CODE OF CONDUCT

GRUPO SECURITY S.A.

“All employees of Grupo Security S.A. must read this Code of Conduct in detail.

It is our responsibility and commitment to maintain, at all times, the highest ethical standards in our daily work. The corporate values of closeness, transparency and professionalism must guide us and be present in all our interactions and decision making. We must remember that we always represent the Company and that we are its best ambassadors."

Fernando Salinas Pinto
Chief Executive Officer
Grupo Security

CONTENTS

1. Scope

This Code of Conduct is applicable to all employees at Grupo Security S.A. It complements the Code of Ethics and is subject to employment contracts, internal regulations, policies, standards and procedures issued by the Company and relevant Chilean and international law.

The obligations imposed by this Code have been established in harmony with the fundamental rights of employees, while expecting that labor relations be conducted in good faith. They seek to avoid conflicts of interest, the abuse of insider information or the abuse of a dominant position, which employees may come across in the course of their duties or within their division.

1.1 Our Mission

To satisfy our customers' requirements for lending, asset management, insurance and services by providing comprehensive services of exceptional quality that exceed their expectations.

1.2 Our Vision

We want to set the standard in all of our relationships, both in business and among staff, in order to comprehensively meet the requirements of our customers, shareholders, employees and the world in which we do business, while encouraging a healthy work-life balance.

1.3 Our Values

Transparency: Always prefer the truth, transparency in relationships and honorable behavior.

Professionalism: Loyalty and commitment to our Company's objectives and motivated to perform the functions of the position efficiently and without hesitation.

Closeness: Inspired by a strong service commitment to third parties, internal and external customers and other market participants, to meet their requirements and resolve them, where possible.

2. Distribution, Validity and Updates

This Code of Conduct is considered to be widely understood as it has been approved by the Board of Directors and subsequently distributed. Therefore, it shall be given to every employee and published on the Intranet of Grupo Security S.A.

It shall have an indefinite life, and must be amended by the Corporate Culture Division in conjunction with the Corporate Compliance Division whenever new behavior rules need to be incorporated. Therefore, each employee is responsible for understanding the updates to this code.

3. General Behavior

This Code of Conduct establishes the following behavioral rules. Employees should:

A) Understand this Code and always behave in a professional, serious, efficient and diligent manner in accordance with the spirit, principles and provisions established herein.

B) Understand and keep up to date with the practices, procedures and regulations related to their position and be aware of their responsibilities.

C) Maintain absolute objectivity and independence when performing their work.

D) Maintain a friendly, dignified and respectful attitude with their internal and external customers and with all other business contacts, such as, competitors, suppliers, etc. Behave with honesty, clarity, accuracy, reliability, loyalty, fairness, integrity, good faith and in accordance with best practice to ensure transparency and security for customers, market integrity and Company profitability.

E) Maintain a cooperative and transparent attitude that builds trust within the Group with staff from Internal Audit, Internal Control, directors, managers, senior executives, etc., and with regulatory, stock market, administrative and judicial authorities in general.

F) Avoid any transaction using money from illegal or inappropriate activities, such as prostitution, drug trafficking, weapons trafficking, corruption, etc.

G) Submit to legally permitted medical examinations and other clinical procedures required to ensure that their physical and mental condition is suitable for their position.

H) Carefully manage their personal finances and keep any borrowing within limits that are compatible with their income.

I) Supervisors should always behave in a manner fitting their position, in accordance with the standards established by the Company. Therefore, they should not request their subordinates to behave in a manner that is inconsistent with established procedures or contrary to ethics.

However, the circumstances mentioned above do not span the complete range of potential situations that an employee may come across. Therefore, each employee is expected to behave in accordance with the values established in the Code of Ethics.

4. Specific Behaviors

The following specific behaviors apply to all employees:

4.1 Law 20.393: Crime Prevention

Law No. 20,393 and its amendments establish criminal liability for legal entities. Accordingly, the Company may be liable for offenses committed by employees and dependents within the scope of their duties.

Therefore, the Company expressly prohibits any conduct that may give rise to criminal charges being brought against the Company caused by owners, controllers, managers, senior executives, representatives, administrators, supervisors or any employee or external collaborator.

In conclusion, the crimes listed in Appendix 9 should not be committed while carrying out company business.

4.2 General Criteria for Conflicts of Interest

What is a conflict of interest?

A conflict of interest is the incompatibility between the Company's interests and those of employees when a particular transaction is executed by an employee on behalf of the Company, while protecting their own interests or those of third parties with whom they have a business or family relationship or any other personal link. Equally, there is a conflict of interest when an employee directly or indirectly enters into the same business as their employer, which has been prohibited. Where conflicts of interest arise, the failure to recognize this incompatibility indicates disloyalty to the Company. In these circumstances, an employee should not be involved in any matter in which they have a direct or indirect interest of any kind, where their objectivity or independence may be compromised.

Clearly, a decision made by the Company regarding a situation containing a conflict of interest may be based on the wrong reasons. But, even if these reasons are correct, such conflicts can affect an organization's reputation and damage private and public confidence in it.

Although a conflict of interest has been defined above, there are countless circumstances that can be interpreted as a conflict of interest, based on the failure to recognize such an incompatibility. Various examples are described below, which might be used to help detect them:

Example 1: The financial interest of a Grupo Security S.A. employee, or any of their relatives, who establishes a business relationship with the Company.

Example 2: An employee associated with a Politically Exposed Person (PEP). This situation should be reported to their supervisor or manager.

Example 3: Receiving a benefit, hospitality or gifts from a third party, who may be affected by a decision or action of Grupo Security S.A.

Example 4: Advice provided by an employee to their relatives or other persons associated with the employee, to buy securities in their portfolio, in violation of the employee's duty of confidentiality.

General considerations to identify potential conflicts of interest are the obligations and prohibitions agreed in the contract and established in the Company's internal regulations, however, additional considerations include:

• Perception: Could the transaction that involves the employee be perceived as a possible conflict of interest? If all the facts are made public, what would be the impact on Grupo Security S.A. or the employee?

• Intention: Do the employee's activities for a third party aim to influence the recipient's or the employee's judgment and impact the Company's interests?

• Impact: Would this be detrimental for the Company, its shareholders or customers, without legitimate reason, if the employee participates in the activity or transaction?

• Objectivity: Would the participation of an employee in an activity or transaction affect the customer's or the employee's judgment when making business decisions?

• Time-related considerations: If the activity involves an external task, would the time required interfere with the employee's ability to effectively carry out their responsibilities to the Company, its shareholders or its customers?

What should you do if you think that there might be a conflict of interest?

You should consult your direct supervisor or manager. If the conflict cannot not be resolved, this should be communicated in writing to your company's Compliance Officer with a copy to the Corporate Compliance Division, along with all accepted mandates related to conflicts of interest.

Company policy is that the interests of our customers should never be compromised. Therefore, employees are required to disclose to their supervisors the nature and extent of any conflict between their own personal, social, financial, or political interests and those of a customer, or even the possibility of such a conflict. The customer's interests should always take precedence and they should always receive fair and equal treatment. If not possible, the employee should refrain from executing the transaction.

If a conflict arises between customers, neither party shall suffer and all available methods to reach an agreement must be used.

Therefore, we should avoid putting the Company in a leading position on both sides of a transaction. We should also refrain from accepting mandates to act on behalf of our customers, to avoid possible conflicts of interest, except when the customer is an employee's spouse or dependent child. If a mandate of this type has been accepted, employees shall be governed by the principle of independence, so they should always protect the interests of the customer over their own or those of third parties.

4.3 Consuming Alcohol, Drugs and Narcotics

Employees must refrain from consuming drugs or medically unauthorized narcotic substances under any circumstances, or consuming alcohol during working hours, except at authorized celebrations. All employees should take care not to consume alcohol to excess outside working hours, due to its negative effect on their health and on the image of Grupo Security S.A.

Any violation of the prohibition on consuming and trafficking illicit drugs or alcohol shall be regarded as a serious violation of this Code, the Code of Ethics, and Grupo Security's Internal Order, Hygiene and Safety Regulations. Likewise, any refusal to submit to a medical examination and other clinical procedures required to ensure that an employee's physical and mental condition is suitable for their position also constitutes a violation. Employees authorize the disclosure of these results to their employer, subject to legal regulations.

4.4 Activities Not Related to the Position

During working hours employees are not permitted to perform work other than as described in their employment contract or specified in their job description. However, outside of working hours employees may engage in any work or activity provided that it is not equivalent to their duties

performed for the Company, or within the business description of their employer (Art. 160, 2 Labor Code).

If an employee is involved in an activity outside working hours that may be related to their duties, such as classes, lectures, presentations, etc., whose content relates to the Company, they should inform their direct supervisor in advance in writing. The supervisor must request the Corporate Culture Division to assess whether these activities interfere, compete or are in conflict with the interests of the Company or with the ability of the employee to fulfill their responsibilities. If so, the employee should refrain from performing these activities.

4.5 Unlawful Coercion

It is strictly forbidden for any employee to behave in a manner inconsistent with a dignified and mutually respectful working environment. Therefore, any unlawful coercion or harassment, sexual or otherwise, exerted by any employee over another, in particular a supervisor over a subordinate, should be immediately reported to the direct supervisor of those involved, or if the situation cannot be resolved or an employee feels uncomfortable reporting their concerns to people within their division, they should contact the Corporate Culture Division using the means provided.

