TekGenio Inc.
Third-Party Risk Management Policy
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This policy establishes the minimum requirements for identifying, assessing, approving, monitoring and managing risks associated with third parties that provide products or services to TekGenio or have access to TekGenio or customer information.

2. Scope

Applies to suppliers, subcontractors, consultants, cloud service providers, SaaS vendors, hosting providers, managed service providers, data processors and any other external organisations engaged by TekGenio.

3. Objectives

Reduce operational, information security, privacy, legal and business continuity risks arising from third-party relationships while meeting customer and contractual obligations.

4. Governance

Executive Management oversees the third-party risk programme. Business owners are responsible for vendor selection and ongoing oversight. IT, Security and Privacy stakeholders support risk assessments where applicable.

5. Vendor Classification

Third parties should be classified based on the services provided, information handled, system access, criticality and business impact.

6. Due Diligence

Prior to engagement, vendors should be evaluated for security, privacy, financial stability, regulatory compliance and operational capability. Supporting documentation may include security questionnaires, certifications or independent audit reports where available.

7. Contractual Requirements

Contracts should include confidentiality, information security, privacy, breach notification, subcontracting, audit rights and data protection obligations where appropriate.

8. Access Management

Third-party access shall be approved, limited to business need, periodically reviewed and revoked when no longer required.

9. Ongoing Monitoring

Critical vendors should be reviewed periodically for security posture, contractual compliance, service performance and material changes to their risk profile.

10. Incident Management

Third parties must promptly notify TekGenio of security incidents or data breaches affecting TekGenio information or customer services in accordance with contractual obligations.

11. Business Continuity

Critical suppliers should maintain appropriate business continuity and disaster recovery capabilities consistent with the services they provide.

12. Termination

Upon termination, third parties shall return or securely dispose of TekGenio and customer information, revoke access and comply with contractual exit obligations.

13. Exceptions

Exceptions require documented management approval, risk acceptance and appropriate compensating controls.

14. Compliance

This policy supports alignment with ISO/IEC 27001:2022, ISO 27036, NIST Cybersecurity Framework, CIS Controls and applicable contractual obligations.

15. Review

This policy shall be reviewed annually or following significant business, regulatory or supplier changes.