# TekGenio Inc.
# Password Standard
# Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

# 1. Purpose

This standard defines the minimum password and authentication requirements for protecting TekGenio information systems, customer environments and cloud services.

# 2. Scope

Applies to all employees, contractors, consultants, interns, third parties and service accounts with access to TekGenio-managed systems.

# 3. Password Requirements

Passwords shall be at least 12 characters long and should use a passphrase consisting of a combination of upper-case letters, lower-case letters, numbers and special characters where supported.

# 4. Password Creation

Passwords shall be unique for each system and must not contain easily guessed information such as names, birthdays, company names or dictionary words alone.

# 5. Password Storage

Passwords must never be stored in plain text. Approved password managers should be used to securely store credentials where appropriate.

# 6. Password Sharing

Sharing passwords is prohibited except where a formally approved technical process exists for emergency administrative access.

# 7. Multi-Factor Authentication

Multi-factor authentication (MFA) should be enabled for cloud platforms, VPN access, privileged accounts, administrative systems and externally accessible applications wherever technically supported.

# 8. Service Accounts

Service account credentials shall be securely stored, assigned to an owner and rotated periodically according to business and technical requirements.

# 9. Password Reset

Password reset requests shall verify user identity before credentials are changed.

# 10. Compromised Credentials

Suspected compromised passwords must be changed immediately and reported to the IT or security function for investigation where appropriate.

# 11. Monitoring

Authentication failures and suspicious login attempts should be logged and monitored where practical.

# 12. Compliance

This standard supports ISO/IEC 27001, CIS Controls, NIST guidance and applicable customer security requirements.

# 13. Exceptions

Exceptions require documented management approval and compensating security controls.

# 14. Review

This standard shall be reviewed annually or following significant technology or regulatory changes.