic benefit obtained by the offender cannot be determined, the maximum fine that can be given is 60,000 annual tax units ("UTA") (approximately US\$ 49 million).
- Modify or terminate acts, contracts, covenants, systems or agreements declared to be contrary to DL No. 211.
- Order the modification or dissolution of the companies, corporations and other private legal entities that have intervened in the aforementioned acts, contracts, covenants, systems or agreements declared illegal;
- In the event of collusion, additional penalties may also be applied:
  - » Prohibition to sign contracts with the state: Economic agents found guilty of collusion may be prevented from:
    - I. signing contracts, in any capacity, with state administrative bodies; autonomous agencies or institutions; agencies, companies or services to which the state makes contributions; the National Congress and the Judiciary; and,
    - II. being awarded any concession granted by the state. Both prohibitions may last for a term of up to five years..
- **Criminal penalty:** anyone who enters into, implements, executes or organizes agreements that fall into the category of hard core cartels may receive a sentence anywhere from minor imprisonment in its maximum degree to major imprisonment in its minimum degree (i.e. from 3 years and 1 day to 10 years). In addition, if any of the alternative penalties in Law No. 18,216 (e.g. conditional remission, partial imprisonment and probation) are applicable, their execution will be suspended for a period of one year. This means that if a person is convicted of collusion, he or she must serve at least one year in prison before any alternative penalty can be applied.
- Additionally, the court can apply an accessory penalty of **ineligibility from holding the position of director or manager of a public corporation** or other entity subject to special rules (e.g. banks, pension fund administrators, insurance companies, mutual fund management companies, among others), of state-owned enterprises or companies in which the state holds a share, and of a trade or professional association, for a term of 7 years and 1 day to 10 years. Criminal penalties are not applied in antitrust proceedings, but require the following requirements to be copulatively met:
  - I. the individual has been previously penalized by the TDLC or the Supreme Court;
  - II. the National Economic Prosecutor files a complaint for the crime of collusion, which allows the Public Prosecutor's Office to intervene; and,
  - III. the competent criminal court convicts the individual of the crime of collusion.

## 6. Compliance Program Pillars



Our Compliance Program is based on four pillars, composed of the following legal, regulatory and best practice aspects of crime risk management.



Prevention  
Activities



Detection  
Activities



Response  
Activities



Supervision  
and Monitoring  
activities



**Prevention Activities:** These are designed to reduce the likelihood of risks occurring by defining controls, guidelines and rules for conduct, preventing violations of the Program and/or laws in force, which consequently helps prevent crimes from being committed.

The baseline for this pillar consists of, but is not limited to, the following prevention activities:

- Board approval of the Compliance Program
- Board appointment of a Compliance Officer (Crime Prevention Officer, CPO)
- Identification and analysis of the risks of crimes or antitrust violations being committed by preparing and updating risk matrices and proposing control measures for mitigation
- Incorporation of CPM guidelines into the Code of Ethics, Internal Order, Hygiene and Safety Rules and all procedures, manuals and protocols that include norms related to the duty of compliance
- Monitoring and control of compliance by the Compliance Officer in conjunction with the Board of Directors and senior management; and by the internal audit area, with support from the Chief Executive Officer and the company's entire Executive Committee.
- Communication and training of all employees on the Compliance Program in general terms and also focused by risk area; and the role each person must play for it to function correctly (orientation programs, regular training, communication on the Intranet, webpage, mass mailings, etc.).



**Detection Activities:** These aim to identify and alert the company to the real or potential occurrence of conditions and events that qualify as violations of the Compliance Program and/or Law No. 20,393 or DL No. 211. Detection activities consist of, but are not limited to:

- Compliance audits and controls by the internal audit function.
- External audits on the compliance and operability of controls on the Compliance Program.
- Follow-up control of actions and commitments arising from audits.
- Special reviews and supervision by the Compliance Officer.
- Review of litigation, lawsuits and contingencies.
- Receipt of complaints through the Whistleblower System and the channels available for reporting irregularities.



**Response Activities:** These seek to respond to irregularities detected; establish resolutions or disciplinary measures for violations; resolve weaknesses detected as a result of detection activities and/or correct situations that are or could be violations of the Compliance Program or Law No. 20,393 or DL 211, leading to updates to the Program and control practices, as well as feedback and continuous improvement.