4.6 Bullying at Work

Bullying at work is abusive behavior that leaves employees feeling uncomfortable and has a negative impact on the lives of people within and outside the workplace. This mainly includes:

- Personal threats
- Derogatory comments
- Public humiliation
- Intimidation tactics
- Verbal abuse
- Deliberately excluding an employee from meetings or discussions
- Excessive demands, impossible deadlines or irrational requests

The Company strives to maintain good working relationships both within and outside the workplace and strictly prohibits bullying behavior among employees, and with suppliers, customers, etc.

If any employee falls victim to or comes across this type of behavior, it should be reported as soon as possible to their direct supervisor, or if the situation cannot be resolved or an employee feels uncomfortable reporting their concerns to people within their division, they should contact the Corporate Culture Division using the means provided.

4.7 Information Security

Grupo Security S.A. employees have access to information that is confidential and for internal use only. It should not leave the Company, nor be totally or partially disclosed, rephrased or shared with anyone, including customers, family members, friends, partners, or other employees who do not need it to

perform their duties, without the express authorization of the corresponding supervisor (see Appendix 1).

Employees should handle the information provided by customers, workers and suppliers with the strictest confidentiality, and be extremely careful to avoid any disclosure to third parties, whether or not intentional, without the party's express written consent. Therefore, all employees should at least abide by the following:

A) Never use information to benefit themselves, a third person or their family.

B) It should only be used within the scope of the tasks assigned by the customer or the Company.

C) Never discuss topics that involve this kind of information in public places, regardless of whether they relate to the Company, its customers or its current or potential suppliers.

D) Divisions that hold such information should ensure that no person outside their team has access to it, except as may be necessary in accordance with Company rules. If another employee requests such information, but does not require it for the performance of their duties, this should be immediately reported to a direct supervisor or their replacement.

E) Ensure that business documents are stored in a secure manner to safeguard customer and Company privacy.

F) Secure all materials relating to customers and any other Company material that might be confidential in locked desks or filing cabinets.

G) Keep information in personal computers under strict control, with passwords that restrict access to information contained on hard disks and the corporate network.

H) Ensure that work areas are secure and private. Access to offices where confidential information is kept should be controlled, likewise with filing rooms or storerooms where historical information is stored.

I) Never carry out transactions away from the areas established for this purpose, nor carry them out using unauthorized cell phones or other devices. Areas established for such transactions are those where confidential information is handled, or the areas used by currency exchange dealers, stock brokers or for similar tasks.

J) Avoid recording, filming or taking pictures on Company premises, without prior approval from a supervisor or the person responsible for that area.

K) Sign a new confidentiality agreement, or extend an existing agreement, to cover special situations where the employee’s involvement might produce a conflict of interest, or their exclusion is necessary or desirable for strategic corporate reasons. This confidentiality agreement should be requested from the Compliance Officer or from the Corporate Culture Division.

Only disclose confidential customer information to third parties when required to do so by a statute, regulation, appropriate legal process or to comply with inspections carried out by regulatory entities or auditors.

These requirements should be reported in advance to a direct supervisor, then validated and approved by Internal Control.

Questions relating to the handling of sensitive and internal information can be resolved by consulting the Manual for Handling Information of Interest to the Market (MHIIM), which is available on the Intranet, and Appendix 1 below.

4.7.1 Law 19,628: Personal Data Protection

All employees must strictly comply with the data protection policies published, trained and implemented by the Company. Any violation of these policies will be considered a serious breach of employment and contractual obligations.

Therefore, it is **prohibited** to:
A) Handle personal data without the due authorization of its owner, except for the exceptions provided for in the legislation in force and in our Information Privacy Policy. Such authorization must always be in writing in a document signed by the holder, either physically or electronically.

B) Handle personal data of workers, temporary workers, subcontracted workers, customers, suppliers, directors, shareholders and in general of any person related to the Company, without their express authorization in the terms indicated in paragraph A, except for legal exceptions.

C) Obtain or access personal data illegitimately or without the owner's express authorization.

D) Fail to use due care in the handling and protection of these data.

E) Allow unauthorized access to personal data of employees, customers, prospects, and in general to any data processed by the employer.

All employees must be aware of the Data Privacy Policy of the group and its companies.

4.8 Handling Inquiries from Customers, Third Parties and the Media

Always check that the person making the inquiry is the customer, when responding to customer inquiries. When responding to inquiries received by telephone, Internet or other means, if the customer is not known, their identity should be checked by requesting an identification document or calling the telephone number registered with the Company. If the customer cannot attend in person and sends a representative, this person should provide supporting legal documentation, which should be validated by Internal Control.

We are not authorized to provide information about our customers to third parties, under our duty of confidentiality, except when formally requested by local authorities (courts of law or regulators).

Every request received from authorities or third parties should be channeled through the Internal Control Division and no response should be provided without prior approval.

Every employee should avoid disclosing any information to the media, unless their duties specifically include that responsibility or they have been expressly authorized to do so. For all intents and purposes, only the Chairman of the Board and the CEO can release information to the press.

4.9 Gifts, Incentives and Social Activities

Receiving gifts and incentives

Employees should abide by the following, in order to maintain business transparency and avoid any kind of misunderstanding:

A) It is expressly prohibited to:

• Require for oneself or for a third party any object/matter of value in exchange for a transaction/business, service or confidential information relating to Grupo Security S.A., or accept any object of value (except for usual authorized compensation or hospitality and gifts of nominal value as listed below) from any person in connection with transactions/business of the Company.

• Accept any donations from customers, except those from a family member. If this happens or might happen, a direct supervisor should be informed.

• Request, either personally or through intermediaries, loans or any financial aid from customers, suppliers, brokers, partners or third parties, except from family members or through corporate links with financial institutions recognized for providing such facilities.

B) The following items may be accepted:

• Advertising items of little value, not exceeding UF 3.5. Any gift, invitation or hospitality valued at over UF 3.5 should be previously authorized by the CEO.

• Normal invitations or social activities that are considered reasonable, not exceeding UF 3.5.

• Occasional gifts for specific and exceptional events that represent an expression of friendship or goodwill, such as Christmas or wedding gifts, provided that they are not in money and are within reasonable limits.

These gifts may only be accepted sporadically and cannot become habitual without appropriate justification. They should never exceed the limit mentioned above.

An employee may participate in occasional events sponsored by suppliers, distributors or customers, provided they obtain their supervisor's authorization, even if these events include free prizes for the participants based on impersonal selection criteria, consisting of articles or benefits such as discounts, trips, accommodation, entertainment, etc.

Finally, if a gift that exceeds these limits cannot be refused, then these details should be immediately reported to your direct supervisor in writing with a copy sent to Corporate Compliance Division. If the value or the characteristics of the gift are excessive, the CEO should also be informed.

Giving Gifts and Incentives

As a general rule, gifts, invitations, hospitality, favors or any other compensation linked to Company business should not be given by employees under their own initiative, either to customers, current or potential suppliers, intermediaries or any other third party. This does not apply to corporate situations such as promotions, contests, etc., that are not related to a particular transaction.

Furthermore, gifts of significant value that denote the intention of the giver or customer to influence any business transaction undertaken by the Company should not be accepted, given, offered, promised or consented to give to national or foreign public officials, either before, during or after the transaction has been carried out, in compliance with Law 20,393 and its amendments regarding the crime of bribery.

The behaviors previously described will not be accepted, either, with respect to employees or private agents, since they could constitute the crime of corruption among private individuals, incorporated into the Criminal Code by law 21,121.

4.10 Donations

All Company donations should be properly documented in advance using the Company Donations Form and Declaration of Donation Receipt Form (see Appendix 2), to maintain transparency and control donated funds. All such forms should be sent to the Corporate Compliance Division, who must process and register this information.

4.11 Bribery

Bribery is offering money or any other compensation with the aim of influencing in an illegal manner the behavior of another person. Therefore, the use of Company resources for illegal or unethical purposes, such as the payment of illegal commissions or compensation, is strictly prohibited. The same applies for the acceptance of any compensation from external persons or institutions or employees.

4.12 Use of the Company's Resources and Assets

All employees should care for, correctly use and safeguard in a responsible manner all the resources and assets provided by the Company. These should not be wasted and employees should constantly seek savings while carrying out their duties. This includes:

A) Company Property and Services: Employees are not personally, nor through any relative, entitled to use Company property or services without prior written authorization from the CEO, or the person designated by them. This extends to repossessed properties or vehicles, as this may cause legal problems for the Company. The disposal of any Company property or service follows a formal and reported process to ensure transparency.

B) Employees are Not Permitted to Personally Benefit from a Legitimate Business Opportunity: They are not permitted to personally benefit from any legitimate business opportunity that has been managed by the Company through its staff, contacts or financial capacity.

C) Using Company Information, Technology Resources and Systems: Likewise, the Company's IT assets and services may only be used for tasks related to the employee's job description. Consequently, employees are prohibited from accessing these assets and services or disclosing through them contents that are not related to their functions or conflict with moral standards. Further information is contained in the Information Security Policy, published on the Intranet, particularly the Communications Management Standard.

D) Using Per Diems: Employees should seek reimbursement of their expenses incurred on each trip or for each service provided, which must include a reasonable per diem, thereby carefully using Company

resources. This should comply with the Grupo Security Travel Policy or guidelines defined by the Corporate Culture Division.

E) Supporting Documentation for Expenses: All claims for the reimbursement of expenses for social activities, per diems, etc., should accurately reflect all the associated costs and be supported by documentation, such as receipts, invoices, etc. In addition, employees should use the Expense Reimbursement Form (see Appendix 3), which should be submitted to the respective Accounting Division. Therefore, the following are prohibited:

• Keeping hidden accounts within the Company

• Altering supporting documentation for expense claims

• Including false expenses within expense claims

• Carrying out transactions or approving payments and using the funds for a different purpose than that originally intended.

