TekGenio Inc.
Encryption Standard
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This standard defines the minimum encryption requirements for protecting TekGenio and customer information throughout its lifecycle.

2. Scope

Applies to all information systems, cloud services, databases, applications, endpoints, removable media and communication channels used by TekGenio personnel and authorised third parties.

3. Objectives

Ensure confidentiality, integrity and protection of sensitive information using industry-recognised cryptographic controls.

4. Data Classification

Confidential and Restricted information shall be encrypted when stored and transmitted. Internal information should be protected based on business risk.

5. Encryption in Transit

Sensitive information transmitted across public or untrusted networks shall use secure protocols such as TLS 1.2 or later, HTTPS, SFTP, SSH or VPN technologies as appropriate.

6. Encryption at Rest

Where appropriate, sensitive data stored on servers, databases, laptops, cloud storage and removable media should be protected using strong encryption such as AES-256 or equivalent.

7. Key Management

Cryptographic keys shall be protected from unauthorised access, assigned ownership, rotated where appropriate and stored separately from encrypted data whenever practical.

8. Certificates

Digital certificates used for HTTPS, APIs and other secure communications shall be obtained from trusted certificate authorities and renewed before expiry.

9. Portable Media

Approved encryption shall be applied before storing Confidential or Restricted information on portable devices or removable media.

10. Email & File Transfer

Sensitive information shared externally should use approved encrypted communication methods or secure file transfer mechanisms.

11. Cloud Services

Cloud platforms should provide encryption capabilities for stored information and encrypted communications between services wherever supported.

12. Backup Encryption

Backups containing sensitive information should be encrypted and protected throughout storage, transport and restoration processes.

13. Exceptions

Exceptions require documented management approval and implementation of appropriate compensating controls.

14. Compliance

This standard aligns with ISO/IEC 27001:2022, NIST Cybersecurity Framework, CIS Controls and contractual customer security requirements.

15. Review

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