CYBERSECURITY POLICY

1. INTRODUCTION

Information and associated systems are critical assets that must be managed and protected against various sources of risks. Risks can be natural, accidental and/or deliberate, resulting in business disruptions and breaches to sensitive business and/or personal data.

As stated in our Code of Conduct, Grifols, S.A. and its subsidiaries ("**Grifols**") has valuable non-financial (e.g. scientific, technical, commercial) and financial information. We must protect this information, as well as our business and continuity of supply. In doing so, we also protect our patients who rely on our products and services for their health and well-being, and donors who make our therapies possible, as well as our customers and suppliers.

Grifols is firmly committed to protecting its business assets by implementing the necessary controls, including policies, processes, and procedures, to safeguard its business and stakeholders and by balancing risk levels with the efficient allocation of resources, guided by principles of proportionality.

2. PURPOSE

The objective of this policy (the "**Policy**") is to set forth the basic principles and the general framework to reduce Grifols' exposure to internal and external cybersecurity threats within the defined tolerance levels while complying with applicable cybersecurity laws and regulations so that Grifols can achieve its goals and fulfill its mission.

3. SCOPE

This Policy applies to all employees of Grifols and covers all Grifols information and associated systems, including information technology, operational technology, and medical devices.

In companies where Grifols has financial interest but does not have management control, Grifols will recommend adoption of, and compliance with, the principles and guidelines set forth in this Policy.

Furthermore, Grifols will extend the principles and guidelines set forth herein to its third-party partners throughout the supply chain.

4. PRINCIPLES

Grifols establishes the following basic principles to govern cybersecurity risks:

- Maintain robust, updated, and resilient systems for processing of personal information, supported by encryption, anonymization, and other relevant measures.
- Define a systematic approach for the continuous identification and assessment of cybersecurity risks, including third party risks, as well as for the response to any cybersecurity incident.
- Implement security measures to protect the confidentiality, integrity and availability of information systems and associated processes (including information systems managed by third parties), and continuously monitor their effectiveness to ensure ongoing improvement.
- Implement procedures and invest in tools to facilitate agile adaptation to changing conditions in the technological environment.
- Ensure that effective response and recovery programs are in place, encompassing people, processes, information systems and technology to: detect, assess, respond within a reasonable time frame to, remedy and, if necessary pursuant to applicable legislation, disclose to investors actual or potential cybersecurity incidents and threats; effectively recover from cybersecurity incidents; escalate cybersecurity incidents to management and the cybersecurity team; and notify authorities of any incidents as required by applicable laws and regulations.
- Maintain a highly qualified cybersecurity team, comprised of management, information technology and legal personnel, by defining adequate hiring criteria and establishing rigorous training plans.
- Ensure training is provided to employees, executives and directors regarding cybersecurity risks, and protection of sensitive and personal data. Training shall include protecting against phishing attacks, guidance on the use of email, internet, and social media to ensure sensitive information is appropriately handled and protected and the escalation process for employees to follow in the event of an identified cybersecurity incident or threat.
- Collaborate with peer companies, industry associations and government agencies to share best practices and effective solutions against cybersecurity threats.

To support the deployment of these principles, Grifols implements the “Information Security Process and Management System" (the "**ISMS**"). The ISMS is based on the appropriate definition of objectives, roles and responsibilities, policies and procedures, and technology to: (i) identify cybersecurity threats and related risks; (ii) protect critical assets; (iii) detect and respond to cybersecurity threats and cybersecurity incidents; and (iv) recover business services due to a cybersecurity incident.

5. ORGANIZATIONAL AND REPORTING MODEL

Grifols' Board of Directors, through the Audit Committee, is responsible for supervising and evaluating the efficiency of the control and management on cybersecurity. Grifols

Internal Audit and Enterprise Risk Management Department supports the Audit Committee in the fulfilment of this responsibility.

The Head of the Information Security Office ("**ISEC**") reports to the Chief Digital Information Officer and has the authority to develop and implement the company's cybersecurity policies, standards, procedures, and oversee the implementation and effectiveness of the ISMS.

To that end, the Head of the ISEC is supported by the Global Cybersecurity Committee, who facilitates the alignment of cybersecurity initiatives with business objectives; ensures global coverage of the ISMS; collaborates in the prioritization and execution of security initiatives and projects; and promotes a culture of protection against cybersecurity threats throughout Grifols. The Committee shall be comprised of representatives of business units, information technology and legal personnel, as well as operations and services areas.

The Head of Internal Audit shall update the Audit Committee, at least twice per year, regarding the control and management on cybersecurity. For these updates the Audit Committee may require the assistance of the Chief Digital Information Officer and/or the Head of the ISEC.

6. ADMINISTRATION AND INTERPRETATION

Grifols' Board of Directors entrusts the monitoring, compliance, and management of this Policy to the Audit Committee.

The Audit Committee is authorized to interpret and construe this Policy and to make all determinations necessary, appropriate, or advisable for the administration of this Policy and for the Company's compliance with any applicable laws.

7. AMENDMENT; TERMINATION

Grifols' Board of Directors, following the proposal of the Audit Committee, may amend this Policy from time to time in its discretion and shall amend this Policy as it deems necessary. Notwithstanding anything in this Section 8 to the contrary, no amendment or termination of this Policy shall be effective if such amendment or termination would (after considering any actions taken by Grifols contemporaneously with such amendment or termination) cause Grifols to violate any applicable laws.

8. DEFINITIONS

For the purposes of this Policy:

- "**cybersecurity incident**" means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through Grifols' information systems that jeopardizes the confidentiality, integrity, or availability of Grifols' information systems or any information residing therein;

- "**cybersecurity threat**" means any potential unauthorized occurrence on or conducted through Grifols' information systems that may result in adverse effects on the confidentiality, integrity, or availability of Grifols' information systems or any information residing therein; and

- "**information systems**" means electronic information resources, owned or used by Grifols, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Grifols' information to maintain or support the Grifols' operations.

9. POLICY VALIDITY

This Policy is effective from November 16th, 2023, date of approval by Grifols' Board of Directors.