
	CORPORATE POLICY OF SECURITY OF THE INFORMATION	
Corporate Management of Finance and Affairs Corporate	PO-GCF-SI-01	Page 1 of 8

1. OBJECTIVE

The Information Security Policy of Viña Concha y Toro SA and subsidiaries (hereinafter the “Holding” or the “Company”) defines the **guides, actions and provisions to preserve the security of the Company's data and information**. Considers activities to ensure the confidentiality, integrity and availability of information, in order to avoid intentional and/or accidental damage from loss or misuse of information assets (data, equipment, printed documentation, etc.), damage in the public image of the company, and risks that affect the continuity of the business in its processes and systems.

2. SCOPE

This document applies to all personnel of Viña Concha y Toro and its national and foreign subsidiaries, including collaborators, contractors, volunteers and external parties who have access to Company information.



This policy includes all information assets that the Company possesses, in any type of format, so that the explicit non-inclusion in this document does not constitute a reason for not protecting information assets that are found in other media or formats, whether this is printed or written on paper, stored electronically, transmitted by mail or using electronic means, including that known by verbal means.

The security of the Vineyard's information will be addressed by the domains in accordance with the ISO 27001 standard, applying the definitions that are relevant in the particular cases of this standard that apply to the Holding's business. It should be noted that the first domain corresponds to the Information Security Policy that provides the general framework for the following domains.

This policy links individual aspects for the management and control of the Company's information security resources. At a specific level, new policies, standards, procedures, implementation of controls, risk assessments will be incorporated to address the needs of the domains mentioned below:

- Responsibilities of collaborators and suppliers.
- Classification, custody and use of information assets.
- Internet use.
- Access control.
- Physical and environmental security (avoid unauthorized physical access, damage and interference with the organization's information processing facilities).
- Security of operations.

PREPARED: CISO	REVIEWED: Internal Control	APPROVED: Cybersecurity Committee	VERSION: 03 MODIFICATION DATE: January 27, 2023
-----------------------	-----------------------------------	---	--

	CORPORATE POLICY OF SECURITY OF THE INFORMATION	
Corporate Management of Finance and Affairs Corporate	PO-GCF-SI-01	Page 2 of 8

- Cryptography.
- Systems acquisition, development and maintenance.
- Management of information security incidents.
- Aspects of information security in Business Continuity management (BCP).
- Compliance with legal and contractual requirements.

This Policy incorporates the most relevant aspects for the Company in this matter, defining guidelines, areas of action, responsibilities and obligations for all employees of Viña Concha y Toro and its subsidiaries.

3. DEFINITIONS

Information asset: All those relevant elements that process store and distribute company information. There are three types of assets: (1) Information in its multiple formats (paper, digital, image, text, audio, video, among others); (2) the equipment or systems that support it and (3) the people who use those assets.



Information: All information contained in any format, digital, printed or other that contains data of the organization, related to its products, services, technology and computer development, systems, work and business plans, pricing and market strategies, as well as the background of its collaborators, directors, executives, suppliers, clients.

Public Information: That information that is currently known to the market or the general public and, therefore, its disclosure does not present risks for the organization.

Information for Internal Use: All information used by the organization to normally carry out its operations, without having the characteristic of Confidential Information, information that does not generate damage or harm to the organization's processes will also be in this category.

Confidential Information: All information that, according to its nature, is private, and its knowledge by third parties has the potential to affect the development of the organization's business (for example, information about clients, associates, suppliers).

Highly Confidential Information: All information whose negligent disclosure or use may cause serious harm to the organization, its directors or managers. It is understood that the following are Highly Confidential Information, among others: the financial results of the company before their publication to the market, the background on ongoing negotiations in which confidentiality has been expressly agreed with the counterparty, the minutes of the Board of Directors of the society, management reports, cost reports, audit reports, system configurations, system passwords, among others.

