

## INFORMATION SECURITY POLICY

Author: Consultant	Validated by: Information Security Officer	Approved by: Director General
Organisation: <b>PROCESIA PROYECTOS Y SERVICIOS SL</b>	Organisation: <b>GRUPO EMPRESARIAL MELÉNDEZ SL</b>	Organisation: <b>GRUPO EMPRESARIAL MELÉNDEZ SL</b>
		Signature:
<b>Date:</b> 10/03/2022	<b>Date:</b> 15/03/2022	<b>Date:</b> 17/03/2022

**Description:** Top management should establish an information security policy that:

- a) is fit for purpose for the organisation;
- b) include information security objectives or provide a framework for setting information security objectives;
- c) include a commitment to comply with applicable information security requirements; and
- d) include a commitment to continual improvement of the information security management system.


The information security policy should:

- e) be available as documented information;
- f) communicate within the organisation; and
- g) be made available to interested parties, as appropriate

*UNE-EN ISO/IEC 27001:2017 Information technology. Security techniques. Information security management systems. Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015) 5.2 Policy*

## VERSION CONTROL

<b>Version</b>	<b>Date</b>	<b>Description</b>
1.0	17/03/2022	First version.

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

## DECLARATION

(public text to be disseminated to third parties: customers, suppliers, regulators, public)


**GRUPO EMPRESARIAL MELÉNDEZ** is a business group from Valladolid, leader in the fresh potato sector in Spain, dedicated to selecting, packing and distributing the best potatoes from its different companies specialised in each sales channel (retail, Horeca, ...).

The business culture of **GRUPO EMPRESARIAL MELÉNDEZ** is based on the control of the quality of the raw material throughout the production process, under an exhaustive concept of food safety, taking the field as the beginning of the chain and following up until its final distribution.

Consequently, the mission of **GRUPO EMPRESARIAL MELÉNDEZ** is to ensure that the consumer has the best experience of identical and unequalled taste and texture 365 days a year.

During 2022 and under its powerful digitalisation strategy, **GRUPO EMPRESARIAL MELÉNDEZ** will have its new 21,600m<sup>2</sup> plant, fully automated and digitalised, which will be positioned as a benchmark in the sector at European level, incorporating the most cutting-edge technology and focused on maximum efficiency.

**GRUPO EMPRESARIAL MELÉNDEZ**, aware of the importance of cybersecurity as a key factor for regulatory compliance, information protection and business continuity, has established security processes and controls in order to guarantee the confidentiality, integrity, authenticity and traceability of information, as well as the availability of the services provided to

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

clients, in accordance with international standards, to facilitate the following **objectives:**

- Raise awareness and train staff in information protection.
- Assess and address information security risks.
- Comply with legislation on personal data protection, intellectual and industrial property and any other applicable legislation.
- Responding to cyber incidents.
- Ensure business continuity in the event of critical events.
- Assess the effectiveness and efficiency of information security processes and controls.
- Continuously improve information security management processes.


The management of **GRUPO EMPRESARIAL MELÉNDEZ**, as a consequence of the above, is committed to allocating reasonable human and material resources to achieve the established cybersecurity objectives.

The supervision of information security management is exercised by the Management of **GRUPO EMPRESARIAL MELÉNDEZ**, delegating to the **Head of Information Security** the competencies for the proper implementation, development and maintenance of this policy, with the support of the entire team and collaborators.

**GRUPO EMPRESARIAL MELÉNDEZ, Managing Director**

Francisco Javier Meléndez Juárez

**12 December 2022**

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	


## INFORMATION SECURITY POLICY

(controlled dissemination text to customers, suppliers, regulators, etc.)

In order to comply with the Information Security Policy of **GRUPO EMPRESARIAL MELÉNDEZ**, an information security management system (hereinafter, ISMS) has been established, in accordance with the standard "*UNE-EN ISO/IEC 27001:2017 Information technology. Security techniques. Information Security Management Systems. Requirements*", which adequately covers all the requirements necessary to guarantee the confidentiality, integrity, authenticity and traceability of the information, as well as the availability of the services provided to customers.

For the implementation and maintenance of the **GRUPO EMPRESARIAL MELÉNDEZ** information security management system, the General Management has taken the following decisions:

1. Designate an information security officer with delegated authority and responsibility for the development, maintenance and improvement of the information security management system.
  
