CYBERSECURITY POLICY

Text approved by resolution of the Board of Directors of 25 January 2024.

(Free translation from the original in Spanish. In the event of discrepancy, the Spanish-language version prevails)

TABLE OF CONTENTS

CYBERSECURITY POLICY

1. BASIS AND PURPOSE

Viscofan S.A. ("Viscofan" or "the Company") has implemented a *Risk Control and Management Policy* aimed at establishing the basic principles and general framework of action to identify, manage and control all kinds of risks faced by the Viscofan Group (indistinctly, the "Viscofan Group" or the "Group", which comprises the group of companies in respect of which Viscofan S.A. is the controlling company within the meaning of the law). This general policy is further developed in the specific policies that may be established in relation to certain risks of the Group.

Viscofan considers information, together with the systems that support and process it, to be one of the most important assets of its business, due to the impact it can have on its own activity and organisation, employees, suppliers, customers and stakeholders, and therefore establishes as a key objective its protection and the effective and efficient management of the risks to which it is subject.

Consequently, the Board of Directors of Viscofan approves this Cybersecurity Policy (the "Policy") of the Company and of the Viscofan Group, which enables the Company to face the new challenges of Cybersecurity by incorporating the recommendations approved in this area.

The Policy establishes the basic principles and the general framework for the control and management of cybersecurity risks to which the Group is exposed, in order to guarantee the protection of its information and the systems that support it by establishing a control framework that facilitates the availability, integrity and confidentiality of its information and allows it to respond appropriately to the threats inherent to the continuous evolution of information technologies.

The specific objectives of the Policy are as follows:

- Define the principles that govern the Viscofan Group's cybersecurity management, so that they protect the Group's information, mitigate the cybersecurity risks to which it is exposed and are aligned with current regulatory requirements.
- Define and assign responsibilities associated with the implementation and maintenance of its management model.
- Establish a framework to facilitate decision-making regarding the implementation of cybersecurity measures, both technical and procedural and organisational, in order to prevent the following impacts:
    - Damage to the image and reputation of the Viscofan Group.
    - disruption of critical processes that support the business.
    - Loss or misuse of information assets.

2. SCOPE

The Policy aims to protect against damage from digital attacks on the confidentiality, integrity, availability, authenticity, reliability of information and assets in cyberspace. It includes and is not limited to the organisation, the collection of resources, processes and structures to ensure end-to-end security throughout the supply chain and applies to both Information Technology (IT) and Operational Technology (OT), Viscofan Group companies and employees, as well as third-party collaborators and external companies accessing the Group's information systems.

IT refers to the entire spectrum of information processing technologies, including software, hardware, communication technologies and related services, as well as the processes implemented to support and manage them.

OT is understood as the hardware, software and communication systems used for the control of industrial equipment, which interact with the physical world of Viscofan's production plants.

The Group has the obligation to guarantee, in the same terms, the security of information concerning its customers, collaborating entities and the competent official bodies.

3. POLICY DEVELOPMENT

The Policy is complemented by a second layer of cybersecurity management standards, appropriate to respond to current and emerging threats as well as regulatory requirements, and will consist of general cybersecurity standards, procedures, operational manuals and technical guides (the "Cybersecurity Policy Body").

The Cybersecurity Policy Framework is reviewed regularly, at least annually, as well as after significant changes affecting the Group's cybersecurity environment and/or business circumstances.

4. PRINCIPLES FOR ACTION AND COMMITMENTS

The principles and commitments that govern the management of cybersecurity in the Viscofan Group are as follows:

- Planning. - Define short-, medium- and long-term plans that ensure a vision for the future and continuous improvement of cybersecurity, enabling it to reduce its exposure to risk within the defined tolerance levels.
- Risk assessment. Assess in advance the cybersecurity risks in activities and operations, adopting the management measures deemed necessary according to their level of risk, and cybersecurity decisions will be taken according to the actual risk of the materialisation of threats to the organisation.
- Incident management and resilience. - Ensure continuity of operational capability for the organisation's purposes and that of stakeholders who may be affected by its activities.

- Monitoring. - Implement a monitoring, detection and early warning system that allows for a permanent and continuous identification of vulnerabilities, new threats and incidents at a global level, as well as defining the appropriate mechanisms to ensure that the people in charge of protecting assets, infrastructures and/or their information systems are informed of such incidents in a timely manner.
- Integrity. - Ensure full integration of cybersecurity commitments with stakeholders and require suppliers and prime contractors who can access Group systems to be responsible for and trained in cybersecurity prior to the commencement of the actual contractual relationship.
- Training. - Promote cybersecurity training, awareness and culture throughout the organisation with the aim of training staff on best practices and habits to prevent and mitigate cybersecurity risks
- Continuity. - Establish procedures and responsibilities for immediate, effective and orderly response to cybersecurity incidents, as well as specific contingency and continuity plans.
- Regulatory compliance. - Ensure compliance with applicable cybersecurity laws and regulations in all countries in which the Group operates. Viscofan collaborates with the competent authorities and organisations to contribute to the improvement of cybersecurity.
- Continuous Improvement. - Viscofan will rely on recognised national, European and international standards, appropriate to its needs, to better monitor the progress of its maturity in this area.

