Information Security Policy

Kicol Tecnologia e Serviços LTDA

Document:	Information Security Policy
Version:	1.0
Approval date:	March 3, 2026
Next review:	March 2027
Approved by:	Eduardo Macedo — Director / Technical Lead
Classification:	Internal use

CNPJ: 64.973.433/0001-06

Rua Alcindo Guanabara, 17, Sala 1313, Centro, Rio de Janeiro - RJ, 20031-130

1. Purpose

This Information Security Policy (ISP) establishes the guidelines, responsibilities and practices adopted by Kicol Tecnologia e Serviços LTDA to protect the information under its responsibility, ensuring the confidentiality, integrity and availability of data belonging to clients, partners and the organization itself.

The policy aims to ensure that everyone involved in the company's operations understands their responsibilities regarding information protection and adopts adequate security practices in their daily activities.

2. Scope

This policy applies to all employees, service providers and partners who have access to systems, data or infrastructure of Kicol Tecnologia, including:

- Systems and applications developed and maintained by the company;
- Hosting infrastructure and servers;
- Source code repositories;
- Databases containing client information;
- Work equipment (workstations, mobile devices);
- Third-party services and platforms used in operations.

As a company with a lean and specialized structure, the controls described in this policy are proportional to the organization's size and the risk level of its operations, without compromising their effectiveness.

3. Definitions and Principles

Information security at Kicol Tecnologia is guided by three fundamental principles:

- **Confidentiality:** ensuring that information is accessed only by authorized individuals.
- **Integrity:** ensuring that information is not altered in an improper or unauthorized manner.
- **Availability:** ensuring that information and systems are accessible when needed.

4. Information Security Guidelines

4.1 Authentication and credentials

All access credentials to systems, servers and platforms must be stored exclusively in an encrypted password manager. Storing passwords in text files, spreadsheets, emails or any unencrypted medium is prohibited.

Passwords must be at least 12 characters long and combine uppercase letters, lowercase letters, numbers and special characters. Password reuse across different services is prohibited.

Two-factor authentication (2FA) must be enabled on all services that offer this functionality, including hosting panels, code repositories and cloud services.

4.2 Encryption

All workstations used in operations must have disk encryption enabled (FileVault on macOS, BitLocker on Windows or equivalent on Linux).

Communication between systems and APIs must be conducted exclusively through encrypted protocols (HTTPS/TLS). Unencrypted connections are prohibited in production environments.

Production databases must use encrypted connections (SSL/TLS) and, where applicable, data-at-rest encryption.

4.3 Infrastructure and hosting

Production servers are hosted by an infrastructure provider with internationally recognized security certifications. Server access is performed exclusively through SSH keys; password-based SSH access is disabled.

The hosting provider's administration panel is protected by two-factor authentication (2FA).

Root or administrative access to servers is restricted to the company's technical lead.

5. Access Control

Access to systems, servers, code repositories and databases follows the principle of least privilege: each person receives only the level of access strictly necessary to perform their role.

Currently, access to production infrastructure (servers, databases and code repositories) is restricted exclusively to the company's technical lead and director. Should the team expand, access will be granted individually, recorded and reviewed quarterly.

All source code repositories are maintained as private on GitHub. Access is controlled through individual permissions linked to 2FA-authenticated accounts.

Upon termination of any professional relationship (employee, service provider or partner), all access is revoked immediately.

6. Data Protection

Kicol Tecnologia acknowledges its responsibility in protecting personal and corporate data processed on behalf of its clients, in compliance with Brazil's General Data Protection Law (LGPD — Law No. 13,709/2018).

Client data is processed exclusively for the contracted purpose. The use of production data in development or testing environments is not permitted. For testing purposes, fictitious or anonymized data must be used.

Sensitive data such as API credentials, authentication tokens and access keys are stored in protected environment variables on the server, never in source code or repositories.

In the event of an incident involving personal data, the client will be notified within 48 hours of incident identification, as provided by the LGPD.

7. Secure Software Development

Kicol Tecnologia's software development process follows secure development practices, including:

- Validation and sanitization of all user input data;
- Protection against common vulnerabilities (OWASP Top 10): SQL Injection, XSS, CSRF, among others;
- Use of parameterized queries for database access;
- Separation of development, staging and production environments;
- Code review before any production deployment;
- Credentials and keys stored exclusively in environment variables, never in source code;
- Third-party dependencies and libraries are kept updated and checked for known vulnerabilities.

Production deployment is performed manually via SSH with key authentication, ensuring that only the authorized technical lead can publish changes to the production environment.

8. Security Incident Management

Kicol Tecnologia maintains a security incident response procedure comprising the following stages:

- **Identification:** continuous system monitoring and analysis of hosting provider alerts;
- **Containment:** immediate isolation of the compromised resource to prevent spread;
- **Eradication:** removal of the root cause and correction of the exploited vulnerability;
- **Recovery:** system restoration from backups and integrity verification;
- **Notification:** client communication within 48 hours, with details of the incident, impact and measures taken;
- **Lessons learned:** incident recording and control review to prevent recurrence.

9. Backup and Recovery

Kicol Tecnologia performs daily backups of all production systems and databases. Backup procedures include:

- Automated daily backup of databases and application files;
- Backup storage in an environment separate from the production server;
- Minimum 30-day backup history retention;
- Periodic restoration tests to validate backup integrity;
- Encryption of backup files in transit and at rest.

10. Use of Technology Resources

The company's technology resources (equipment, servers, software licenses and cloud services) must be used exclusively for professional purposes related to the company's activities.

Installing unauthorized or unknown-origin software on equipment that accesses the company's or its clients' infrastructure is prohibited.

Operating systems and software in use must be kept updated with the latest security patches released by manufacturers.

11. Third-Party and Client Relationships

All client contracts include confidentiality and data protection clauses, establishing each party's responsibilities regarding information security.

When working with client data or systems, Kicol Tecnologia commits to following the client's security policies, when applicable, in addition to its own.

Third-party platforms and services used in operations (hosting, repositories, development tools) are evaluated for their security practices and certifications before adoption.

12. Sanctions and Disciplinary Measures

Non-compliance with this policy by any employee, service provider or partner may result in disciplinary measures proportional to the severity of the infraction, including:

- Formal written warning;
- Immediate suspension of access to systems and infrastructure;
- Termination of the contractual relationship;
- Civil and criminal liability, where applicable, under current legislation.

All security incidents caused by non-compliance with this policy will be recorded and investigated.

13. Review and Updates

This policy will be reviewed annually or whenever there is a significant change in the company's structure, services provided, technology infrastructure or applicable legislation.

The person responsible for the review is the company's director and technical lead. Each review generates a new version of the document, with a record of the date and changes made.

Version	Date	Description	Owner
1.0	03/03/2026	Initial version	Eduardo Macedo

14. Approval

This document has been approved by the management of Kicol Tecnologia e Serviços LTDA and takes effect on the date of its publication.

_____

Eduardo Macedo
Director / Technical Lead
Kicol Tecnologia e Serviços LTDA
March 3, 2026