F) Intellectual Property: The Company owns all the rights to and interests in intellectual property, including inventions, improvements, ideas, processes, software programs and all discoveries conceived or developed by employees while carrying out their duties. Therefore, employees are expected to carefully use the property developed during the course of their duties. Further information is contained in the Information Security Policy, published on the Intranet, particularly the Compliance Standard.

Moreover, every employee should inform their direct supervisor when they need to protect such intellectual property.

G) Using Company Brands, Logos and Image: It is prohibited to use Grupo Security brands or logos in any documentation for personal or unofficial purposes.

4.13 Acquisition of Goods or Personal Services through the Company

Employees may purchase goods or services through the Company, though in order to maintain business transparency they should comply with the following conditions:

A) They should use the same regular procedures, unless the corresponding Company has a special policy for this situation.

B) Employees should report the details to their direct supervisor in writing and request the corresponding authorization (see Appendix 4). They should send a copy to the Corporate Compliance Division.

C) The purchase should be carried out by a person that has been authorized by the corresponding supervisor and should be someone other than the employee who is acquiring the good or service.

D) The goods or service should be purchased under the same conditions and at the current fair market price, unless the corresponding company has a special policy for this situation.

Employees in asset management areas wishing to use personal accounts must also comply with the provisions of Section 5.4.6 of this code.

4.14 Acquisition of Repossessed Goods

Repossessed goods are those received by the Company for non-payment of obligations due from a debtor, for example: vehicles or properties.

Repossessed goods should initially be offered for sale through any public means of communication, such as newspapers or the radio, or through brokers for properties or through automotive dealers for vehicles or to other similar businesses. Employees should not participate in this process, in order to maintain transparency and avoid conflicts of interest. If this process does not result in a sale, they should be offered to Grupo Security employees under the procedure established by each company.

4.15 Acquisition of Company Furniture

Grupo Security periodically renews its furniture. The furniture being replaced must initially be offered to employees in accordance with the established policies and procedures for each Company.

4.16 Political Activities

Those employees who exercise their democratic rights by participating in political activities should inform their direct supervisor in writing of these activities in accordance with the procedures established by the Corporate Culture Division. These must be permitted provided they do not affect the employee's job performance and the image of Grupo Security.

4.17 Prohibited Behavior

Certain employee behavior is expressly prohibited as it could seriously damage our image and the trust that our customers have placed in us. These are:

When carrying out their duties, employees should never:

A) Receive on behalf of a customer correspondence sent by the Company to customers, as we should ensure that they control this process, thereby ensuring proper transparency.

B) Accept money from customers to pay for products or services in places or from staff not authorized for this process.

C) Make recommendations without giving prior warning to customers of the risks involved investing in volatile markets nor for any reason suggest evading taxes.

D) Incorrectly use or send information contained in Company networks, by any means, whether magnetic, electronic or in writing using notebooks, mobile telephones, documents, flash drives, CDs, etc. See Appendix 1.

E) Ask our customers for their passwords or receive them in order to perform transactions.

F) Attract or retain customers by providing benefits that are not compatible with good market practice.

G) Offer products or services at prices lower than their associated costs in order to close a business transaction to the detriment of the competition.

H) Collude to reduce the options available to customers.

I) Build business relationships based on misinformation, or mislead customers or suppliers regarding a specific transaction or the scope of the Company's responsibilities.

J) Falsify or alter Company information.

Within the organization, employees should never engage in:

A) Illegal activities of any kind.

B) Betting or any form of gambling.

C) Fundraising, unless previously approved by the Corporate Culture Division.

D) Personal money-making businesses within the Company or using Company resources or facilities.

E) Sending obscene, vexatious or abusive messages.

F) Doing anything contrary to the Code of Ethics.

G) Sending mass emails or mail chains.

H) Voluntarily creating, transmitting or receiving offensive, defamatory, threatening or abusive material, which includes but is not limited to comments based on race, nationality, gender, sexual orientation, age, disability, religion or political belief.

I) Deliberately damaging computer networks or systems to impair their performance.

J) Negligently or intentionally introducing a virus or destructive program into Company or external computers, workstations, systems or networks.

K) Deciphering or attempting to decipher any system, user password or encrypted user file, unless duly authorized to do so.

L) Using the complaints procedure for any other purpose than registering complaints, for example jokes in bad taste, sending spam, criticizing a colleague without reason.

5. Special Rules of Conduct

5.1 Special Rules of Conduct for Employees Involved in Payments and Collections

Employees involved in collections may not collect their own debts, or those of businesses or individuals that they are related to, to avoid conflicts of interest. These transactions should be reported to a direct supervisor in advance, and should be collected by someone else authorized to do so (see Appendix 4).

Likewise, managers within these areas should not encourage their subordinates to collect their own debts, or those of businesses or individuals that they are related to, or that do not comply with all requirements, for example documents with incorrect signatures, without an endorsement, that have expired or are damaged.

5.2 Special Rules of Conduct for Employees Involved in Procurement

Employees involved in any procurement process should sign the declaration in Appendix 5, stating that the transaction does not create a conflict of interest for them.

5.2.1 Goods and Services Purchasing Process

Employees responsible for choosing goods and services during procurement processes should always select the best alternative in the interests of the Company, in accordance with the internal customer's requirements. This person should use comparison criteria, they should document their evaluation of the alternatives and record their final decision in writing.

5.2.2 Bidding process

Companies or individuals related to employees may not participate in tender processes in order to maintain business transparency. Therefore, companies or individuals are required to complete a signed statement declaring that they have no family ties with employees at Grupo Security and identifying their main shareholders. If a conflict of interest arises, it must be analyzed on a case-by-case basis and that tender evaluated under the same conditions as the remaining participants.

5.3 Special Rules of Conduct for Employees Involved in Sales and Marketing

5.3.1 Handling of Products or Services to Related Individuals or Companies

Employees in commercial divisions, or individuals or companies related to them, may not be part of their own customer, goods or service portfolio in order to maintain business transparency and avoid any conflict of interest. Consequently, all employees in commercial areas should complete the declaration in Appendix 6, stating all their holdings in related companies. This declaration should be updated at least once a year.

Therefore, if a family member or a Company related to an employee wants to receive a product or a service, they may do so through that employee. However, an unrelated employee should handle that portfolio. Furthermore, the acquisition process for these products or services should be the regular customer process and under the same conditions and market prices prevailing at the transaction date.

5.4 Special Rules of Conduct for Employees Involved in Asset Management Areas

Special rules of conduct for Grupo Security employees involved in asset management areas. These rules of conduct apply to employees of the following companies: Banco Security, Valores Security S.A., Corredores de Bolsa, Adm. General de Fondos Security S.A., Securitizadora Security S.A., Seguros Vida Security Previsión S.A., Factoring Security S.A., Inmobiliaria Casanuestra S.A., Hipotecaria Security Principal S.A. or to any other applicable company. These rules should be followed by all managers, administrators, legal representatives, operators, executives and all other employees that by nature of their position, functions or duties are affected by these rules.

5.4.1 Fundamental Principles

The following guiding principles are applicable, in compliance with the provisions of Chapter XXI of Stock Market Law (SML), to ensure the correct handling of insider information and to avoid conflicts of interest:

• Transparency: A transparent market is where prices can evolve and decisions be appropriately made, as a result of sufficient efficiency, competitiveness and timely and clear information among the participants involved.

• Confidentiality: Employees should exercise a duty of care and refrain from disclosing confidential or personal information. They should also refrain from making comments about such information that might directly or indirectly reveal its existence or content.

• Proper Use of Information: Employees involved in the market should refrain from using insider information for themselves or for a third party.

• Loyalty: Loyalty is understood to be the obligation of employees to be simultaneously full, frank, faithful and objective in their dealings with everyone involved in the markets, including customers and competitors. Loyal conduct is when employees:

1. Avoid conflicts of interest.

2. Avoid providing fictitious, incomplete or inaccurate information.

3. Avoid conduct that could cause errors in the purchase or sale of securities.

4. Avoid participating in transactions that are not under market conditions.

5. Refrain from participating or recommending any transaction based on privileged, confidential or public information owned by customers, employees, suppliers or any other third party belonging to companies outside the Grupo Security and its subsidiaries.

• Professionalism: Employees involved in the market should always operate on the basis of information that is serious, complete and objective. They should also provide advice on optimal order execution, in accordance with the customer's requirements.

• Compliance with the Law: Employees are required to comply with all legal provisions, in particular the duties with respect to information. It is very important that they communicate to the customer any unforeseen circumstances that could affect their contractual commitments.

• Equity: Employees involved in the asset management area should avoid transactions that favor some customers to the detriment of others.

• Healthy Competition: Employees should interact with other companies and institutions in the market in a suitable manner.

5.4.2 Specific Rules of Conduct within Asset Management Areas

The following general rules have been established in order to generate confidence in the business, avoid conflicts of interest and establish clear behavioral criteria for employees involved in market transactions. Employees should:

• Not cause uncontrolled movements in quoted prices or in market return rates.

• Take due care when receiving or executing buy and sale orders for securities.

• Take care when proposing, discussing and closing any business, to ensure that the customer correctly understands the nature, scope and conditions of the transaction, in particular the following:

• A clear understanding of the product or proposed transaction.

• A mutual understanding of all the elements necessary to close the transaction.

• A clear understanding of the risk inherent in the transaction.

• Register all their transactions in the registers required by law and promptly send the corresponding official documentation to interested parties.

• Never spread alarmist or biased rumors based on insufficient data.

• Avoid participating in practices that directly or indirectly create false conditions of supply or demand that influence market prices or that are intended to prevent, restrict or distort fair competition.