5. CYBER SECURITY ORGANISATION

5.1 Executives

Cybersecurity is a function whose responsibility is exercised from the highest hierarchical level of the organisation and corresponds to:

- The Board of Directors is responsible for approving the Policy and monitoring it, ensuring that the bodies with responsibility for achieving the objectives set have sufficient material and human capacities to be able to carry out the assigned functions effectively and efficiently.

- The Audit Committee, by delegation of the Board of Directors, shall be responsible for the executive supervision of the implementation of the Policy and especially for the prior validation of the Group's Cybersecurity Plans and objectives and the periodic monitoring of the CISO reports.

- Senior management assumes the commitment to promote and encourage, under the responsibility of the Chief Information Security Officer (hereinafter CISO), the implementation of cybersecurity management systems in their respective areas of responsibility and, in particular, the monitoring of cybersecurity risks through the Group's Global Risk Committee.

5.2 Cybersecurity and CISO Committee

Notwithstanding the responsibilities of senior management, there will be a Cybersecurity Committee whose essential function is to define, promote and control cybersecurity and which will participate in making decisions and strategies in this area.

The Cybersecurity Committee shall be composed of the CISO and an appropriate number of areas of the organisation to adopt any resolution, with relevance to information security, that may substantially affect the organisation's activity.

The ordinary management and execution of the above measures corresponds, by delegation of the Cybersecurity Committee, to the CISO, who must have the appropriate knowledge, experience and skills to perform the function and will have sufficient decision-making capacity and influence in the organisation. The CISO shall have sufficient capabilities and resources, both material and human, to achieve its objectives. This individual will report functionally to the Corporate Director of Strategy, Organisation and Systems of the Company, guaranteeing due independence with respect to those responsible for network and information systems.

5.3 Local Cybersecurity Responsibilities

In each of the Viscofan Group's subsidiaries, a local Cybersecurity Manager will be appointed who, under the direction of the CISO, will carry out the coordination functions in the implementation and supervision of the Cybersecurity Policy and the Cybersecurity Regulatory Body.

5.4 Employees and collaborators

In addition to the responsibilities set forth in this Policy, all employees of the Viscofan Group are responsible for complying with the Cybersecurity requirements within the exercise of their functions. This ensures that there is a shared responsibility between employees, managers, collaborators, and the Cybersecurity organisation. In particular, it shall duly comply with the training activities promoted in the organisation.

6. RISK AND INCIDENT MANAGEMENT AND REPORTING

6.1 Risk and incident management

The Cybersecurity Regulatory Body will promote the analysis of risks, including the classification of assets and vulnerabilities, classifying potential incidents according to their impact, both in the field of Information Technology (IT) and industrial or Operational Technology (OT) in order to determine mitigation plans as well as the intervention and application of existing crisis management committees and protocols in the Group in order to minimise the impact on the business and ensure regulatory compliance and adequate internal or external communication.

The capabilities shall be in place to enable the organisation to be resilient to ensure continuity of operations and full recovery of services within an appropriate timeframe to be determined in the business continuity plan.

6.2 Periodic reporting and reports

The Board of Directors, directly or through the Audit Committee, shall regularly monitor cybersecurity, including this issue on the agenda of its meetings. Particularly:

- When a topic that may affect cybersecurity is on the agenda of the Board of Directors' meetings, the implications of cybersecurity for the topic should be discussed, for example: major digital transformation initiatives, implementation of new technologies and major investments in technology assets, mergers and acquisitions, facility expansion or major upgrades.

- The Cybersecurity Committee, through the CISO, shall inform the Audit Committee of cyber threats that could affect the organisation's objectives. This will take into account at least the main actors and the main and most recent cyber threats, considering their potential impact on the organisation's operations. In any event, it must submit its activity report to the Audit Committee every six months and must contain at least the state of cybersecurity, the progress of the degree of maturity and cyber risk, the development of threats, the allocation of resources allocated to the security of the networks and information systems, the significant incidents managed, if any, the security status of supply chain operations that depend on third parties, as well as any relevant cybersecurity resolutions adopted by the management team that may materially affect the organisation's business. The CISO shall also report, where appropriate, any obstacle or impediment that could restrict the proper performance of its activity.

7. CONTINUITY

Regular comprehensive tests that test the organisation's resilience mechanisms shall be conducted as part of the Cybersecurity plans. In this context, tests of the business continuity plan as well as simulations and preparedness exercises for crisis management committees will be carried out.

In general, companies should systematically implement effective drills and tests of the various protection, response and recovery measures. These exercises should involve the entire organisation, with particular attention to the company's critical processes, including the supply chain.

8. AUDIT

Independent audits are carried out periodically, by Internal Audit or through external companies, either total or partial, with the aim of verifying the degree of compliance with the Policy and the rules set out in manuals and procedures that make up the Viscofan Group's Cybersecurity Regulatory Body.

9. VALIDITY AND REVISIONS

The Policy shall enter into force on the next business day following its approval by the Board of Directors upon proposal of the Company's Audit Committee. It shall remain in force until such time as it is amended or repealed by a later one.

From its entry into force, there are 6 months to adjust any incompatibilities with the provisions of the Policy that may exist in other rules, both global and local.

The Policy will be reviewed periodically and in the light of organisational, legal or business changes from time to time, in order to maintain its relevance, adequacy and effectiveness.

This Policy is available on the Intranet for all employees and on the corporate website for all stakeholders of the Company.