MAAKAL

INFORMATION SECURITY POLICY

1. Objective

This Information Security Policy aims to establish a reference framework for protecting the information of Maakal, Inc. and its subsidiaries, ensuring its confidentiality, integrity, and availability. This policy seeks to mitigate risks associated with information management, prevent security incidents, and ensure compliance with applicable laws and regulations, including the protection of customer information.

1.1 Management System and Leadership Commitment

Maakal, Inc. establishes, implements, maintains, and continually improves an Information Security Management System (ISMS) in accordance with **ISO/IEC 27001:2022**. Top Management is committed to providing the necessary resources, integrating information security into business processes, meeting applicable requirements, and driving the continual improvement of the ISMS. This commitment includes compliance with Colombian personal data protection legislation (**Law 1581 of 2012** and **Decree 1377 of 2013**) and other applicable regulations in force.

1.2 Information Security Objectives

Information security objectives, their targets, and measurable indicators are established and measured in the document *"Objetivos e Indicadores de Seguridad de la Información"* (*Information Security Objectives and Indicators*), approved by Top Management and reviewed at least once a year. The CISO must monitor them on a quarterly basis and report the results to Top Management.

2. Scope

This policy applies to all employees, contractors, suppliers, and third parties that access, process, store, or manage information belonging to Maakal, Inc. It extends to

all information systems, databases, storage devices, and any other technological resources used in the company's operations.

ISMS Scope. The boundaries and applicability of the ISMS—including internal and external issues, interested parties and their requirements, and interfaces and dependencies with other organizations—are defined in the document *"Alcance del SGSI"* (*ISMS Scope*), approved by Top Management and maintained as documented information.

3. Definitions

- **Information security:** A set of measures and controls aimed at protecting information against unauthorized access, alteration, or destruction.
- **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** Ensuring that information remains accurate, complete, and free from unauthorized modification.
- **Availability:** The property of being accessible and usable upon demand by an authorized entity.
- **ISMS (Information Security Management System):** A set of policies, processes, procedures, roles, and controls through which the organization manages information security in accordance with ISO/IEC 27001:2022.
- **Information asset:** Any data, system, device, or resource that holds value for the organization and contains or processes information.
- **Interested party (Stakeholder):** A person or organization that can affect, be affected by, or perceive itself to be affected by Maakal, Inc.'s information security decisions or activities (customers, suppliers,employees, authorities).
- **Security incident:** An event that puts information security at risk.
- **Information security risk:** The potential that a threat will exploit a vulnerability, causing an impact on the organization.

- **Supplier:** An external company or entity that provides goods, services, or technologies to Maakal, Inc.,and that must comply with the information security requirements established in this policy.
- **Customer:** A person or entity that receives services from Maakal, Inc., and whose information must be protected in accordance with this policy.

4. Responsibilities

Information security roles and responsibilities are defined and assigned according to the needs of the organization. Individuals with assigned responsibilities may delegate tasks, but remain accountable for verifying their proper execution.

Role	**Responsibility**
Top Management(*Alta Dirección*)	Approve the Information Security Policy and ISMS objectives, ensure alignment with strategic direction, provide necessary resources, and accept corresponding residual risks.
CISO	Responsible for designing, implementing, maintaining, and reviewing the Information Security Policy. In addition, leads information-related risk management, coordinates control implementation, oversees policy compliance, and reports periodically to Top Management.
IT / Administrators(*Administradores/TI*)	Implement and operate technical controls defined in specific policies (MDM, encryption, antivirus, web filtering, backups, access control), and generate evidence of their operation.

Role	Responsibility
Service Lead(*Líder de Servicios*)	Coordinate the detection, containment, eradication, and recovery of security incidents, and maintain the corresponding records.
Employees / Collaborators(*Colaboradores*)	Comply with this policy and specific policies, protect the information they access, and report incidents and suspicious activities.

5. General Overview

Maakal, Inc. recognizes the importance of information security in its operations and in its relationships with employees, customers, and suppliers. Information is a fundamental asset that must be protected against internal and external threats to ensure business continuity and the achievement of strategic objectives.

