TekGenio Inc.
Information Security Policy
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

Purpose

TekGenio is committed to protecting the confidentiality, integrity and availability of company and customer information while delivering ERP, AI/ML, SAP, cloud, data analytics, data warehousing and software engineering services.

Scope

Applies to all employees, contractors and third parties with access to TekGenio information, systems or customer environments.

Governance

Executive Management is responsible for governance. Security responsibilities are assigned to management and personnel.

Information Classification

Data shall be classified as Public, Internal, Confidential or Restricted.

Asset Management

Information assets shall be inventoried and protected throughout their lifecycle.

Access Control

Least privilege, need-to-know, unique identities, approval and periodic access reviews are required.

Authentication

Strong passwords and MFA should be used for privileged and cloud access where supported.

Data Protection

Sensitive data shall be encrypted in transit and protected at rest where appropriate.

Secure Development

Secure coding, peer review, version control and testing are required before production deployment.

Vulnerability Management

Security vulnerabilities should be assessed, prioritised and remediated in accordance with business risk.

Logging and Monitoring

Critical systems should generate logs supporting operational monitoring and investigations.

Backup and Recovery

Critical business data shall be backed up and restoration tested periodically.

Incident Response

Security incidents shall be reported, contained, investigated and documented promptly.

Third-Party Security

Suppliers handling customer information should be evaluated for appropriate security controls.

Security Awareness

Personnel shall receive recurring security awareness training.

Compliance

TekGenio aligns its practices with recognised frameworks including ISO 27001, NIST CSF and applicable contractual and privacy obligations.

Review

This policy is reviewed at least annually or after significant organisational or technology changes.