

INFORMATION SECURITY POLICY

In a constantly evolving technological environment, where threats that can affect corporate information occur and evolve daily, it is necessary to implement a cybersecurity governance framework and best practices for the handling of corporate information to enable Farmhispania Group to fulfill its business activities, while maintaining high security standards that protect the confidentiality, integrity, and availability of information, in compliance with applicable regulations, and adhering to the following guidelines:

- **Confidentiality:** The information handled by Farmhispania Group will be known exclusively to authorised persons, following the principles of Need to Know basis and Least Privilege, at the right time and by the authorised means.
- **Integrity:** The information handled by Farmhispania Group will be complete, accurate, and valid, with its content being that provided by the interested parties and those affected, without any type of manipulation.
- **Availability:** The information handled by Farmhispania Group will be accessible and usable by users who are authorised and identified at all times, ensuring its permanence in the event of any anticipated eventuality.

The Management of Farmhispania Group, by approving this Policy, is committed to improving the level of cybersecurity and information security maturity in internal processes by implementing an Information Security Management System that considers the following cybersecurity functions:

- **Identification:** Understanding the current context, identifying potential threats that may materialise and pose a risk to Farmhispania Group.
- **Protection:** Establishing appropriate security measures, both technical and organisational, to guarantee the work of Farmhispania Group, limiting or containing the impact of a potential cybersecurity incident.
- **Detection:** Defining appropriate activities to identify and discover potential threats that exploit vulnerabilities and lead to an incident.
- **Response:** Establishing appropriate activities to take action in the event of a security incident affecting the availability of information, and minimising the time during which systems are down.
- **Recovery:** Promoting appropriate activities to maintain resilience plans and restore any service or system that is affected by an incident, preventing the lack of integrity or availability of information.

Consequently, Farmhispania Group maintains the following application guidelines to be taken into account within the framework of the Information Security Management System.

- The protection of personal data and the privacy of individuals will be respected.
- The organisation's records will be kept secure.
- Intellectual property rights will be protected.
- The security regulations on corporate information will be made available to interested parties that are affected by them.
- Information security responsibilities will be assigned.
- Information security training and education will be carried out.

- Information security incidents will be monitored and recorded.
- Business continuity plans will be in place.
- Any changes related to information security that may occur will be managed.

This policy will be made available to members of Farmhispania Group in an appropriate repository for their access.

This policy, and all the regulations that have led to its development, as well as the security measures implemented, will be monitored and updated based on existing needs.

Firmado por Sergi Ruiz



Signed by Sergi Ruiz

Sergi Ruiz

Apruebo este documento
06/05/2025 | 10:31 CEST

CEO Farmhispania Group

816B089C711B4824B22B08DCD28E6E35