

TekGenio Inc.
AI Governance Policy
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This policy establishes governance principles for the responsible design, development, deployment and operation of Artificial Intelligence (AI) solutions delivered by TekGenio.

2. Scope

Applies to AI, machine learning, generative AI, predictive analytics, intelligent automation and data science solutions developed, implemented or supported by TekGenio.

3. Governance

Executive Management oversees AI governance. Project managers, technical leads and solution architects are responsible for ensuring AI systems comply with organisational policies and customer requirements.

4. Responsible AI Principles

TekGenio promotes fairness, transparency, accountability, privacy, security, reliability, human oversight and compliance throughout the AI lifecycle.

5. Data Governance

Training and operational datasets should be obtained lawfully, protected appropriately and used only for authorised purposes. Data quality should be validated where practical.

6. Human Oversight

AI outputs supporting business decisions should be subject to appropriate human review where the solution or customer requirements warrant such oversight.

7. Security of AI Systems

AI applications should follow secure development practices, access controls, encryption, logging, monitoring and vulnerability management consistent with company security standards.

8. Bias & Fairness

Where AI is used for decision support, project teams should evaluate datasets and models for potential bias and document significant limitations.

9. Transparency

Customers should receive appropriate information regarding the intended purpose, capabilities and known limitations of AI-enabled solutions where contractually required.

10. Model Monitoring

Operational AI solutions should be monitored for reliability, accuracy, performance degradation and significant anomalies where applicable.

11. Model Changes

Material model updates should follow change management, validation and approval processes before production deployment.

12. Third-Party AI Services

External AI platforms and models should be evaluated for security, privacy, licensing and contractual suitability before use in customer engagements.

13. Incident Management

AI-related incidents, including unexpected behaviour, security events or material model issues, should be reported and investigated under the incident response process.

14. Compliance

TekGenio seeks alignment with recognised guidance including the NIST AI Risk Management Framework, applicable privacy legislation and contractual obligations.

15. Training & Awareness

Personnel involved in AI development or deployment should receive appropriate training on responsible AI, privacy and information security.

16. Review

This policy shall be reviewed annually or after significant changes in technology, regulation or business operations.