



Access Control Policy

Kicol Tecnologia e Serviços LTDA

Document:	Access Control 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 the rules and procedures for granting, reviewing and revoking access to systems, servers, code repositories, databases and other technology resources of Kicol Tecnologia e Serviços LTDA.

2. Principles

- **Least privilege:** each person receives only the level of access strictly necessary for their role;
- **Need to know:** access is granted only when there is a legitimate business need;
- **Individual accountability:** each access is linked to an individual identity; credential sharing is prohibited.

3. Authentication

3.1 Password requirements

- Minimum 12 characters;
- Combination of uppercase, lowercase, numbers and special characters;
- Password reuse across different services is prohibited;
- All passwords must be stored exclusively in an encrypted password manager (Bitwarden or equivalent);
- Storing passwords in text files, spreadsheets or emails is prohibited.

3.2 Two-factor authentication (2FA)

2FA is mandatory on all services that offer it, including hosting panels, code repositories and cloud services.

3.3 Server access

Production server access is performed exclusively through SSH keys. Password-based SSH access is disabled. SSH keys are passphrase-protected and stored only on the technical lead's authorized devices.

4. Access Granting

Currently, production infrastructure access is restricted exclusively to the company's director and technical lead. Should the team expand, access granting will follow formal request, least privilege definition, individual account creation with mandatory 2FA, and documented record.

5. Access Review

Granted access is reviewed quarterly to ensure it remains adequate and necessary.

6. Access Revocation

Upon termination of any professional relationship, all access must be revoked immediately, including SSH keys, repository access, API tokens and hosting panel access.

7. Review

This policy will be reviewed annually or whenever there is a significant change in the company's access structure.

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

8. Approval

Eduardo Macedo

Director / Technical Lead

Kicol Tecnologia e Serviços LTDA

March 3, 2026