TekGenio Inc.
Identity & Access Management (IAM) Policy
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This policy establishes TekGenio's Identity and Access Management (IAM) requirements to ensure only authorised users have appropriate access to company and customer information systems.

2. Scope

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

3. IAM Principles

Identity management shall follow least privilege, need-to-know, segregation of duties, accountability and lifecycle management.

4. Identity Lifecycle

User identities shall be created, modified and removed through a controlled Joiner-Mover-Leaver (JML) process with documented approvals.

5. Authentication

Unique user IDs are required. Strong passwords are mandatory and multi-factor authentication (MFA) should be enabled for privileged, cloud and remote access wherever supported.

6. Authorisation

Access shall be role-based (RBAC) where practical. System owners approve access according to business responsibilities and contractual obligations.

7. Privileged Access

Administrative accounts shall be limited, periodically reviewed and used only for authorised administrative activities. Shared privileged accounts should be avoided.

8. Service Accounts

Service and application accounts shall be documented, secured, assigned an owner and reviewed periodically. Credentials must be protected and rotated where appropriate.

9. Access Reviews

Managers and system owners should perform periodic reviews to confirm access remains appropriate and remove unnecessary permissions.

10. Logging & Monitoring

Authentication events, privilege changes and significant access events should be logged and monitored to support investigations and compliance.

11. Third-Party Access

Supplier and customer identities shall be approved, limited to business need and removed promptly when no longer required.

12. Remote Access

Remote access must use approved secure technologies such as VPN or equivalent encrypted methods and comply with company security requirements.

13. Compliance

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

14. Exceptions

Exceptions require documented management approval and appropriate compensating controls.

15. Review

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