

INFORMATION SECURITY POLICY



INDEX

1. Objective	3
2. Definitions	3
3. Responsibilities	3
4. Information security Policy	3
5. Scope	4
6. Versioning & approval	4

1. Objective

Establish the global guidelines of the organization for the protection of the company's information assets, according to a management system focused on the mitigation of information security risks, continuous improvement, and other principles of ISO / IEC 27001: 2013.

2. Definitions

- **Information asset:** Element or set of elements necessary for the use and processing of information (paper or electronic documents, databases, applications, operating systems, software, services, equipment, hardware, infrastructure, people and information).
- **Information:** Refers to an organized set of data that the organization's workers generate, obtain, acquire, transform, or control.
- **Risk:** Effect of uncertainty on the achievement of objectives.

3. Responsibilities

Information Security Officer:

- Ensure adequate communication of the information security policy

Director:

- Review and approve the information security policy

Organization staff:

- Comply with the information security policy

4. Information security Policy

Walmeric is a company that contributes to the development of its clients, through the provision of its software for the management of potential clients, a leader in assisted sales and increased conversion, considering the information of its clients and interested parties as an asset fundamental for its operation; reason for which there is a firm commitment to protect its confidentiality, integrity and availability that materializes with the implementation of an information security management system (ISMS) in accordance with ISO / IEC 27001, guided by the following principles:

- Continuous improvement of its processes and services, especially in terms of information security.
- The effective treatment of information security risks.
- The participation of competent and conscientious personnel in matters of information security.
- Contribution to the improvement of the provider's service provision, through an adequate control process.
- Compliance with the applicable ISMS requirements, such as standard, legal, regulatory, statutory, and contractual.

This policy is approved and promoted by senior management, as part of their leadership functions in the ISMS. Its compliance is essential for the organization, so it is ensured through communication and availability, not only to internal staff but to all relevant stakeholders.

We make every effort to protect Walmeric and our users from any unauthorized alteration, disclosure, or destruction of the data we maintain or from unauthorized access to this information. For it:

- We use encryption to keep user data private while in transit.
- We review our data collection, storage, and processing practices (including physical security measures) to prevent unauthorized access to our systems.
- We restrict access to personal information to only Walmeric employees, contractors and agents who need the information to process it. Anyone with access to this information is bound by strict contractual confidentiality obligations and may be disciplined or terminated if they fail to comply.

5. Scope

Preservation of information assets for the development, exploitation, and professional services of lead to revenue management solutions owned by Walmeric according to current SOA

6. Versioning & approval

Version	Date	Changes	Review Date & Signature	Approved Date & Signature
1.0	04/07/2022	Review	Fernando Lopez	José A. Torres

If you need more information, please contact: information.security@walmeric.com