• Be independent when conducting business, freely able to accept or reject requests for their services without needing to explain their reasons for doing so.

• Never disclose false information in order to influence market prices.

• Never sell products or services with the sole purpose of generating commission or income without any real benefit for the customer.

• Keep their professional activities confidential with respect to third parties, unless expressly authorized by the person concerned, or when required by the Constitution and the law.

• Conduct business in such a manner that prevents the contracting parties from committing errors.

• Refrain from providing background information to a third party who has no right to receive it or based on such information provide advice on the purchase or sale of a market security.

• Purchase or trade issued, endorsed or accepted securities or those whose emission is managed by companies that are at risk of bankruptcy, or their affiliates or subsidiaries, without the corresponding authorization.

• Fully identify customers to prevent their transactions from being used in money-laundering, terrorism financing, bribery or other illegal activities. They should report any suspicious circumstances to the Company Compliance Division or the Corporate Compliance Division and collaborate with the competent authorities as required.

• Avoid executing instructions that are contrary to current regulations or good market practice.

• Never participate in decision-making or represent parties when involved in any kind transactions that are related or linked in some way to their personal or family interests.

• Never abuse a dominant position in order to obtain better conditions than those available on the open market.

• All market transactions should be executed in compliance with the current relevant rules, regulations and standards.

5.4.3 Handling Insider Information

Any employee within an asset management area with access to insider information should comply with Article 165 of SML, in order to preserve the principle of equal access to information by the participants, secure market transparency and avoid conflicts of interest. They should:

• Avoid using for their own benefit or that of third parties insider information about securities, or purchasing or selling such securities, for themselves or third parties, directly or through anyone else.

• Avoid using such information to make profits or avoid losses, through any transaction involving such securities or with instruments whose returns are determined by such securities.

• Never communicate such information to third parties, unless within the normal course of their duties.

• Never recommend that a third party purchases or sells such securities or makes someone else do so on the basis of this information.

However, employees can carry out transactions using insider information on behalf of unrelated third parties provided that the order and the specific transaction conditions come from the customer, without the advice or recommendation of a broker, and the transaction complies with all our internal standards in accordance with Article 33 of SML.

Incompatible Business or Abuse of Position:

Employees should avoid using Company information, resources, and infrastructure, such as equipment, systems, and communication channels, in transactions that are within their authority but that benefit themselves or a third party, or are incompatible with Company's objectives, regardless of whether they are expressed in a direct or indirect contract or transaction.

Article 240 of the Criminal Code, amended by law 21,121, also penalizes the director or officer of a corporation that takes a direct or indirect interest in any negotiation, act, contract, transaction or procedure involving the corporation, thus failing to comply with the conditions established by law, as well as any person governed by rules regarding duties established for directors or officers of these corporations.

Employees, directors and managers must refrain, under the same circumstances, from giving or letting an interest be taken by, when they should have impeded it, their spouse or civil partner, a relative of any degree in a straight line or up to the third degree in a collateral line, whether by blood or affinity.

They must also refrain from, under the same circumstances, giving or letting an interest be taken by, when they should have prevented it, third parties related to them or their spouse or civil partner, a relative of any degree in a straight line or up to the third degree in a collateral line, whether by blood or affinity, or corporations, partnerships or companies in which they, those third parties or other persons exercise powers of administration in any form or have a corporate interest, which must be greater than ten percent if the company were a corporation.

Misappropriation:

Employees must refrain from, for their own, the Company's or third-party benefit, appropriating or embezzling money, goods or any other tangible object that has been received in custody, commission or management or for any other reason that produces an obligation to hand it over or return it.

Unfair administration:

Employees must refrain from exercising any abuse of powers to dispose, on behalf of or obligate another individual or legal entity, executing or omitting actions manifestly contrary to the interest of the owner of the assets concerned.

5.4.4 Conduct that Breaks the Law

Conduct that violates the terms of this Code of Conduct, in accordance with Articles 52 and 53 of Chapter VIII of SML, is as follows:

• Trading securities for the purpose of stabilizing, fixing or artificially altering prices. However, price stabilization may be carried out in accordance with the general rules issued by the Superintendency of Securities and Insurance, and only to complete a public offering of new securities or previously issued securities that had not been part of a public offering.

• Issuing fictitious quotations or execute fictitious transactions for any security, whether open market transactions or through private negotiations.

• Executing transactions, inducing or attempting to induce the purchase or sale of securities, regardless of whether they are regulated by the SML, using any misleading or fraudulent means.

5.4.5 Corporate Transactions

No person within asset management areas should execute corporate transactions that are detrimental to the interests of their customers. When a conflict arises between the interests of a customer and the Company, those of the customer shall prevail.

Therefore, no person within an asset management area should buy securities on behalf of the Company when one of their customers has submitted a buy order that can be met by purchasing the same securities on this date.

Similarly, no person within an asset management area should sell or buy securities from their own portfolio to a customer, when another customer has submitted a sell order that can be met by matching it to the buy order received on this date.

No person within an asset management area should sell or buy securities on behalf of the Company under better conditions than those for pending buy or sale orders for the same securities on behalf of their customers.

Finally, no person within an asset management area should buy securities on behalf of the Company for which customers have submitted sale orders, or sell from their own portfolio securities for which customers have submitted buy orders, without the express authorization of those customers. These transactions should be carried out at market prices and following the stock market procedures established for this purpose.

5.4.6 Conduct when Executing Personal Transactions

Employees with an asset management area can personally invest in financial instruments, such as investment funds, mutual funds, Central Bank and Treasury instruments, fixed-term deposits and repo agreements, either for their own account or for equivalent personal transactions (see 5.4.7) using any broker.

However, they can only buy and sell shares that are traded on Chilean stock exchanges and debt instruments such as corporate non-banking bonds for their own account or for equivalent personal transactions (see 5.4.7) using one of the companies within Grupo Security. This rule maintains market transparency and avoids speculation and the misuse of insider information. Furthermore, these transactions should be carried out by a different employee or the relevant manager.

Other transactions not related to the employee's position should be carried out at current market conditions on that date.

Other transactions not related to the employee's position should be carried out at current market conditions on that date.

When the transaction or investment is carried out at a financial institution other than Grupo Security, the employee must report this fact to the respective Company using a form available on the Intranet, any other channel, or request it from the Compliance Officer, with a copy to their direct supervisor.

5.4.7 Equivalent Personal Transactions

Equivalent personal transactions are listed below:

• Those done for the employee's spouse, regardless of their marital agreement.

• Those done for their dependent children, regardless of where they live.

• Those done for a Company directly owned by the employee or indirectly owned through other individuals or legal entities with an interest greater than 10% in the capital or profits of that Company.

5.4.8 Conflicts of Interest in Personal Transactions

Employees within an asset management area should not execute personal transactions detrimental to the interests of Grupo Security customers. When a conflict arises between the interests of a customer and employees, those of the customer shall prevail.

Therefore, an employee within an asset management area should not personally buy securities when a Grupo Security customer has submitted a buy order that can be met by purchasing the same securities on this date.

An employee within an asset management area should not personally sell or buy securities under better conditions than those for pending buy or sale orders for the same securities on behalf of Grupo Security customers.

Therefore, an employee within an asset management area should complete a form (see Appendix 6), stating their financial situation and any individuals or legal entities that meet the description in the previous point, in order to avoid conflicts of interest and the abuse of insider information. This form

should be updated annually, or every time one of these persons or entities change. This form should be sent to the Compliance Officer, who must monitor the participation of individuals and legal entities related to employees in transactions carried out through Grupo Security and the changes in the financial situation of all employees within an asset management area.

5.4.9 Settlement and Transaction Matching

Employees should not execute any personal transaction or equivalent personal transaction where the counterparty is a Grupo Security Company, without having sufficient funds or securities to promptly comply with the corresponding obligations on the settlement date.

Therefore, employees, including related persons referred to in point 5.4.7, should never match transaction balances whose settlement dates do not match. These transactions should always be settled in full as they fall due.

5.4.10 Conduct for Personal Transactions Associated with Various Instruments

Rules of conduct for personal transactions in markets for fixed income instruments or equities and for personal transactions in foreign exchange markets (purchase/sale of foreign currency)

The Company has established clear rules for personal transactions involving fixed-income instruments or equities, to facilitate these transactions, to maximize market transparency, seriousness and security and to avoid conflicts of interest. Therefore, employees within asset management areas should comply with the following:

A) Securities acquired by employees should never be sold during the same session or day that they were purchased. The CEO, or their designee, may lift this prohibition under justifiable circumstances. Subsequently this transaction should be reported to the Board.

B) Furthermore, the CEO, or their designee, may decide that securities acquired by employees may not be sold for a minimum period from their purchase date. Subsequently this transaction should be reported to the Board.

C) The minimum period before securities can be sold shall be **10 CALENDAR DAYS** from their purchase date.

Rules of conduct for personal transactions in the futures market or derivative personal investments in mutual funds

Employees, and anyone related to them referred to in point 5.4.7, entering into any personal futures or derivative contract, such as a simultaneous, fixed-income forward, inflation forward, short sales or options contract, with a Grupo Security Company should have express authorization from the CEO, or their designee. They should submit the respective guarantees in the same manner as that required for unrelated third parties, and subsequently inform the Board, in order to secure maximum market transparency, reliability and security and avoid conflicts of interest.

Until employees within asset management areas, and anyone related to them referred to in point 5.4.7, have obtained the relevant written permission, they should not enter into personal contracts with a Grupo Security company. Moreover, the amounts involved should not exceed the limits defined by the Employee Credit Policy prepared by the Corporate Culture Division and approved by the Board.

