TekGenio Inc.
Secure Software Development Lifecycle (Secure SDLC) Policy
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This policy establishes the minimum security requirements to be integrated into the software development lifecycle for applications, integrations, APIs, AI solutions and data platforms delivered by TekGenio.

2. Scope

Applies to all internally developed software, customer projects, customisations, integrations, cloud solutions, AI/ML applications, ETL pipelines and third-party components used by TekGenio.

3. Secure SDLC Principles

Security and privacy shall be incorporated throughout planning, design, development, testing, deployment and maintenance using a 'security by design' approach.

4. Requirements & Design

Projects shall identify security, privacy and compliance requirements during planning. Threats, data flows and security controls should be considered during solution design.

5. Secure Coding

Developers shall follow secure coding practices, minimise hard-coded secrets, validate inputs, implement output encoding and address common risks such as those identified in the OWASP Top 10.

6. Source Code Management

Source code shall be maintained in an approved version control system. Changes should be traceable, peer reviewed and linked to authorised work items where practical.

7. Code Reviews

Peer review is required before production deployment. Reviews should consider functionality, security, privacy, maintainability and coding standards.

8. Dependency Management

Open-source libraries and third-party packages should be evaluated, kept up to date and monitored for known vulnerabilities.

9. Security Testing

Applications should undergo appropriate testing including functional testing, authentication checks, input validation, vulnerability scanning and regression testing before release.

10. Change Management

Production deployments shall follow approved change management processes including testing, approvals, rollback planning and release documentation.

11. Secrets Management

API keys, passwords, certificates and tokens shall not be stored in source code repositories. Approved secure storage mechanisms should be used.

12. Logging & Monitoring

Applications should generate appropriate audit logs while protecting sensitive information from unnecessary exposure.

13. Vulnerability Management

Reported vulnerabilities shall be assessed, prioritised and remediated according to business risk. Critical issues should be addressed promptly.

14. Third-Party Components

Third-party software, AI services and cloud platforms shall be evaluated for security, licensing and contractual suitability before adoption.

15. AI Development

AI-enabled solutions should include controls for dataset quality, model validation, human oversight and secure deployment consistent with the AI Governance Policy.

16. Training

Developers should receive periodic secure coding and application security awareness training.

17. Compliance

This policy supports alignment with ISO/IEC 27001:2022, OWASP ASVS, OWASP Top 10, NIST Secure Software Development Framework (SSDF) and applicable customer requirements.

18. Review

This policy shall be reviewed annually or after significant changes to technologies, regulations or development practices.