 <p>VIÑA CONCHA Y TORO — FAMILY OF WINERIES —</p>	<p align="center">CORPORATE POLICY OF SECURITY OF THE INFORMATION</p>	
<p>Corporate Management of Finance and Affairs Corporate</p>	<p align="center">PO-GCF-SI-01</p>	<p align="right">Page 3 of 8</p>

Cyberattack: An intentional action seeks to cause damage or interruptions to computer systems, networks or devices connected to the Internet. It may include actions such as introducing viruses, illegally obtaining information, identity theft, interrupting services, and the data destruction.

Cyberdefense: A set of measures and strategies aimed at protecting the networks, systems and computing devices of an organization or country from possible cyberattacks.

Cyberspace: Term used to describe the virtual space existing on the Internet network, in which users interact through devices connected to the network. It includes all types of digital content, from websites, social networks, among others.

Information infrastructure: That infrastructure made up of the people, processes, procedures, tools, facilities and technologies that support the creation, use, transportation, storage and destruction of information.

Critical information infrastructures: Physical and information technology facilities, networks, services and equipment whose impairment, degradation, denial, interruption or destruction can have a significant impact on security.

Email: Communication system that allows sending and receiving messages over the Internet.

Phishing: Online fraud technique that seeks to obtain personal or financial information from a person through identity theft in emails, websites or text messages.

Malware: General term for malicious software used to cause damage to a device or network. Includes viruses, worms, Trojan horses, ransomware and other types of malicious software.



Ransomware: It is a type of malware that encrypts the files on the infected system and demands a ransom to recover them.

Botnet: Term referring to various computer equipment infected and controlled by cybercriminals remotely with a malicious purpose.

Firewall: Communications equipment that allows the internal networks of a company to be connected to the public Internet securely, only allowing previously validated data to enter/exit and allowing unauthorized access to be blocked to the organization's internal network.

4. RESPONSABILITIES

Viña Concha y Toro has established an internal structure that allows it to manage the security of the

	CORPORATE POLICY OF SECURITY OF THE INFORMATION	
Corporate Management of Finance and Affairs Corporate	PO-GCF-SI-01	Page 4 of 8

information within it, which defines specific strategies to prevent, detect and respond appropriately to security events.

Internal Collaborators: Know, understand, apply and comply with the aspects of the current Information Security Policy, within their scope of competence. They have the responsibility to comply with what is established in this document and apply it in their work environment. They have the obligation to alert their Management and the Chief Information Security Officer (CISO) in a timely and appropriate manner regarding any incident that violates the provisions of this policy (detailed in section 5. Fundamentals of the Policy). Make available to the Cybersecurity area all background information, information or data requested.



Suppliers and Third Parties: Service providing companies, contractors, subcontractors and anyone who, on their own behalf or on behalf of third parties, develops work for or on behalf of “Viña Concha y Toro”. In cases where these providers have access to confidential or highly confidential information of the Company, responsibility and confidentiality agreements must be signed with them.

Chief Information Security Officer (CISO): He is the main person responsible for defining information security and cybersecurity criteria in Viña Concha y Toro and subsidiaries, for which he must permanently analyze the level of existing risk, in addition to maintaining the validity of this document, generating the necessary modifications in accordance with the new threats and risks in the environment. On the other hand, it is responsible for publishing and disseminating new versions of the document within the Company, informing the Cybersecurity Committee and senior Management of the risks associated with Cybersecurity, establishing relevant mitigation measures and proposing changes to the Committee for its approval. subsequent validation and approval. Finally, it is key within their role to detect the need for induction and/or training in the understanding and adoption of the information security policy in cases where it is necessary.

Cybersecurity Committee: It is responsible for aligning the Cybersecurity strategy with the Holding's strategy, giving priority to projects, in accordance with the strategic plans proposed by the General Management and the Board of Directors, as well as establishing the appropriate control criteria to be effective and efficient, achieving confidentiality and integrity, complying with the Company's policies and procedures. The Committee is made up of the Corporate Finance and Corporate Affairs Management, Corporate Communications Management, Information Technology Management, People Management, Fiscal Office and Internal Audit.

5. POLICY FOUNDATIONS

Viña Concha y Toro and its subsidiaries must permanently manage the risks of their business, complying with all the regulations and demands that the market requests. All collaborators are obliged to protect the Company's information. In this policy we provide instructions to collaborators on how to avoid security breaches.