Furthermore, the futures or derivatives transactions carried out by employees within asset management areas, and anyone related to them referred to in point 5.4.7, should be performed by strictly complying with the deadlines established by the respective stock exchanges or other regulatory bodies.

However, the minimum term required for transactions described in the preceding paragraph shall be 30 calendar days from the execution date and they must never be paid in advance or prepaid while valid.

Rules of conduct for personal investments in mutual funds

Employees within an asset management area, and anyone related to them referred to in point 5.4.7, who invests in any of the funds administered by a Grupo Security Company should strictly adhere to the corresponding rules, procedures and regulations.

5.4.11 Formalization of Orders

Customer orders always need to be in writing or use any other authorized procedure that is legally recognized as normal admissible practice. Orders can also be sent using other means, provided they can be located and identified through electronic voice or data records. The latter should be included in an order receipt file or contained in computer files.

6. Employee Termination

All employees whose contractual relationship with the Company is voluntarily or involuntarily terminated should abide by the following:

• All intellectual property created by the employee remains the property of the Company.

• The resources provided by the Company to enable employees to fulfill their daily activities should be formally returned to their direct supervisor or whoever replaces them. This should be evidenced in writing using the Declaration of Items Returned Form (see Appendix 7), and a copy should be kept. This should include mobile telephones and demand accounts, credit cards, etc.

• The Company email account enables employees to fulfill their daily activities and remains the property of Grupo Security. Therefore, once employees have left the Company they cannot keep it.

• All internal or confidential information regarding Company customers, suppliers, etc., should not be disclosed once employees have left the Company.

Further information is contained in the Information Security Policy, particularly the Human Resources Security Standard.

7. Reporting Events and Irregularities

All employees are obliged to immediately report to their direct supervisor any illegal or fraudulent conduct that comes to their attention, which might reasonably be considered a crime, a significant

violation of the law, dishonest, a misappropriation of funds or anything of value belonging to the Company, inappropriately accounting for Company assets or liabilities, a violation of trust, or any other conduct that could seriously affect the reputation of the Company and violate this Code.

However, if there are no specific guidelines in the Code of Conduct or other Company publications regarding a particular situation, employees should initially contact their direct supervisor, who should gather all the corresponding background information and inform the Company Compliance Officer.

If the situation cannot be resolved, or you feel uncomfortable reporting violations of this code to people within your department, you may wish to contact the Corporate Culture Division using the e-mail: culturacorporativa@security.cl or the Corporate Compliance Division using the e-mail: cumplimientocorporativo@security.cl or utilize other channels of communication set forth in manuals or policies.

It is emphasized that every effort must be made to keep the identity of any employee that reports violations of this code strictly confidential in order to avoid any potential retaliation.

Finally, if an internal investigation is required, all employees should collaborate and disclose everything they know when requested to do so.

8. Control and Monitoring

The following measures shall ensure adequate and sufficient control.

• The Internal Audit Division must review and monitor conduct with the aim of verifying compliance with this code.

• Back office teams must regularly send reports on all the personal transactions performed by employees in asset management areas to the company Compliance Officer, who must ensure that they comply with the provisions established in the Code of Conduct with respect to minimum time limits, the conditions attached to such transactions, etc.

• An Ethics Committee must be established within the internal control framework, to monitor compliance with the rules of this Code, other complementary rules, and analyze violations. This committee must be composed of representatives from: Corporate Culture, Corporate Internal Control, etc. (see point 8.1)

• Finally, managers throughout the Company are responsible for ensuring that their subordinates sign the Acceptance of the Code of Conduct Declaration Form.

8.1 Ethics Committee

The Ethics Committee is responsible for ensuring the correct distribution and application of the Code of Ethics and Code of Conduct, which requires them to:

• Promote the fundamental values, principles and behavior described in the Code of Ethics and the Code of Conduct.

• Assist the Crime Prevention Officer to develop, implement and operate the Crime Prevention Model.

• Receive consultations.

• Assist in the resolution of conflicts arising from violations of the Code of Ethics or the Code of Conduct.

• Hear and resolve complaints as indicated in this Code, while respecting the rights of employees, in particular the right to be heard, to defend themselves, and that judgments against them are well founded.

• Report special cases to the appropriate authorities.

• Propose updates and amendments to the Code of Ethics or the Code of Conduct.

• Review requests to clarify specific situations.

• Issue any necessary circulars and instructions, to ensure compliance with the Code of Ethics or the Code of Conduct.

The Ethics Committee shall have the following members:

- Controller
- Corporate Culture Manager
- General Counsel
- CEO of the company

Any employee may report infringements to this Code or the Code of Ethics using the means provided for this purpose (point 7), which must always be treated with the utmost confidentiality.

9. Violations of Regulations and the Code of Conduct

Any employee who violates any of the standards described in this code is understood to be in violation of the Code of Conduct. Therefore, they shall be subject to disciplinary proceedings, which shall depend on the severity of the violation and may involve terminating their employment. If applicable, the situation may be reported to the relevant authorities.

Questions relating to the content of this Code can be resolved by contacting the Corporate Compliance Division using the email: cumplimientocorporativo@security.cl.

10. Acknowledgment and Commitment to the Code of Conduct

All employees are required to complete and sign the "Acceptance of the Code of Conduct Declaration Form" (see Appendix 8), which should be sent to the Corporate Culture Division.

Appendix 1:
The Confidentiality Standard

1. Objective and Scope

The Company is responsible for information, and aims to secure the availability, confidentiality and integrity of information, to regulate the proper use of its physical and technological resources, and to protect intellectual property when appropriate.

Its scope includes the logical security and physical security at all those facilities where it has technological resources, including at external companies that support Company information services.

This standard applies to everyone authorized to use the Company's Information Systems and is an integral part of the Code of Conduct.

2. Definitions

"user" means any person who is authorized to use the Company's Information Systems. This includes any permanent employee, temporary fixed-term employee, and those working for companies contracted to provide services to, or on behalf of, the Company.

"Information Systems" or "Company's Information Systems" means computers, printers, networks, phones, software packages, packaged or internally developed applications, Internet access, among others, which a user can access in the normal course of their duties within the Company or when providing a service to the Company.

3. Responsibilities

Users are responsible for complying with the rules described in this Code.

Managers, deputy managers, heads, delegated administrators and supervisors are responsible for ensuring that all employees working in their divisions understand and comply with this Code.

Furthermore, users share the responsibility for keeping information secure. Therefore, if any user suspects that information has been incorrectly used or a policy contained in this Code has been violated, this should be immediately reported to a supervisor, delegated security administrator, the Policy Management Division at email: gestionnormativa@security.cl and the Corporate Culture Division at email: culturacorporativa@security.cl.

4. Consequences of a Violation

The Corporate Culture Division supported by the Security Division reserves the right to define the misuse of Information Systems, and any other user conduct that is not in accordance with the provisions of this Code.

Any employee who violates any of the standards described in this code is understood to be in violation of the Code of Conduct. Therefore, they shall be subject to disciplinary proceedings, which shall

depend on the severity of the violation and may involve terminating their employment. If applicable, the situation may be reported to the relevant authorities.

Failure to complete the Security and Cybersecurity courses or to comply with the Security information issued through formal communication channels may be sanctioned.

5. Correct Use of Information Systems

The Company provides Information Systems and electronic tools, such as Internet access, e-mail service and remote access to the Company's email, to enable the business to function. Further information is contained in the Information Security Policy, published on the Intranet, particularly the Communications Management Standard.

The Company's Information Systems, or those to which a user has access, should not be used for external business purposes, or for charitable, political or religious organizations, without prior written authorization from the Corporate Culture Division.

Also the following conduct is strictly prohibited:

• Illegal activities of any kind.

• Betting or any form of gambling.

• Performing collections, unless previously approved by the Corporate Culture Division.

• Activities for personal profit.

• Sending obscene, vexatious or abusive messages.

• Unethical activities.

• Sending mass emails or mail chains.

• Voluntarily creating, transmitting or receiving offensive, defamatory, threatening or abusive material, which includes but is not limited to comments based on race, nationality, gender, sexual orientation, age, disability, religion or political belief.

• Unauthorized and deliberately damaging computer networks or systems to impair their performance.

• Negligently or intentionally introducing a virus or destructive program into Company or external computers, workstations, systems or networks.

• Deciphering or attempt to decipher any system, user password or encrypted user file, unless duly authorized to do so.

6. Information Confidentiality and Security

The Company considers its information to be one of its most important business assets. All employees ae responsible for protecting the confidentiality, integrity, and availability of information. Further information is contained in the Information Security Policy, published on the Intranet, particularly the Assets Management Standard.

To ensure that Company information is adequately protected, user access to information must be based solely on the responsibilities of each user, without engaging in discriminatory practices.

"Confidential Information" contains, but is not limited to, the following: all technical and non-technical information relating to the business of the Company, its customers, suppliers, trademarks, invention patents, profit models, industrial designs, techniques, sketches, drawings, know-how, processes, machines, equipment, algorithms, computational programs, documents, and formulas, provided they relate to current products and services or those that the Company may develop in the future, research, experimental work, development, design and engineering details and specifications, financial information, materials requirements, purchasing, manufacturing, customer lists, studies, strategies, market information, sales and marketing.

The following conduct is prohibited:

• Altering or amending information, except where required by the user's job description. Any alteration that is not made using the operational processes and systems defined for this purpose must be formally justified.

• Any attempt to gain access to unauthorized information.

• Using data-processing facilities or computing resources in a manner inconsistent with the user's job description or incompatible with the Code of Conduct.

Information Systems and their contents are Company assets and should be protected against unauthorized access, disclosure, amendment or destruction. Managers are responsible for ensuring that information systems and technological tools are properly used.

