TekGenio Inc.
Vendor Security Policy
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This policy defines the minimum security requirements that vendors, subcontractors and service providers must satisfy when providing services to TekGenio or handling TekGenio or customer information.

2. Scope

Applies to all external organisations that provide products, cloud services, managed services, consulting, development, hosting, data processing or support services.

3. Security Principles

Vendors are expected to protect confidentiality, integrity and availability of information using industry-recognised security practices and comply with contractual obligations.

4. Vendor Selection

Business owners shall perform security due diligence appropriate to the vendor's risk profile before engagement.

5. Information Protection

Vendors shall implement appropriate access controls, encryption, logging, monitoring and secure handling of TekGenio and customer information.

6. Privacy

Where personal information is processed, vendors shall comply with applicable privacy laws and contractual data protection obligations.

7. Access Control

Vendor access must be approved, restricted to business need, periodically reviewed and revoked when no longer required.

8. Incident Notification

Vendors shall promptly notify TekGenio of security incidents, data breaches or events that could affect TekGenio systems or customer information.

9. Business Continuity

Critical vendors should maintain documented business continuity and disaster recovery capabilities appropriate to the services provided.

10. Compliance

Vendors may be requested to provide evidence such as security questionnaires, policies, certifications or independent assessments where appropriate.

11. Contractual Requirements

Vendor agreements should include confidentiality, security, privacy, audit rights, subcontracting controls and secure termination requirements.

12. Offboarding

Upon contract termination, vendors shall return or securely destroy TekGenio and customer information and confirm revocation of access.

13. Exceptions

Exceptions require documented approval and risk acceptance.

14. Review

This policy shall be reviewed annually or after significant regulatory, business or technology changes.