5.1 Security Principles

- The principle of least privilege is applied, limiting access to information only to those who require it for their duties.
- Access control measures are implemented to ensure proper authentication and authorization.
- Periodic backups are performed to guarantee information availability.
- Cryptographic controls are applied to protect sensitive data.
- An incident response plan is established to mitigate potential security breaches.
- Periodic risk assessments are conducted to identify potential threats and apply appropriate mitigation measures.

- Suppliers are required to comply with security standards and report relevant incidents; this compliance is enforced and backed by contractual agreements and confidentiality clauses.
- Customer information is protected through appropriate processes and controls in accordance with data protection legislation.
- Threat intelligence information is gathered and analyzed to keep the organization prepared for the emerging risk landscape.
- Information security is managed in the use of cloud services by establishing clear requirements for the acquisition, use, administration, and termination of such services.
- Preventive and technical measures are implemented to mitigate the risk of data leakage across systems,networks, and devices processing sensitive information.

5.2 Risk Management

The organization must conduct periodic information security risk assessments according to a documented methodology that evaluates impact and likelihood and determines risk levels. Risk treatment must select the necessary controls and map them against Annex A through the Statement of Applicability (SoA). Results are retained as documented information and reflected in the Risk Register (*Matriz de Riesgos*) and ISMS indicators.

5.3 Security Incident Management

- A formal incident management process is established, covering detection, notification, analysis,containment, eradication, and recovery.
- The Incident Response Lead coordinates a team with clearly defined roles and responsibilities.
- Every incident must be reported immediately to the CISO / Information Security Officer.
- A post-incident review is conducted to identify root causes and prevent recurrence.
- Detailed incident records are maintained for audit and improvement purposes.

- Suppliers are required to report any incident that could affect Maakal, Inc. or its customers.

5.4 Information Backups

- Backups of information, software, and system images are performed according to data criticality and business recovery requirements.
- Backups include appropriate physical and logical protection measures (such as encryption) and, when feasible, are stored in a geographic location separate from the primary site to prevent data loss from physical disasters.
- Periodic restoration tests are conducted to verify that backup media are reliable and that information can be effectively recovered within the required timeframe.

5.5 Training and Awareness

- Information security training programs are carried out for all personnel, tracked via the passed-assessments indicator.
- A security culture based on good practices and regulatory compliance is fostered.
- Specific risk management training is provided for key personnel, along with training for suppliers regarding Maakal, Inc.'s security expectations.
- Personnel are trained in the secure handling of customer information.

5.6 Audit, Compliance, and Continual Improvement

Periodic internal and external audits are conducted to evaluate policy compliance, verifying the proper implementation of security measures and adherence to standards by suppliers. Findings are documented,improvement plans are executed, and Top Management is briefed on security results and progress.

5.7 Information Classification

All information and its associated assets must be classified and labeled in accordance with the *Política de Clasificación y Etiquetado de la Información* (*Information Classification and Labeling Policy*), using the levels:**Public** (*Público*), **Internal Use** (*Uso*

Interno), **Confidential** (*Confidencial*), and **Secret** (*Secreta*). Assigning this classification is the direct responsibility of the asset owner.

To guarantee data protection, in the absence of an explicit classification, information is treated by default as **Internal Use**; it is never assumed to be Public by default.

Operational Exception: Promotional material, marketing campaigns, and commercial communications officially issued by the Marketing area are exempt from this default rule. Such material, due to its nature and distribution purpose, is considered **Public** information, even if it lacks an explicit classification label.

6. Review Cadence

The CISO must review this policy at least once a year and, additionally, upon changes in business strategy,technological environment, legislation or contracts, risk landscape, or threat landscape, as well as following lessons learned from incidents or audits. Any change must be approved by Top Management and recorded in the change control log.

7. Disciplinary Measures / Sanctions

Non-compliance with this policy by employees, contractors, suppliers, or any affiliated third party is addressed through a formal, communicated, and progressive disciplinary process that considers severity, intent,recurrence, and prior training of the offender, while respecting applicable labor law and the confidentiality of the individual involved. Measures may include a warning, suspension, or termination of the employment or commercial contract and, in severe cases, legal action. These measures also apply in cases of negligence in protecting customer information or failure to report security incidents.

8. References

This policy is developed in conformity with **ISO/IEC 27001:2022** and **ISO/IEC 27002:2022**, ensuring alignment with international best practices in information security management.

9. Effective Date

This policy enters into force upon approval and is mandatory for all members of Maakal, Inc.