The Company reserves the right to monitor the use of computer systems, to read and copy all the data contained on workstations at any time, with or without prior notice, unless expressly prohibited by law, through the Internal Audit Division supported by the Security Division.

Monitoring may take place using internal administrative procedures, or during internal or external audits or by legal mandates.

7. User Login

The use of other people's ID (user name) and password to access the Company's systems, assets or services is expressly prohibited. Disclosing your password or sharing it with others so that they can log in on your behalf is also prohibited. Any person involved in this practice may be sanctioned by the Company.

All computer systems, networks and applications, including packages purchased by the Company, have access control functions that enable them to identify and uniquely restrict the privileges for each user. Further information is contained in the Information Security Policy, published on the Intranet, particularly the Access Control Standard.

Managers can request an information systems user profile that matches the user's job description, in accordance with the user account creation process. Once access is granted, users are expected to use these systems in a responsible manner at all times.

Managers, supervisors or delegated security administrators are responsible for initiating the "user account creation" process for those staff in their divisions that require access. All access requests without exception require the respective form to be completed in accordance with established procedure.

The Company monitors all active computer service access accounts. These accounts will be blocked if unused for 60 days and any accounts unused for 90 consecutive days will be deleted, with the exception of accounts for employees on medical leave, which will remain inactive until their return.

8. Handling Confidential Information

Confidential Information belongs exclusively to the Company. Further information is contained in the Information Security Policy, published on the Intranet, particularly the Asset Management Standard.

Confidential information belongs to the Company and is specially protected, according to Article 8 of Law 17,366 on Intellectual Property, and Articles 68 onwards of Law 19,039 on Industrial Privileges and the Protection of Industrial Property Rights, notwithstanding any other relevant laws or regulations.

Employees are expected to take proper precautions to prevent unauthorized persons from reading or amending data during an active working session under their user account.

Employees should terminate their work session, log out or lock their workstation when leaving it unattended. Users are obliged to use a corporate screen saver with password.

Every electronic document that contains confidential information should be saved to a secure area, ideally backed up and additionally could be protected from unauthorized use by using a password. Consult with your supervisor on how to guarantee information is protected.

Copies of confidential information that have been printed by any means should be identified as such and stored in a secure place to avoid unauthorized access. The responsibility for the foregoing rests with the information's owner.

Employees should promptly retrieve all printed material that contains confidential information from printers, to avoid unauthorized access.

All confidential information should be backed-up regularly. Employees are responsible for requesting and ensuring that critical data stored on their work stations is backed up. The Company is responsible for providing the necessary mechanisms to properly back-up and store the backed-up information.

All surplus copies of information generated during the copying, printing, microfilming, micro-fiching, etc., should be promptly destroyed in a safe manner in accordance with the importance of the information. This applies to both electronic and printed copies. The destruction of private and confidential data requires physical documents to be shredded.

Once the electronic information that requires deletion has been identified, all electronic copies should be eliminated from the systems.

All the information contained in magnetic data storage devices, such as hard drives or flash drives should be eliminated before they are exchanged, serviced or retired. This elimination should be secure, either by overwriting or reformatting the device.

9. E-mail and Telephones

The main objective of e-mail and telephone services is to broaden commercial communications for the Company. Complementary information is contained in the Information Security Policy, published on the Intranet, particularly the Asset Management Standard and the Communications Management Standard.

User's Company e-mail addresses are owned by Grupo Security and regardless of their content, are subject to appropriate controls within the provisions of the law. Appropriate language and good manners should be used in e-mails and in all other oral or written business communications.

Offensive, degrading or defamatory messages are prohibited. Users are responsible for content sent via e-mail or over the Internet regardless of the format, including text, sound or video. All messages should comply with the relevant legal regulations in relation to copyright, trademarks and intellectual property. Messages should include the identity of the user that sent them.

The Company reserves, in accordance with the law, the right to access e-mail, understood as an information system provided by the Company to carry out the duties for which the employee was hired. For the aforementioned reasons, the Company reserves the right to make copies of backups and archives of information from e-mails.

It is recommended to avoid using an e-mail address provided by the Company for personal matters, and its use is the sole responsibility of the employee.

Accessing or attempting to access the e-mail of another user without written permission from the Company’s operational risk manager is prohibited.

Access to corporate e-mail on personal devices implies that the employee has agreed to install security mechanisms put in place by Security to safeguard and protect the Company's and/or its customers' information.

10. Internet Use

Internet access is granted to Company employees, suppliers, contractors and customers, as required by the business. The Company reserves the right to restrict access to the Internet as it deems appropriate and without engaging in discriminatory practices (For more information, see the Information Security Policy posted on the Intranet, particularly the Communications Management Policy).

Acceptable Internet use to perform job duties includes, but is not limited to:

• Communicating between employees and external persons for commercial purposes.

• Reviewing vendor web sites for information on products.

• Searching for regulatory or technical reference information.

• Conducting research requested by management or the Corporate Culture Division.

Users should avoid any activity that is incompatible with the Code of Conduct. The "Communications Management Standard" published on the Corporate Intranet, indicates some specific Internet uses that are strictly prohibited. Further specific uses that are prohibited include, but are not limited to:

• Accessing information that is not within the scope of an employee's job description.

• Using any means to obtain unauthorized access to an internal or external computer system or network.

• Transmitting confidential information belonging to the Company without using the proper controls.

• Betting or any form of gambling.

• Visiting conversation sites or chatting, except when authorized to meet business requirements and validated by the Security Division.

• Using technology available on the Internet that is not required for commercial purposes, such as streaming music, videos or television.

Any file downloaded from the Internet should be scanned to avoid the spread of computer viruses. Usually virus detection software installed on each computer automatically performs this scan. Every user is responsible for ensuring that it functions correctly and is up to date. If a user suspects that a file contains a virus, or has reason to believe that it represents a specific risk, they should contact soporte@security.cl for support before downloading that file.

Information that users send, view or download from the Internet may be protected by copyright law. Reproducing protected information is only permitted if used in a fair manner and authorized by the manager, or if expressly permitted by the copyright owner.

Under no circumstances should computers connected to Company networks be simultaneously connected to the Internet through a modem. Further information can be found at Section 1.14 of the Communications Management Standard published on the Corporate Intranet.

Questions about acceptable Internet use should be addressed to the Policy Management Division at e-mail: gestionnormativa@security.cl

11. Protection from Computer Viruses (See Unlicensed Software Installed on Grupo Security Equipment)

Viruses are computer programs that self-replicate and spread to various data storage media, such as disks or magnetic tapes or through a network. They can cause damage ranging from slower response times and unexplained file loss, through to the total failure of a computer system. Controls should prevent a virus from entering computer systems and the Company's corporate network, thus minimizing the damage caused by viruses. Further information is contained in the Information Security Policy, published on the Intranet, particularly the Communication Management Standard.

In general, users should:

• Refrain from installing programs or external software that are not an integral component of their authorized systems.

• Delete email messages of unknown origin. Users should never open any attachments included in such e-mail messages.

• Ensure that virus protection software is functioning correctly on their desktop or laptop, which should never be uninstalled.

• Stop using their equipment if they suspect that it has been infected with a virus, and immediately inform the help desk on extension: 4357.

• Verify that electronic files do not contain viruses before sending them to third parties, to avoid exposing the image of the Company to such risks.

12. Company Telephones

The Company offers telephones to support Company business activities. Personal calls are permitted if charged at local call rates, provided that their frequency and duration are reasonable. Complementary information is contained in the Information Security Policy, published on the Intranet, particularly the Asset Management Standard.

The Company must provide access to international calls for those employees who require these services to fulfill their duties. Users of IP telephony must be assigned a personal secret code that allows them to carry out long distance calls from any telephone extension with this facility.

The Company reserves the right to monitor calls, including the number called, the date, time and duration of the call, and request that the cost be reimbursed for those calls considered to be unconnected with business activities.

13. Mobile Telephones

The Company must provide mobile telephones to those employees who require one to fulfill their duties. The Company reserves the right to audit this service when necessary, including the number called, the date, time and duration of the call, and request that the cost be reimbursed for those calls considered to be unconnected with business activities. Complementary information is contained in the Information Security Policy, published on the Intranet, particularly the Asset Management Standard.

14. Remote Access

"Remote access" significantly increases the risk of unauthorized access to the network and computing infrastructure, so requires strict access and control procedures. Further information is contained in the Information Security Policy, published on the Intranet, particularly the Standard for the Organization of Information Security and the Mobile Devices Security Standard (BYOD). Users should comply with the following basic guidelines:

A) External lines should never be connected to Company technological resources, such as digital, analog or cable connections, without prior approval from the appropriate Division and validation by the Security Division. All requests to install analog lines, modems or modem access should be in writing to the Security Division, who must submit them to the request approval process.

B) Under no circumstances should computers or devices connected to the Company network be simultaneously connected to external networks through a modem. This situation causes a security

violation that may allow unauthorized access or allow destructive programs to enter the Company's network and computer infrastructure.

C) Access to Company networks using a Virtual Private Network or VPN connection via the Internet should have the appropriate controls and configuration to ensure security is sufficient. This issue should be addressed to the Security Division.

Other connections to the Company's Information Systems require approval from the Security Division. Access to Company networks through personal computers owned by employees is prohibited, unless prior written authorization has been obtained from the manager and the Corporate Culture Division and this has been validated by the Security Division.

15. Computing Hardware

Users should not move computing equipment, desktop computers, docking stations, fax machines, network servers, etc. Users should not remove the "fixed asset" labels on computing equipment. Complementary information is contained in the Information Security Policy, published on the Intranet, particularly the Asset Management Standard.

