TekGenio Inc.
Security Awareness Policy
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This policy establishes the requirements for providing information security, privacy and cybersecurity awareness training to all TekGenio personnel to reduce security risks and promote a strong security culture.

2. Scope

Applies to all employees, contractors, consultants, interns, temporary staff and authorised third parties with access to TekGenio information assets, systems or customer environments.

3. Objectives

Ensure personnel understand their security responsibilities, recognise cyber threats, protect customer information and comply with organisational policies and contractual obligations.

4. Governance

Executive Management sponsors the awareness programme. Managers ensure participation. Personnel are responsible for completing required training and applying secure working practices.

5. Mandatory Training

Security awareness training shall be completed during onboarding and refreshed at least annually. Additional role-based training may be required for developers, administrators and personnel handling sensitive information.

6. Awareness Topics

Training should include phishing awareness, password security, multi-factor authentication, data classification, privacy, secure remote working, acceptable use, incident reporting, social engineering, ransomware, AI security awareness and secure handling of customer information.

7. Phishing Exercises

Where appropriate, simulated phishing exercises may be conducted to evaluate awareness and identify opportunities for additional training.

8. Incident Reporting

Personnel shall promptly report suspected phishing attempts, lost devices, malware, unauthorised access or other security concerns using approved reporting channels.

9. Training Records

Completion of awareness activities should be recorded and retained in accordance with organisational requirements.

10. Continuous Improvement

The awareness programme should be reviewed periodically based on incidents, emerging threats, regulatory changes and customer requirements.

11. Non-Compliance

Failure to complete mandatory training or repeated policy violations may result in additional training, management review or disciplinary action in accordance with company procedures.

12. Compliance

This policy supports ISO/IEC 27001:2022, ISO 27701, NIST Cybersecurity Framework 2.0, CIS Controls v8 and applicable contractual obligations.

13. Review

This policy shall be reviewed annually or following significant changes to business operations, technology or regulatory requirements.