Response activities consist of, but are not limited to:

- Actions to improve Program weaknesses detected as a result of some type of violation and/or irregularity.
- Complaint management and investigation procedure and timely response.
- Recording of complaints, investigations and reporting to Ethics Committee.
- Application of internal disciplinary measures; and evaluation of the filing of legal actions or complaints by the Public Prosecutor's Office, the National Economic Prosecutor's Office, the Financial Market Commission or any other competent body, when appropriate.



**Monitoring Activities:** These are intended to generate ongoing reviews of adequate compliance with the Program and the set control activities, as well as constant monitoring of any amendments to the laws in force and structural changes within the company and the processes it executes, in order to update the risk matrices and mitigating controls.

Monitoring activities consist of, but are not limited to:

- Monitoring of the Compliance Program for SAAM TERMINALS and subsidiaries within its scope
- Updating of Program
- Biannual reports to the Board regarding the operation and updating of the Program
- External certification of the Compliance Program.

## 7. MAIN CONTROLS FOR COMPLIANCE PROGRAM

### a. STRUCTURAL CONTROLS:

- Code of Ethics
- Risk Management Policy
- Compliance with internal company regulations
- Defined structure of powers of action and representation for executives
- Obligations and prohibitions defined in the Employment Contract, especially for positions of responsibility (or by contract appendix)
- Incorporation of control measures for Compliance Program in Internal Order, Hygiene and Safety Rules
- Supplier contract addendum acknowledging awareness of our Compliance Program
- Application of "Know Your Counterparty" or "Due Diligence" (M&A, donations, suppliers and third parties in general, based on risk level)
- Internal and compliance audits
- Communication and Training Plan
- Whistleblower Channel and Complaint Management Procedure

### b. PROCESS-LEVEL CONTROLS:

- Protocols and controls for donations, contributions, grants and sponsorships
- Best practices for engaging with public officials and PEPs
- Public official and PEP engagement matrix
- Conflict of Interest Management and Declaration of Related Parties
- Policies and procedures for purchasing, bidding, selection and relationship-building with suppliers
- Procedure for payments and advances to suppliers and third parties
- Travel Expense Policy
- Procedures for requesting funds, reporting expenses and using corporate credit cards
- Procedure for personnel recruitment and selection
- Protocols for giving and receiving gifts, invitations and hospitality
- Use of "Knowledge Your Counterparty" for relevant purchases

- Treasury Manual for controls on funds and banks
- Procedures for travel expenses, requesting funds and reporting expenses
- Supplier applications reviewed by the Award Committee.
- Review, approval and monitoring of major purchases and investment projects by the Investment Committee

These measures should help the Company maintain a Compliance Program that effectively, efficiently and opportunely addresses the risks to which we are exposed.

## 8. COMPLAINTS OF VIOLATIONS

To ensure Program compliance, the Company has set up a Whistleblower System with a respective governance layer and procedures to handle every report received:

The system is available on our corporate website and on each business unit's website.

Our system offers three reporting channels:

- **Web platform:** accessible anywhere with Internet connection. The whistleblower can access an online, confidential, independently managed platform and choose whether they want their report to be anonymous. Click here: <https://saamterminals.eticaenlinea.com/>

In addition, two other possible channels are available for filing reports or complaints of irregularities. They are governed by the same principles of confidentiality and anonymity and the same management procedure.

- **Email:** Alternatively, reports may be filed by emailing: [denuncias@saamterminals.cl](mailto:denuncias@saamterminals.cl)
- **In person:** You can also file a report through your direct supervisor, your department manager, the Ethics Committee, the Human Resources department or the Compliance Department. These individuals/ departments all have the obligation to promptly deal with this report through the channels available for centralized management.

Our whistleblower system is available to all parties covered by the scope of this Code of Ethics.

Keep in mind that:

- The Whistleblower Channel is **confidential** and the Company will ensure that confidentiality is protected, except for exceptions contemplated in the Law.
- SAAM TERMINALS undertakes that there **will be no retaliation** in the event of a report made in good faith, even if an investigation determines that no violation has occurred. An employee targeted by retaliation may file a complaint.
- All complaints are **reviewed by the Company's Ethics Committee**, which meets quarterly.

