GENERAL STATEMENT OF THE INFORMATION SECURITY AND CYBERSECURITY POLICY ISMS – SQDM S.A.S

At **SQDM S.A.S,** we recognize that information and information assets are fundamental for the effective performance of our operations and a key pillar in achieving our mission, vision, and corporate objectives. Accordingly, we reaffirm our unwavering commitment to the comprehensive management of information security and cybersecurity.

In line with this commitment, **SQDM S.A.S** integrates information security and cybersecurity management across all its operations, with the objective of reducing exposure to cybersecurity threats that may compromise the confidentiality, integrity, and availability (CIA) of information through appropriate administrative, technical, and physical safeguards. This is achieved through the continuous operation of the Information Security Management System (ISMS), the adoption of best practices aligned with ISO/IEC 27001:2022 and industry-recognized frameworks such as the NIST Cybersecurity Framework, strict compliance with applicable legal and regulatory requirements, and full alignment with the corporate strategy.

1. PRINCIPLES

The principles governing the effective management of information security and cybersecurity at **SQDM S.A.S** are as follows:

- A risk-based approach is applied to operations and corporate decision-making, including risk assessment and risk treatment activities.
- Roles and responsibilities have been established to ensure the proper operation of the ISMS.

- We conduct ongoing security awareness and training activities and promote responsible information security behaviors across the organization.
- We adhere to applicable legal and regulatory requirements.
- Information security and its associated security controls are core elements embedded in all company activities.
- The design of our Information Security Management System is based on a continuous improvement framework.
- We share valuable information with relevant stakeholders.

2. SCOPE

This statement, together with its associated policies and guidelines, is mandatory for all permanent and temporary employees, suppliers, interns, third parties, and any other legal or natural persons who use the information and technologies provided by **SQDM S.A.S**. under contractual or operational arrangements.

3. ROLES AND RESPONSIBILITIES

- Responsibility for the maintenance and continuous improvement of this document lies with the Chief Information Security Officer (CISO).
- Responsibility for approving the provisions of this document lies with the Security Committee.
- All Users are responsible for protecting the information and systems to which they have access, in accordance with the established security policies and procedures.
- The CISO is responsible for overseeing the implementation, enforcement, and ongoing compliance with this policy.

4. EXCEPTIONS

Any exception to this policy must be formally documented, reviewed, and approved in advance by the Security Committee.

5. NOTIFICATION AND PUBLICATION

All employees, suppliers, interns, third parties, and entities with access to **SQDM S.A.S.** and/or its clients' information assets will be informed of this policy and its guidelines. This policy and its derived policies will be made available on the company website, cloud-based network drives, and corporate notice boards.

6. NON-COMPLIANCE

Failure to comply with this statement and its associated policies and guidelines may result in disciplinary actions for employees, in accordance with the Internal Work Regulations. Additionally, any violation of information security requirements by a supplier may result in early termination of the contract, without liability for penalties or damages, in accordance with applicable contractual terms.

7. INCIDENT RESPONSE

SQDM S.A.S. maintains an Incident Response Plan to address security incidents and data breaches in accordance with applicable legal, regulatory, and contractual notification requirements.

8. CONTACT

If you have any questions or concerns regarding this policy, please contact: ***legal@sqdm.com***

Publication Date:

Next scheduled review: August 28, 2026

Revision History

Date	Version	Description of Change	Modified by
July 11, 2025	1.0	First version of the document	Bayron Angel Delgado
August 28, 2025	1.1	Approved by the Security Committee	Bayron Angel Delgado