Information Classification Policy

Kicol Tecnologia e Serviços LTDA

Document:	Information Classification 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

To establish criteria and guidelines for classifying information handled by Kicol Tecnologia e Serviços LTDA, ensuring that each piece of information receives the appropriate level of protection according to its value, sensitivity, legal requirements and business criticality.

2. Scope

This policy applies to all information generated, received, stored, processed or transmitted by Kicol Tecnologia, in any format (digital or physical), including client data, source code, credentials, internal documents and communications.

3. Classification Levels

3.1 Confidential

Information whose unauthorized disclosure could cause significant damage to the company or its clients. Access is restricted exclusively to the technical lead and, when contractually required, to the data-owning client.

Examples:

- Server, database and API access credentials;
- SSH keys and authentication tokens;
- End-client personal data (name, ID, address, banking details);
- Client project source code;
- Client financial data (sales values, commissions, transfers);
- Contracts and commercial proposals with values.

3.2 Internal Use

Operational company information that should not be externally disclosed, but whose leakage would not cause serious damage. Access is restricted to the company's team.

Examples:

- Technical system architecture documentation;
- Internal policies and procedures;
- Log and incident records;
- Internal project communications;
- Environment configuration data (without credentials).

3.3 Public

Information that can be freely disclosed without risk to the company or its clients.

Examples:

- Institutional information published on the company website;
- Summarized versions of security policies;
- Company commercial contact information.

4. Handling by Classification Level

Control	Confidential	Internal Use	Public
Storage	Encrypted	Protected environment	No restriction
Transmission	HTTPS/TLS only	HTTPS/TLS only	No restriction
Access	Technical lead	Authorized team	No restriction
Sharing	Prohibited without authorization	As needed	Open
Disposal	Secure deletion	Standard deletion	No restriction
Backup	Required, encrypted	Required	Optional

5. Secure Disposal

Confidential information must be securely disposed of, ensuring it cannot be recovered. Upon project or contract termination, all client data must be eliminated from Kicol Tecnologia environments within 30 days, unless otherwise required by law or contract.

6. Review

This policy will be reviewed annually or whenever there is a significant change in the services provided or applicable legislation.

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

7. Approval

_____

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