When laptops are not being used, where possible they should be kept in a lockable cabinet or locked to a workstation. When employees are required to undertake business trips they should take appropriate measures to safeguard computing equipment, such as not leaving it unattended, or in hotel rooms, or with any other person. During flights laptops should be carried as hand luggage.

Users are strictly forbidden from deleting, adding or amending the hardware configuration of the Company's equipment.

If employees lose or are robbed of equipment as a result of violations to Company regulations, they should bear the cost of replacing such equipment.

16. Mobile Devices

Having access to information at any time and place has now become part of our daily lives. Mobile devices, such as iPhones, iPads, tablets, Blackberrys and Smartphones, can be connected and synchronized with some corporate applications, such as email, calendars and contacts, and can enable documents to be retrieved, edited and stored. This functionality helps the business to stay competitive in today's world, and can increase productivity.

Therefore, minimum security safeguards for these devices have been established and detailed in the Policy on the Mobile Device Security Standard (BYOD).

Appendix 2 (Part A): Donations Form

Company (area) making the donation

Name of the person making the donation

Name of the person authorizing the donation

Name of the institution receiving the donation

Name of the person receiving the donation at the receiving institution

Donation type

- ☐ Tangible (e.g., Materials)
- ☐ Intangible (e.g., Hours of work)

Donation amount (Attach a copy of supporting documentation: receipt, invoice, etc.)

Currency (pesos, UF, US dollars, etc.)

Other (Comments)

Donation date (dd/mm/yyyy)

Signature of the person making the donation

Signature of the person authorizing the donation

Appendix 2 (Part B):
Declaration of Donation Receipt Form

I,_____, Chilean National ID_____,
represent the institution _____,
and declare that we have received from_____
the following donation: _____
_____

which shall be used for the following purposes: _____
_____
_____
_____

Consequently, as a representative of _____,
I commit to ensuring that the donation is used for these purposes.

In……, on……of……20……..

_____
Signature of the person representing the institution

Appendix 3:
Expense Reimbursement Form

I,_____, Chilean National ID_____,
declare that I have received from _____
the sum of _____ for the following expense:_____
_____,
which took place between _____ 20____ and _____ 20____.

I declare that the details of the costs incurred are as follows:

Receipt or invoice number	Date	Description	Currency	Amount
TOTAL				
BALANCE PAYABLE				
BALANCE RECEIVABLE				

All the supporting documentation for these expenses is attached.

In ……, on……of……20……

_____

Signature

Appendix 4:
AUTHORIZATION TO COLLECT, PAY OR PURCHASE GOODS OR SERVICES WITHIN THE DIVISION FORM

I, _____(*name of supervisor*), Chilean National ID _____, understand and authorize the following transaction: (*e.g.: airline ticket purchase, cashing personal checks, etc.*) _____

_____

on behalf of _____ (*name of the employee who pays, collects or purchases a product or service*), to be carried out by _____ _____*(name of the person authorized to carry out the transaction).*

I declare that this transaction shall be carried out in accordance with established procedures.

In _____, on_____of_____20_____

_____

Supervisor's Signature

Appendix 5:
Declaration of Interests for Procurement Division Form

I_____, Chilean National ID_____,
am aware of the provisions of the Code of Conduct, the need to maintain business transparency and avoid all conflicts of interest. Therefore, I declare that I do not have any interest in the following transaction:

_____
_____.

Likewise, I declare that I have no family relationship or ownership interest in the companies or with the individuals involved in this transaction.

In _____, on_____of _____ 20_____

_____

Signature

Appendix 6:
Declaration of Related People and Interests in Companies Form

I,_____, Chilean National ID_____, am aware of the provisions of the Code of Conduct, the need to maintain business transparency and avoid all conflicts of interest. Therefore, I declare that I have an ownership interest in the following companies:

Name	Company Name	Taxpayer ID	Ownership %

Furthermore, I declare that I have a direct blood relationship, e.g., spouse, parents, children, etc., with the following people:

Name	Taxpayer ID	Relationship

In ……., on…… of……20……

_____

Signature

Appendix 7 (Part A):
Declaration of Items Received Form

I,_____,Chilean National ID:_____, declare that I have received from_____ (*name of company*) to enable me to fulfill the responsibilities of my position as _____the following items (*mobile telephones, computers, notebooks, landline telephones, PC monitors, vehicles, corporate credit cards, keyboards, IDs, keys, passwords, etc.)*:

	Item	Quantity	Model
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Furthermore, I declare that I shall carefully use these items, ensure that they are working properly and use them only for the purposes for which they are intended.

In ……, on……of……20……

_____

Signature

Appendix 7 (Part B): Declaration of Items Returned Form

I, _____Chilean National ID_____, formally return all the items received _____ (*name of company*) while I performed the role of _____
with the aim of maintaining good relations and ensuring that these items are not lost.

The items that I formally return in writing are (*mobile telephones, computers, notebooks, landline telephones, PC monitors, vehicles, Corporate credit cards, keyboards, IDs, keys, passwords, etc.*):

	Item	Quantity	Model
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

In ……., on…… of……..20……

_____
Signature

Appendix 8:
Acceptance of the Code of Conduct Declaration Form

First and middle names: _____

Last name(s): _____

Chilean National ID: _____

Professional address: _____

Telephone and Ext: _____

Company: _____

Job title: _____

Division: _____

I declare that I have received, understood and accepted the "Code of Conduct" and that I have a copy. Likewise, I confirm the accuracy of the declared information and formally commit to complying with the regulations therein.

I understand that the "Code of Conduct" is an integral part of my employment contract and therefore represents an extension thereof.

In ……., on…… of…… 20……

_____

Signature

Appendix 9:
Crimes in Law 20,393 and its Amendments

Money Laundering: Any attempt to hide or conceal the illegal origin of property, knowing that it came from crimes supporting illicit drug trafficking, terrorism, weapons trafficking, child prostitution, kidnapping, corruption, etc. Likewise, anyone acquiring, owning, possessing or using such assets with the intention of profiting from them who is aware of their illicit origin when they are received.

Terrorism Financing: Any person who requests, collects or provides funds by any means for use in any of the terrorist crimes identified in Article 2 of Law 18,314.

- Seizing or attacking public transport while in service.
- Attacking the Head of State or other authorities.
- Criminal conspiracy to commit crimes of terrorism.

Bribing a Chilean or Foreign Public Official: This consists of offering, giving or consenting to give a public employee (domestic or foreign) an economic benefit or benefit of any nature to benefit them or a third party so that they:

- Performs a task that they are entitled to carry out, though in this case is not justifiable.
- Omits a task that they should carry out.
- Performs a task that they are not entitled to carry out.

Handling Stolen Goods: Any person who handles, transports, buys, sells, processes or markets any goods or animals that are received through theft or misappropriation, provided they know about their origin or should know of it. Likewise, the crime of handling stolen goods punishes any negligent behavior by anyone who acquires or possesses such goods.

Incompatible Negotiations: The law penalizes the director or officer of a corporation that takes a direct or indirect interest in any negotiation, act, contract, transaction or procedure involving the corporation, thus failing to comply with the conditions established by law, as well as any person governed by rules regarding duties established for directors or officers of these corporations.

Likewise, penalties will be imposed on these persons if, under the same circumstances, they gave or let an interest be taken by, when they should have impeded it, their spouse or civil partner, a relative of any degree in a straight line or up to the third degree in a collateral line, whether by blood or affinity.

The same will hold if these persons, under the same circumstances, gave or let an interest be taken by, when they should have prevented it, third parties related to them or their spouse or civil partner, a relative of any degree in a straight line or up to the third degree in a collateral line, whether by blood or affinity, or corporations, partnerships or companies in which they, those third parties or other persons exercise powers of administration in any form or have a corporate interest, which must be greater than ten percent if the company were a corporation.

Corruption Among Individuals: Any employee or representative that requests or agrees to receive an economic or other benefit, for themselves or a third party, to favor or for having favored in exercising their duties the contracting of one bidder over another.

Misappropriation: Those who, to the detriment of others, appropriate or embezzle money, goods or any other tangible object that has been received in custody, commission or management or for any other reason that produces an obligation to hand it over or return it.

Unfair Administration: Anyone charged with safeguarding or managing the estate of another individual or legal entity, or any part of it, by virtue of the law, an order from authorities or an act or contract, who inflicts damage, whether by abusively exercising their powers of disposal on behalf of them or binding them to do so, whether by executing or omitting any act that is expressly contrary to the interests of the owner of the affected estate.

Crime of Water Pollution (Article 136 of the Fisheries Act): The former criminal type of pollution in the Fisheries Act is replaced and now the following is punishable by law: an act committed by someone who, without authorization, in disobedience of their conditions or in violation of applicable regulations, dumps or orders someone to dump chemical, biological or physical pollutants that harm hydrobiological resources into the ocean, rivers, lakes or any other body of water. The associated penalty is minor imprisonment in its medium to maximum degree and a fine of 100 to 10,000 monthly tax units, notwithstanding the corresponding administrative sanctions.

Banned Products (Article 139 of the Fisheries Act): The processing, stockpiling, transformation, transportation, commercialization and storage of forbidden hydrobiological resources, as well as the elaboration, commercialization and storage of products derived from them, will be sanctioned with minor imprisonment in its minimum to medium degree, notwithstanding the corresponding administrative sanctions. In order to determine the penalty, the volume of hydrobiological resources resulting from the penalized conduct must be taken into consideration.