	CORPORATE POLICY OF SECURITY OF THE INFORMATION	
Corporate Management of Finance and Affairs Corporate	PO-GCF-SI-01	Page 5 of 8

a) Classification of Information

Information is an asset for the Company, and its classification is essential to ensure its security and privacy. All information generated, received or stored by the Holding must be classified according to its level of sensitivity. Classification levels include: Public, Internal Use, Confidential and Highly Confidential.

b) Responsible use of information

All information classified as Highly Confidential or Confidential must be treated with the utmost caution and security. Responsible use must be made of the information that each collaborator and user of the systems uses and manages. It is prohibited to disclose any information classified as “Confidential”, “Highly Confidential” or “Internal Use” in any medium, including verbally, unless explicitly authorized in writing by the Company's Attorney. Everything that is not expressly permitted is prohibited, and it is necessary to expose the situation in conflict so that explicit authorization is granted for what is needed. This implies disabling everything that is not necessary.

The information and its technological resources must be used exclusively for purposes related to the business and must be authorized by the corresponding management. Criteria for responsible use of the Holding's assets must be applied when there is no explicit policy or regulation for their use.

c) Communication and information from the Company to external parties

If necessary, the communication of internal information of the Company to external entities (media, press in general, discussion forums on the web, magazines, among others), must be channeled through the regular channels and procedures established. the Company's Communications Management, authorization must be requested and a strategy established that does not harm the corporate image of the Holding, with the objective of avoiding unwanted levels of exposure when disclosing Confidential or Highly Confidential Information without prior authorization.



d) Internet Use

On the Internet we can constantly be exposed to cyber attacks that can cause damage and affect the operations and technological infrastructure of the Company. To guarantee the safe use of the Internet by the Holding's employees, measures must be established that include restrictions on access to websites with inappropriate or malicious content, as well as the downloading of prohibited information or disclosure of unauthorized information.

Guidelines on safe Internet use are specified in PO-GCF-SI-02 Internet Use Policy.

e) Documents Printing

It is not permitted to keep printed documents classified as “Confidential”, “Highly Confidential” or “Internal Use” information on desks; these must be properly safeguarded.

	CORPORATE POLICY OF SECURITY OF THE INFORMATION	
Corporate Management of Finance and Affairs Corporate	PO-GCF-SI-01	Page 6 of 8

f) Document Deletion

All documents and information classified as “Confidential” or “Highly Confidential” must be disposed of securely, and in accordance with applicable regulations or standards (if applicable). This includes physically deleting any paper documents and securely deleting any information stored on electronic devices.

If the elimination or destruction of printed documents that contain “Confidential” or “Highly Confidential” information is required, destruction techniques must be used that make their recovery by third parties impossible (for this it is advisable to use machines or paper shredder tools).

Legal documents that must remain in the Company cannot be deleted or destroyed for the periods established by current laws and regulations. In case of doubt, the Prosecutor's Office should be consulted.

g) Access to offices

Physical access to offices must be restricted to authorized personnel only. All employees, contractors, outsiders and visitors must present valid identification before entering Company facilities. Additionally, all work areas and server rooms must be secured to prevent unauthorized access. Security personnel must monitor the entrances and exits of the facilities, record and report any suspicious activity.



h) Protection of personal and Company devices

When employees use their personal devices to access email or their accounts, they have the responsibility of keeping their personal devices and those assigned by the Company (mobile phone, tablet or personal computer) securely. To achieve this they must:

- Keep all access passwords protected.
- Keep your antivirus updated.
- Do not leave the device exposed to third parties or unattended.
- Install web browser and system security updates at least once per month or as updates become available.
- Access Company accounts and systems only through secure and private networks.
- Lock their devices when they leave their desks or leave their computers unattended.
- Connect devices with USB connection only in case of mouse and keyboard, the rest of the devices is not allowed.
- Install only programs authorized by the Company ([Corporate Listing](#)).

Additionally, they are prohibited from accessing accounts and internal systems from other user's computers and/or lending their assigned equipment to other collaborators.

