Security Policy Information.

Purpose	Summary of the Information Security Policy
Scope	All processing of personal data and other information carried out by VALFONDO HOLDING, S.L. and its affiliates (hereinafter referred to as "VALFONDO"), as well as the security measures applicable to such information.
Trainers	General Management, Information Security Officer and Data Protection Officer.

Versions

Version	Date	Content of the modification
0.0	10/12/2020	Initial Drafting
0.1	14/12/2020	Modification of the initial document
0.2	24/03/2021	Approval
0.3	12/12/2023	Update (various sections)
0.4	24/06/2026	Information Security Management System (ISMS) Compliant Upgrade

1 COMMITMENT TO INFORMATION SECURITY

At VALFONDO we consider information security as a strategic pillar for the development of our activity, business continuity, and the protection of the interests of customers, employees, suppliers and other interested parties.

Through the Information Security Policy, VALFONDO establishes the principles, responsibilities and controls necessary to manage the risks associated with information and personal data, integrate security into its processes and promote an organizational culture based on shared responsibility, continuous improvement and compliance with applicable regulations on information security and personal data protection. including the General Data Protection Regulation (GDPR).

2 PILLARS OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

- **Confidentiality:** Ensuring that information is accessible only to persons authorized to have access.

- **Integrity:** Ensuring that the information and methods of its processing are accurate and complete.

- **Availability:** Ensure that authorized persons have access to information and its associated assets, when required for the exercise of their functions.

3 OBJECTIVES

- Protect systems, applications, information assets and personal data from unauthorized access, alteration, loss, destruction or misuse.

- Raise awareness and train staff in relation to their responsibilities in terms of information protection, protection of personal data and secure use of systems, applications and technological resources.

- Prevent the improper use of systems, applications, devices and other technological resources, reducing the risks arising from their use.

- Detect, communicate and appropriately manage security incidents, through the application of controls and procedures aimed at guaranteeing security in the processing of one's own information, that of third parties and personal data.

4 MAIN MEASURES TAKEN

- Control of physical and logical access to the organization's systems and devices.
- Secure password management with multi-factor authentication.
- Regular backups and disaster recovery plans.
- Management and monitoring of security incidents.
- Classification and proper treatment of confidential information.
- Restriction of the use of external storage devices.
- Continuous training and awareness of all staff on good practices in cybersecurity.

The measures adopted are reviewed on an ongoing basis and updated when necessary, taking into account the results of the risk assessment, the effectiveness of the controls implemented, the results of internal and external audits, the security incidents and events recorded, as well as the suggestions and opportunities for improvement identified, in order to ensure the continuous improvement of the Information Security Management System.

5 GOVERNANCE AND COMPLIANCE

The Policy establishes clear roles and responsibilities in matters of information security, including among others, the General Management, the Security Officer, the Data Protection Officer and Users. These profiles collaborate in a coordinated manner to ensure regulatory compliance, risk assessment, and response to potential threats or vulnerabilities.

In short, this Policy responds to VALFONDO's commitment to strict compliance with current regulations on information security and personal data protection, as well as to the implementation of good practices that guarantee operational continuity and the protection of the interests of all parties involved.