Illegal Fishing of Seabed Resources (Article 139 bis of the Fisheries Act): Whoever carries out extractive activities in areas where benthic resources are being managed without possessing the rights referred to in the final paragraph of Article 55 B of this law, shall be punished with minor imprisonment in its minimum to maximum degree. In the case of catches, the higher degree of the penalty must be imposed. The court must order the confiscation of diving equipment, boats and vehicles used to commit the offense.

Processing and Storage of Scarce Products (Collapsed or Overfished) Without Proving their Legal Origin (Article 139 ter of the Fisheries Act): It is a crime for anyone to process, prepare or store hydrobiological resources or products derived from them for which the legal origin is not accredited and that are resources in a state of collapse or overfishing, according to the annual report of the Undersecretariat of Fisheries. This crime shall be punished with minor imprisonment in its minimum to maximum degree and a fine of 20 to 2,000 monthly tax units. The same sanction will be applied to those who, as a seller registered by the Fisheries Service, market hydrobiological resources that are in a state of collapse or overfished, or products derived from them, without proving their legal origin.

In addition, due to the health emergency affecting the country, two new crimes have been added:

Failing to Observe Quarantine or Other Preventative Measures Mandated by Public Health Officials in the Event of an Epidemic or Pandemic: This penalizes those who force their workers to go to their workplaces in person when they are in quarantine or sanitary isolation. Article 318 ter of the cited Chilean Criminal Code textually states: "*Anyone who knowingly and with the authority to coordinate the work of a subordinate, orders them to attend their place of work when this is other than their home or residence, and the worker is in mandatory quarantine or isolation decreed by the health authority, will be punished with minor imprisonment in its minimum to medium degrees and a fine of ten to two hundred monthly tax units for each worker who has been ordered to attend.*"

Unemployment Insurance Benefits: This crime refers to situations where the benefits considered by this law are obtained fraudulently, and this can extend to legal entities, where these have not fulfilled their duties of oversight and supervision to avoid their perpetration by their owners, controllers, primary executives or representatives. *Article 14, Law 21,227* *www.bcn.cl/leychile/navegar?idNorma=1008668.*

All employees should take special care not to do anything that may be perceived as a crime and potentially risk making the Company responsible for this situation. Therefore, employees should avoid interacting with individuals or entities suspected of being involved in illegal businesses. They should be fully committed to complying with the Crime Prevention Regulations. They should report suspicious transactions that come to their knowledge as they carry out their duties to the Compliance Division.

Arms Control: Pursuant to this amendment, the penalties set forth in Law No. 17,798, Title II, on arms control, will be applied to the crimes contemplated in Law No. 20,393 for crimes or misdemeanors, in accordance with the provisions of Article 14, in consideration of the penalty assigned to each crime in the abstract.

The reform sets forth that the individuals or legal entities who have abandoned them, who have not communicated or reported their loss, theft or robbery in a timely manner, and those who have not updated the authorized location of the firearms, shall be jointly and severally liable for the civil effects of those illicit acts in which their firearms have been used (article 5, third paragraph). Such joint and several liability, in the case of legal entities, shall extend to both the legal entity and its legal representative.

Human Trafficking: On migration and foreigners, for which regulations were recently approved and took effect, the crimes of smuggling of migrants and trafficking in persons and others contained in Article 411 quater of the Criminal Code became part of those offenses that may also give rise to criminal liability of legal entities. "Article 411 quater.- Anyone who employs violence, intimidation, coercion, deception, abuse of power, abuse of the victim's vulnerability or dependence, or receives payments or other benefits to obtain consent from someone with authority to capture, transfer or receive people for any type of sexual exploitation, including pornography, forced work or services, servitude, slavery or similar practices, or for organ extraction, shall be punished with major imprisonment in its minimum to medium degree and a fine of fifty to one hundred monthly tax units. If the victim is a minor, even in the absence of violence, intimidation, coercion, deception, abuse of power, taking advantage of a situation of vulnerability or dependence of the victim, or the granting or receiving of payments or other benefits to obtain the consent of a person having authority over

another, the penalties shall be major imprisonment in its medium degree and a fine of fifty to one hundred monthly tax units. Individuals who promote, facilitate or finance the conducts described herein must be sanctioned as perpetrators of the crime."

Attack on the Integrity of a Computer System: Whoever hinders or prevents the normal operation, in whole or in part, of a computer system, through the introduction, transmission, damage, deterioration, alteration or suppression of computer data, shall be punished with minor imprisonment in its medium to maximum degree.

Unlawful Access: Whoever accesses a computer system without authorization or exceeding the authorization they have and overcoming technical barriers or technological security measures shall be punished with minor imprisonment in its minimum degree or a fine of eleven to twenty monthly tax units.

If the access was made with the intent to seize or use the information contained in the computer system, the penalty shall be minor imprisonment in its minimum to medium degree. The same penalty shall apply to the person who discloses the information to which access was obtained unlawfully, if it was not obtained by them.

In the event that the same person has obtained and disclosed the information, the penalty shall be minor imprisonment in its medium to maximum degree.

Unlawful Interception: Whoever unduly intercepts, interrupts or interferes with, by technical means, the non-public transmission of information in a computer system or between two or more of them, shall be punished with minor imprisonment in its medium degree.

Whoever, without due authorization, captures, by technical means, data contained in computer systems through electromagnetic emissions coming from them, shall be punished with minor imprisonment in its medium to maximum degree.

Attack on the Integrity of Computer Data: Whoever unduly alters, damages or deletes computer data, shall be punished with minor imprisonment in its medium degree, provided that this causes serious damage to the owner of such data.

Computer Forgery: Whoever unduly introduces, alters, damages or suppresses computer data with the intention that they be taken as authentic or used to generate authentic documents, shall be punished with minor imprisonment in its medium to maximum degrees.

When the conduct described in the preceding paragraph is committed by a public employee, abusing their office, they shall be punished with minor imprisonment in its maximum degree to major imprisonment in its minimum degree.

Reception of Computer Data: Whoever, knowing its origin or being unable but to know it, sells, transfers or stores for the same or any other illicit purpose, in any way, computer data resulting from the conducts described in articles 2, 3 and 5, shall suffer the penalty assigned to the respective offenses, reduced by one degree.

Computer Fraud: Whoever manipulates a computer system and causes harm to another through the introduction, alteration, damage or suppression of computer data or through any interference in the

operation of a computer system with the purpose of obtaining an economic benefit for themselves or for a third party.

Abuse of Devices: Whoever, in committing the crimes provided for in articles 1 to 4 of this law or of the conducts indicated in article 7 of law No. 20,009, delivers or obtains for its use, imports, disseminates or otherwise makes available one or more devices, computer programs, passwords, security or access codes or other similar data, created or adapted mainly for the perpetration of such crimes, shall be punished with minor imprisonment in its minimum degree and a fine of five to ten monthly tax units.

Timber and Other Related Theft: Law No. 21,488 amends the Criminal Code and the Code of Criminal Procedure in the following articles.

Article 448 septies
"Whoever commits robbery or theft of logs or timber commits the crime of timber theft and shall be punished with the penalties set forth in Paragraphs II, III and IV of this Section. When the value of the stolen timber exceeds 10 monthly tax units, a fine of 75 to 100 monthly tax units will also be applied. If the value of the stolen timber exceeds 50 monthly tax units or if the theft is the result of a systematic or organized procedure, the special investigative techniques provided for in Article 226 bis of the Code of Criminal Procedure may be applied.

Motorized or other vehicles, tools and instruments used in the commission of the crime shall be confiscated.

Article 448 octies
Anyone in whose possession logs or timber are found shall be punished for timber theft, with the penalties provided for in Article 446, 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.

Likewise, whoever falsifies or maliciously makes use of false documents to obtain guides or forms to illegally transport or sell timber shall be punished with minor imprisonment in its medium to maximum degrees."

Glossary

Group: All companies that belong to Grupo Security, whether subsidiaries or associates of Grupo Security S.A.

Employee: Everyone who belongs to a company, including permanent staff, temporary fixed-term staff and those working for companies contracted to provide services to, or on behalf of, that company.

MHIIM: The Manual for Handling Information of Interest to the Market. This Grupo Security internal document was approved by the Board on March 25, 2010, and is available on the Intranet.

Transactions: The generic name for regulated or unregulated business transactions carried out within or outside the Company.

Confidential Information: Any technical or non-technical information relating to any Grupo Security business, customer or supplier, including trademarks, invention patents, profit models, industrial designs, techniques, sketches, drawings, know-how, processes, machines, equipment, algorithms, computational programs, documents, and formulas, provided they relate to current products and services or those that the Company may develop in the future, research, experimental work, development, design and engineering details and specifications, financial information, materials requirements, purchasing, manufacturing, customer lists, studies, strategies, market information, sales and marketing.

Internal Information: Information of interest to the market that is not public knowledge and that could affect the answer to the following question: Is that information critical with regard to a particular business decision?

Conflict of interest: When a person faces various alternatives and some resulting outcomes are incompatible with their duties, though all comply with legal or contractual obligations. A conflict of interest exists when an employee can choose to benefit:

- Themselves or a customer.
- A third party linked to the Company or a customer.
- A managed portfolio or a customer.
- A third party linked to an employee of the Company or a customer.
- The business or market transparency.
- A managed portfolio or themselves.

SML: Stock Market Law 18,045.

Securities: (Article 3 SML) Any transferable instruments including equities, options to buy and sell equities, bonds, debentures, mutual fund units, savings plans, commercial papers and, in general, any debt or investment instrument.

Instruments: Publicly offered securities that can be traded on the financial market.

Personal transactions: Those transactions carried out by employees for their own benefit, with a Grupo Security company or another market entity as the counterparty.

Corporate transactions: Those market transactions carried out by asset management areas on behalf of the Company.