2. Establish an information security management organisation with clearly defined roles and responsibilities.
  
3. Allocate talent resources and reasonable material means to develop the production process, from the field to the dispatch of the product to customers, with exhaustive control over the raw material, with cybersecurity as the basis, maintaining the balance between cost and benefit.

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	


4. Plan training and awareness-raising for all staff and collaborators to be aware of the risks and threats to information security and to know how to act in the event of cyber-incidents.
5. Promote the analysis of information security risks as an essential process for implementing controls for their proper treatment.
6. Measure and analyse the information security management indicators that allow the General Management to monitor the security objectives.
7. Regularly monitor, review and audit the information security management system.
8. Proactively comply with applicable legal, policy and regulatory requirements.

In order to implement the decisions taken, the General Management of **GRUPO EMPRESARIAL MELÉNDEZ** establishes the following policies:

**Information security is everyone's responsibility**

Information security measures shall be supervised by the Directorate General and shall be the responsibility of all staff and collaborators.

The Directorate General will provide the necessary means, in accordance with a model of continuous improvement, with special emphasis on the training of human resources and on the control and analysis of results to verify the efficiency and effectiveness of the measures.

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

### **Proactive cyber risk management**


The following measures are taken to manage the risks arising from threats to assets:

- The allocation of the specialised resources needed to carry out the risk analysis.
- Record the risk analyses performed and submit the acceptance of the residual risk level for approval by the Directorate General.
- Set the unacceptable risk value at 35% of the maximum possible average score, aiming to be within the range of 20%.  
- 35% as a tolerable range, with 20% being the target value.
- The Information Security Manager of PATATAS MELÉNDEZ updates the risk analysis annually and the risk treatment plans will be established to achieve the risk objective.

### **Protection of computer equipment, software and communications.**

The following measures are taken to ensure the proper use of the equipment and installed programmes, which are delivered to users properly configured for their performance:

- The equipment and systems are assets owned by **GRUPO EMPRESARIAL MELÉNDEZ**, assigned to its users, duly inventoried and placed at their disposal exclusively for the performance of their functions.
- The installation and use of any software programme or digital content, other than those installed or expressly authorised, is strictly restricted. Likewise, modifications to the hardware elements delivered are not permitted.

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

- All software programs installed on the equipment have the appropriate user and/or maintenance licences issued by their manufacturers.

### Physical access control

In order to guarantee access to the offices and facilities of **GRUPO EMPRESARIAL MELÉNDEZ**, where the equipment and information systems are located, the following measures are followed:


- Access to the offices and facilities of **GRUPO EMPRESARIAL MELÉNDEZ** by persons not belonging to its organisation or collaborators is controlled at reception and authorised in advance by the person in charge of the unit to be visited.
- Visitor access is supervised at all times, with entry and exit being recorded.
- Visitors accessing the areas where the equipment and information systems are housed, duly delimited, are accompanied at all times by a person responsible for **GRUPO EMPRESARIAL MELÉNDEZ**.

### Protection of infrastructures and installations

The following measures are taken to guarantee the protection of **GRUPO EMPRESARIAL MELÉNDEZ**'s infrastructures and installations:

- Power supply to information systems in the event of a general power failure.
- The provision of fire detection and extinguishing means.
- The provision of intrusion detection means.



Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

- The protection of data and voice network cabling by conduit against accidental or deliberate incidents.
- The existence and availability of alternative facilities to be able to work in case the usual facilities are not available.

### **User identification and authentication**


In order to guarantee proper access to the information systems of **GRUPO EMPRESARIAL MELÉNDEZ**, the following measures are taken:

- Each user is assigned a unique user name and password, which are strictly personal and non-transferable, given according to his or her information access needs.
- The passwords are initially configured by the **GRUPO EMPRESARIAL MELÉNDEZ** IT services.
- User passwords are renewed every 180 days.
- User names and passwords are changed or deleted when there is a change of functions or termination, respectively.

### **Good use of Internet access**

The following measures are taken to ensure access to the Internet and the correct use of its resources by users:

- Internet access is monitored at all times and activity is recorded.

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

- Internet browsing is tailored to the performance needs of each user, recognising the value and usefulness of its content and services for internal and external effectiveness and efficiency.
- User access is restricted to those areas of the Internet deemed unsafe or inappropriate, in accordance with recognised good usage practices and current legislation.


