# TekGenio Inc.
# Patch Management Policy
# Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

# 1. Purpose

This policy establishes the requirements for identifying, testing, approving, deploying and verifying security patches and software updates across TekGenio-managed systems and customer environments where contractually applicable.

# 2. Scope

Applies to servers, workstations, cloud resources, network devices, operating systems, applications, databases, virtual machines, containers and third-party software managed by TekGenio.

# 3. Objectives

Reduce security risk by ensuring vulnerabilities are remediated in a timely, controlled and documented manner while minimising business disruption.

# 4. Roles and Responsibilities

Executive Management provides oversight. IT and Infrastructure teams coordinate patch deployment. System owners approve maintenance windows. Project teams validate application functionality after updates.

# 5. Asset Inventory

Systems shall be inventoried to ensure applicable patches can be identified and tracked.

# 6. Patch Identification

Security advisories from software vendors, cloud providers and trusted security sources should be monitored regularly for applicable updates.

# 7. Risk Prioritisation

Patches should be prioritised based on vulnerability severity, exploitability, business criticality and customer commitments.

# 8. Testing

Patches should be tested in a non-production environment where practical before production deployment to reduce operational risk.

# 9. Deployment

Approved patches shall be deployed during authorised maintenance windows using documented change management procedures.

# 10. Emergency Patching

Critical security vulnerabilities that present significant business risk may require expedited deployment following appropriate approval and risk assessment.

# 11. Verification

Following deployment, systems should be validated to confirm successful installation and expected service operation.

# 12. Rollback

Rollback procedures shall be documented for critical systems to enable recovery if an update causes unacceptable impact.

# 13. Documentation

Patch activities, approvals, exceptions and deployment results should be recorded and retained according to operational requirements.

# 14. Exceptions

Deferred patches require documented risk acceptance, compensating controls and periodic review.

# 15. Compliance

This policy aligns with ISO/IEC 27001:2022, NIST Cybersecurity Framework, CIS Controls v8 and customer contractual security obligations.

# 16. Review

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