TekGenio Inc.
Access Control Policy
Version 1.0

Classification: Internal Use
Review: Annual

1. Purpose

This policy defines the requirements for granting, modifying, reviewing and revoking access to TekGenio information assets, customer environments and business applications.

2. Scope

Applies to all employees, contractors, consultants, interns, third parties and service accounts accessing TekGenio-managed systems or customer systems.

3. Principles

Access shall follow the principles of least privilege, need-to-know, segregation of duties and accountability.

4. Identity Management

Each user must have a unique account. Shared user accounts are prohibited except where technically unavoidable and formally approved.

5. User Provisioning

Access requests require management approval and shall be granted according to business role and customer contractual requirements.

6. Privileged Access

Administrative privileges shall be restricted, approved, periodically reviewed and used only for authorised business activities.

7. Authentication

Strong passwords are required. Multi-factor authentication should be enabled for cloud platforms, VPNs, privileged accounts and externally accessible systems where supported.

8. Remote Access

Remote access must use approved secure methods such as VPN or equivalent encrypted connections. Public or unmanaged devices shall only be used where authorised.

9. Access Reviews

Managers and system owners should review user access periodically to verify continuing business need and remove unnecessary permissions.

10. Joiner, Mover, Leaver

Access shall be provisioned for new personnel, modified when roles change and removed promptly upon termination or contract completion.

11. Third-Party Access

Supplier and customer access shall be approved, time-bound where appropriate and removed when no longer required.

12. Logging & Monitoring

Authentication events, privileged actions and access failures should be logged where practical and retained according to operational requirements.

13. Exceptions

Exceptions require documented approval by management and appropriate compensating controls.

14. Compliance

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

15. Review

The policy shall be reviewed annually or after significant organisational, regulatory or technology changes.