## 1. CLASSIFICATION: PUBLIC[1]

## 2. OBJECTIVE

This public version corresponds to an extract of the Corporate Information Security Policy of Viña Concha y Toro S.A. and its subsidiaries (hereinafter, the "Holding" or the "Company"). Its purpose is to communicate the general principles and corporate commitments regarding information security, without including all the controls, procedures, responsibilities and internal provisions contained in the current corporate policy.

The Information Security Policy of Viña Concha y Toro S.A. and its subsidiaries establishes the general principles and guidelines for protecting information and the assets associated with it. The Company promotes the preservation of the confidentiality, integrity and availability of information, with the objective of safeguarding its operations, protecting the information of employees, customers, suppliers and other stakeholders, and supporting the continuity of its business processes.

## 3. SCOPE

This document applies to Viña Concha y Toro and its domestic and foreign subsidiaries, as well as to its employees, contractors and third parties who, in the performance of their duties, have access to Company information.

This Policy covers all information assets owned or managed by the Company, regardless of their format, storage medium or means of transmission.

Information security within the Company is managed considering international best practices and recognized frameworks, including the principles of ISO/IEC 27001, in those areas relevant to the Holding's business.

The Company develops and maintains complementary policies, standards, procedures and controls to manage information security and cybersecurity risks, considering, among others, the following areas:

- Responsibilities of employees, suppliers and third parties.

[1] This document corresponds solely to a summarized and excerpted version of the Company's Corporate Information Security Policy, prepared for informational and disclosure purposes. Its content does not replace, amend or constitute the official and complete text of the Policy, which prevails in all respects. Consequently, this extract may not be interpreted in isolation or used to create rights, obligations, interpretation criteria or any other effect other than those expressly contained in the current official version of the Policy.

- Classification, custody and use of information assets.
- Secure use of the Internet and technological resources.
- Access control.
- Physical and environmental security.
- Operations security.
- Cryptography.
- Secure acquisition, development and maintenance of systems.
- Information security incident management.
- Information security in business continuity management.
- Compliance with legal, regulatory and contractual requirements.

This Policy incorporates the principles most relevant to the Company in this area, establishing guidelines and areas of action applicable to Viña Concha y Toro and its subsidiaries.

## 4. RESPONSIBILITIES

Viña Concha y Toro has established a governance structure to manage and continuously improve information security, aimed at preventing, detecting and appropriately responding to events that may affect its information assets.

**Internal Employees:** They must know, apply and comply with the Information Security Policy within their area of responsibility, protect the information they access and promptly report any event that may compromise it through the channels defined by the Company.

**Suppliers and Third Parties:** They must protect the information they access and comply with the security and confidentiality obligations established by the Company, contracts and applicable regulations.

**Information Security Governance:** The Company has formally defined responsibilities for establishing criteria, overseeing risks, keeping the regulatory framework up to date and promoting the continuous improvement of information security.

## 5. POLICY FOUNDATIONS

Viña Concha y Toro and its subsidiaries continuously manage information-related risks and seek to comply with applicable regulations, contractual obligations and requirements. All employees and third parties must contribute to protecting the Company's information.

### a) Information Classification

Information is an asset of the Company and must be protected according to its level of sensitivity. The defined classification levels are: Public, Internal Use, Confidential and Highly Confidential.

### b) Responsible Use of Information

All information classified as Internal Use, Confidential or Highly Confidential must be handled according to its level of sensitivity. Its disclosure may only take place when there is formal authorization, granted in accordance with the Company's internal policies and procedures and applicable regulations.

Information and technological resources must be used responsibly and exclusively for legitimate purposes related to the Company's activities, in accordance with established authorizations and controls.

### c) Document Disposal

Documents and information must be securely disposed of in accordance with their classification, defined retention periods and applicable regulations.

### d) Secure Data Transfer

Information must be transferred through authorized mechanisms, considering its classification, the recipients and the risks associated with its processing.

- Confidential or Highly Confidential information may only be transferred when there is a legitimate purpose and the corresponding authorizations and protection measures have been applied.
- Information must be shared only through tools and mechanisms authorized by the Company.
- Information must be protected during transmission, storage and processing, applying controls consistent with its classification.
- Before sharing information, it must be verified that the recipients are duly authorized.
- Any event that may compromise information security must be promptly reported through the channels defined by the Company.

Personal data is processed in accordance with the applicable laws and regulations in the jurisdictions where the Company operates.

## 6. NON-COMPLIANCE AND SANCTIONS

Violations of the Corporate Information Security Policy will be managed in accordance with internal procedures, contracts and applicable regulations.

Non-compliance with this Policy may result in the corresponding administrative, contractual or legal measures, in accordance with the applicable laws and regulations in each jurisdiction.

## 7. EXCEPTION MANAGEMENT

The Policy and other Information Security standards are mandatory for the individuals and third parties within their scope.