- It is in the Company's best interest that all those who **use the Whistleblower Channel do so in good faith and responsibly.**
- To **file a complaint, you must follow** the considerations in the **General Complaint Management Procedure** and the Instructions for the Whistleblower, both available on the Company's website or its whistleblower web portal:

## 9. CPM GOVERNANCE AND RESPONSIBILITIES

The SAAM TERMINALS Compliance Program requires adequate corporate governance and assignment of roles and responsibilities for optimal operation.

The main responsibilities involving the Compliance Program include:

The Board of Directors, Chief Executive Officer and Compliance Officer of SAAM TERMINALS shall be jointly responsible for the Program's adoption, implementation, administration, updating, supervision and proper functioning.

The Compliance Officer (or Crime Prevention Officer) reports functionally to the Board of Directors, which means that:

- The appointment, confirmation and dismissal shall be made by the Board of Directors for a term of 3 years and may be renewed.
- They will have direct access to the Board to promptly inform it of the Program's functioning and the measures and mitigation plans implemented in doing their job, and will render an account of their management at least once every six months.
- They will have autonomy with respect to the Company's management and that of its subsidiaries
- The Board of Directors will provide sufficient resources for the Program to function, based on the size and complexity of the Company.

Program-related obligations, prohibitions and internal disciplinary measures must be expressly incorporated into internal regulations, employment contracts and service contracts for all company employees, suppliers and service providers.

In short, we would like to underscore that:

- All employees are individually responsible for their actions.
- All employees undertake to abide by the Company's principles and values.

In this context, employees:



- Are prohibited from committing acts that may constitute crimes or antitrust violations
- Must exercise due care with the Company's assets and resources
- Have an obligation to report conflicts of interest and links with Public Officials and/or Politically Exposed Persons; and to file a declaration of related parties.
- Are prohibited from making improper payments
- Must comply with internal company regulations
- Must attend training sessions as requested.
- Must communicate any violation of internal rules and laws in force through the available channels.

All executives and employees in charge of activities with potential risk scenarios are responsible for knowing the scope of the Program, providing the available information regarding their processes as requested for a review process and/or similar, ensuring compliance with the controls for the processes under their responsibility and supporting the prevention, detection, response and monitoring activities outlined in the model.

## 10. EXTERNAL CERTIFICATION

The certification process is carried out at the Company's request and involves reviewing background information, risk situations, the operability of existing controls and the risk management governance model. If the conditions set by Law No. 20,393 for crime prevention models are substantiated, the certifying entity accredits and reports the terms of the certification to the Financial Market Commission (CMF). The maximum validity for a certification of this type is two years. To certify antitrust regulatory compliance, a certifying company reviews compliance with the standards set forth in TDLC case law. Por su parte, en cuanto a la certificación del cumplimiento normativo en materia de libre competencia, también se realiza un proceso por parte de una empresa certificadora, la que revisa el cumplimiento de los estándares dispuestos en la jurisprudencia del TDLC.

## 11. 10 EFFECTIVE DATE, UPDATING, PUBLICATION AND COMMUNICATION

This document will take effect on the date it is approved in the respective minutes of a regular board meeting.

The Compliance Officer is responsible for updating the Compliance Program, which must be reviewed at least annually and updated as needed.

This document will be published on the Company's Intranet and an extract of the document will be published on the website. It will be distributed digitally and made available to all employees, who must acknowledge receipt using the electronic signature platform.



## PROOF OF DELIVERY AND ACKNOWLEDGMENT OF RECEIPT

### Compliance Program

Date: \_\_\_\_\_

Employee Name: \_\_\_\_\_

Tax ID Number: \_\_\_\_\_

Position: \_\_\_\_\_

Company: \_\_\_\_\_

Declares to receive in this act a digital copy of this document containing the relevant aspects of the Compliance Program that the company has implemented to comply with Law No. 20,393 on Criminal Liability of Legal Entities, as well as the antitrust regulations in DL 211; whose provisions, obligations and responsibilities it undertakes to fulfill.

---

#### Employee's Signature

(The document is signed by means of an electronic signature platform, through which a PDF copy can be accessed once signed)