Secure Development Policy

Kicol Tecnologia e Serviços LTDA

Document:	Secure Development 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 security practices and guidelines adopted during the software development lifecycle at Kicol Tecnologia e Serviços LTDA, ensuring that applications are designed, developed and maintained with protection against known vulnerabilities and threats.

2. Secure Development Principles

2.1 OWASP Top 10 protection

All applications developed by Kicol Tecnologia must implement protections against the most common vulnerabilities:

- **Injection (SQL, NoSQL, OS):** mandatory use of parameterized queries and ORMs; concatenating user data into queries is prohibited;
- **Broken authentication:** robust authentication with secure password hashing (bcrypt/argon2), brute-force protection and 2FA support;
- **Sensitive data exposure:** encryption in transit (mandatory HTTPS/TLS) and at rest where applicable;
- **XSS (Cross-Site Scripting):** sanitization and escaping of all output rendered in the browser;
- **CSRF (Cross-Site Request Forgery):** anti-CSRF tokens on all state-changing operations;
- **Security misconfiguration:** removal of default credentials, debug disabled in production, HTTP security headers configured;
- **Vulnerable components:** dependencies kept updated and checked for known CVEs.

2.2 Credential and secret management

- Credentials, API tokens and encryption keys are never included in source code;
- All secrets are stored in server environment variables;
- The .env file is included in .gitignore for all projects;
- Production credentials differ from development and staging credentials.

2.3 Environment separation

Development, staging and production environments are separated. Production data is not used in development or testing environments. Fictitious or anonymized data is used for testing purposes.

3. Security Testing

- Security tests are performed before each production deployment;

- Tests include input validation, authentication/authorization testing and security header verification;
- After significant updates, vulnerability tests are conducted;
- Identified vulnerabilities are fixed before production release.

4. Dependencies

All third-party dependencies must come from trusted sources, be kept updated, be checked for known vulnerabilities and be continuously monitored through GitHub security alerts (Dependabot).

5. Review

This policy will be reviewed annually or when there are significant changes to the development technologies or practices.

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

6. Approval

_____

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