TekGenio Inc.
Remote Working Policy
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This policy establishes the minimum security and operational requirements for employees and authorised contractors working remotely while accessing TekGenio or customer systems.

2. Scope

Applies to all personnel performing work from home, customer sites, travel locations or any remote location using company-managed or approved personal devices.

3. Remote Working Principles

Remote work must protect the confidentiality, integrity and availability of TekGenio and customer information and comply with company policies and contractual obligations.

4. Approved Devices

Personnel should use company-issued or approved devices configured with supported operating systems, endpoint protection and security updates.

5. Authentication

Unique user accounts are required. Multi-factor authentication (MFA) should be enabled for cloud services, VPNs and privileged access wherever supported.

6. Secure Connectivity

Remote connections shall use approved encrypted methods such as VPN, HTTPS, SSH or equivalent secure technologies. Public Wi-Fi should only be used with appropriate protections.

7. Information Handling

Confidential and Restricted information shall only be accessed, stored and transmitted using approved systems. Printing sensitive information at remote locations should be minimised.

8. Physical Security

Users shall protect devices from theft or unauthorised viewing, lock screens when unattended and store company equipment securely.

9. Collaboration Tools

Only approved collaboration, messaging, video conferencing and file-sharing services may be used for company business.

10. Incident Reporting

Lost devices, suspected phishing, malware, unauthorised access or other security incidents shall be reported immediately using the company's incident reporting process.

11. Monitoring

Company systems may be monitored for operational, security and compliance purposes in accordance with applicable laws and contractual commitments.

12. Responsibilities

Employees are responsible for complying with this policy. Managers ensure remote workers understand security requirements. IT supports secure remote access and endpoint management.

13. Compliance

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

14. Review

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