With respect to new income, and the equipment provided to them by the Company, they must follow the following instructions:

	CORPORATE POLICY OF SECURITY OF THE INFORMATION	
Corporate Management of Finance and Affairs Corporate	PO-GCF-SI-01	Page 7 of 8

- Access the Company network/unlock-change password system.
- Use of software for remote connection.
- Access the Company's systems that correspond to you.
- Access the Company's email, using a second authentication factor.

Guidelines on the safe use of computing equipment are specified in PO-GCF-SI-03 Policy on the use of computing equipment (see [Policy](#)).

i) Safe use of Email

Email often receives spam and even attempts at scams and malware. To avoid virus infection or data theft, we instruct collaborators to:

- Do not open documents and click on attached links when the content is not clearly explained.
- Be cautious of shocking titles and/or content or urgent requests that prompt you to act or take an action immediately.
- Check email and names of people sending email to ensure they are legitimate.
- Look for inconsistencies in writing (e.g. grammatical errors, capital letters, excessive use of exclamation points).

If the collaborator is not convinced that the email they received is safe, they must report it through the channels provided for this by the Cybersecurity area.



Guidelines on secure email use are specified in the EST-GCF-SI-02 Corporate Email Usage Standard.

j) Proper password management

Passwords for access to the computer systems provided by the Company **are individual, non-transferable and the sole responsibility of the assigned person.** The leak or loss of passwords can compromise the Company's entire IT infrastructure. Passwords must be secure, robust and remain secret, for this reason, we instruct our collaborators to:

- Choose passwords with at least 12 characters (include lowercase letters, uppercase letters, numbers and symbols) and avoid information that is easy to guess (e.g. birthdays, names, etc.)
- Remember passwords instead of writing them down. If collaborators need to write down their passwords, they are required to keep the paper or digital file confidential and destroy it when their work is finished.
- Change your passwords every 60 days.

Guidelines on proper password management are specified in the EST-GCF SI-01 Password Standard.

	CORPORATE POLICY OF SECURITY OF THE INFORMATION	
Corporate Management of Finance and Affairs Corporate	PO-GCF-SI-01	Page 8 of 8

k) Secure data Transfer

The transfer of data generates security risks, for this reason collaborators must:

- Do not transfer “Confidential” or “Highly Confidential” Information (e.g. customer information, collaborator records, among others), to other devices or accounts. When bulk data transfer is necessary, collaborators must contact the team of IT specialists and request the corresponding authorizations.
- Share information only through the technological tools and programs that the Company makes available to all collaborators ([Corporate List](#)).
- When strictly necessary, confidential or highly confidential information should be shared only through the Company Network/Systems, not over the public Internet, or through external devices.
- Ensure that data recipients are authorized and have security policies suitable.
- Report scams, security breaches and unauthorized entry attempts to the Company's systems to the Cybersecurity area (ciberseguro@conchaytoro.cl)

The processing of data by the Company is based on current regulations for the protection of personal data, corresponding to each location.

l) Safe Remote Work

Collaborators working remotely (for example, from home, from a hotel, from a cafe, etc.) must follow the guidelines set forth in this policy. Remote access to the Company's systems must be done through a secure private network (VPN); as well as follow all data encryption controls, standards and protection settings.

6. NON-COMPLIANCE AND SANCTIONS

Violations of the Corporate Information Security Policy will be evaluated by the Cybersecurity Committee, to define possible sanctions with the Company's People Management, purchasing areas, management of external services or prosecutor's office, if applicable. adjusting to what is stated in our Internal Regulations of Order, Hygiene and Safety (RIOHS).

Such sanctions may include a reprimand, recording of the facts for consideration in the future professional development of the offender, the termination of the contract in question and the possible reporting of the facts to the respective authorities. All of the above, according to the nature and severity of the events and their consequences for the Company, its shareholders and the market in general.

Failure to comply with the Corporate Information Security Policy may constitute a serious violation of the Employment Contract, which is why the Company reserves the right to take administrative or legal measures as appropriate against those who do not comply with the provisions of this policy and its reference documentation.

7. EXCEPTION HANDLING

The Policy and other regulations on Information Security are mandatory, so no exceptions are allowed.