TekGenio Inc.
Risk Management Policy
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This policy defines TekGenio's approach to identifying, assessing, treating, monitoring and reporting information security, privacy, operational, AI and technology risks.

2. Scope

Applies to all business units, employees, contractors, customer projects, cloud services, software development, AI solutions and supporting infrastructure.

3. Objectives

Establish a consistent risk management process that supports business objectives, customer commitments and regulatory obligations.

4. Governance

Executive Management oversees the risk management programme. Risk owners are responsible for identifying and managing risks within their areas.

5. Risk Management Process

Risks are identified, assessed, prioritised, treated, monitored and periodically reviewed. Significant risks are escalated to management.

6. Risk Categories

Risk assessments should consider information security, privacy, cyber threats, AI, operational resilience, legal, third-party, infrastructure and business continuity risks.

7. Risk Assessment

Risks are evaluated based on likelihood and business impact. Appropriate treatment options include mitigation, transfer, acceptance or avoidance.

8. Risk Register

Material risks should be documented in a risk register including owner, status, treatment plan, review date and residual risk.

9. AI Risk

Projects involving AI should consider bias, model performance, explainability, privacy, misuse and human oversight as part of project risk assessments.

10. Third-Party Risk

Suppliers handling customer information or critical services should be assessed for security, privacy and operational risks before engagement where appropriate.

11. Monitoring & Review

Risks should be reviewed periodically and following significant technology, regulatory or business changes, security incidents or customer requirements.

12. Reporting

Management should receive periodic summaries of significant risks, treatment progress and emerging threats.

13. Training

Personnel shall receive appropriate awareness regarding risk identification and reporting responsibilities.

14. Compliance

This policy supports alignment with recognised frameworks such as ISO/IEC 27001, ISO 31000, NIST Cybersecurity Framework and contractual obligations.

15. Review

This policy shall be reviewed annually or after significant organisational, legal or technology changes.