### **Good use of e-mail**

To ensure the proper use of e-mail by users, the following rules are followed:

- The e-mail accounts assigned to users for the performance of their professional activities are the property of **GRUPO EMPRESARIAL MELÉNDEZ**.
- The contents of the e-mails are confidential and comply with the law.
- All users of e-mail accounts are assigned a unique e-mail address and a password, which is strictly personal and non-transferable.
- The password is initially set up by the IT services of the **MELÉNDEZ BUSINESS GROUP**.

As security guidelines, users follow the following measures:

- ✓ Never open or forward mail from unknown senders.
- ✓ Never open or forward e-mails from known senders, but with subjects in languages other than the sender's own.
- ✓ Never open attachments from emails of dubious origin.

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

### Back-up copies

In order to ensure the recovery of data stored by users, in case of loss or destruction, the following measures are taken:

- The centrally stored data is backed up by the **GRUPO EMPRESARIAL MELÉNDEZ** IT services.
- The backup copies are kept and maintained by the IT services of **GRUPO EMPRESARIAL MELÉNDEZ**.

### Content filtering


In order to guarantee the identification, blocking and elimination of potentially malicious content, **GRUPO EMPRESARIAL MELÉNDEZ** installs and maintains an antivirus system in the users' equipment, and compliance with the following measures is obligatory:

- Never disable anti-virus software.
- Always restart the computer or device to complete the installation of all updates.

### Protection of operating systems and other utilities

To reduce vulnerabilities in operating systems and other utilities installed on users' computers, the following measures are taken:

- Never disable update programs.
- Always restart the computer or device to complete the installation of all updates received.

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

## Monitoring of servers and network electronics.

Servers and network electronics are monitored to ensure that they are operational with availability rates close to 100%.

## Incident management


The following measures are taken to mitigate and correct any incidents affecting information and communications systems:

- The immediate communication by users to the Security Officer of any event, such as: computer or communications anomaly, malfunctioning, loss of control of programmes, sudden disconnection of the system, suspicious external communication, physical presence of unidentified strangers on the premises, etc.
- Communication is preferably via the e-mail account [sistemas@patatasmelendez.com](mailto:sistemas@patatasmelendez.com) created for this purpose.
- Recording and tracking to closure of incidents.
- Root cause analysis for preventive measures.

## Protection of information

To prevent the loss, theft or unauthorised transfer of classified information or intellectual property of **GRUPO EMPRESARIAL MELÉNDEZ**, the following measures shall be followed:

- The identification and classification of all information, on whatever medium, considered to be of special protection.

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

- The monitoring and supervision of controls for the access, handling, transmission and reproduction of such information.
- The monitoring by users of a practice of workstation clearance of files and screen locking by password when the equipment is unattended or not in use.

### **Continuity of operations**


The following measures are taken to reduce the risks arising from the occurrence of a cyber-attack, accident, catastrophe, attack or sabotage:

- The preparation and regular updating of the business continuity plan.
- Dissemination and training on business continuity measures to staff and partners.

### **Legal compliance**

In order to avoid legal contingencies arising from the handling of personal data, the following measures are taken:

- The identification and recording of applicable legal or contractual information security and privacy requirements.
- Regulatory compliance, with special emphasis on compliance with current legislation on personal data protection.
- Periodic auditing of compliance in order to verify and make evidence of compliance available to regulators and authorities.

Project: ISMS	Version:1.0	Date: 31/01/2022	
<b>MELÉNDEZ BUSINESS GROUP</b> <b>ISMS Information Security Policy</b> <b>v1.0.docx</b>		Classification: <b>PUBLIC</b>	

## Continuous improvement

In order to optimise and continuously improve information security management, the following measures are taken:

- Proposals for any suggestion, measure or action for improvement, on the part of users, are addressed to the Information Security Manager.
- The recording and monitoring, from proposal to closure, of proposed improvements.
- Periodic analysis of proposed improvements and implementation, where appropriate.
- Recognition of users who propose improvements.

-----  
This Information Security Policy is known and subscribed to by all personnel and collaborators of **GRUPO EMPRESARIAL MELÉNDEZ**.

The Security Policy is reviewed annually or when significant changes occur, to ensure its continuing suitability, adequacy and effectiveness.

Changes to the Information Security Policy will be approved by the General Management of **GRUPO EMPRESARIAL MELÉNDEZ** and distributed in a timely manner by the Information Security Manager.