TekGenio Inc.
Incident Response Plan
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This Incident Response Plan establishes a structured process for identifying, reporting, analysing, containing, eradicating, recovering from and learning from information security incidents affecting TekGenio or customer environments.

2. Scope

Applies to employees, contractors, third parties, cloud services, applications, infrastructure, AI solutions, customer data and managed environments.

3. Incident Categories

Examples include malware, phishing, ransomware, unauthorised access, data breaches, denial-of-service, insider threats, cloud security events, AI-related incidents and third-party security events.

4. Roles & Responsibilities

Executive Management provides oversight; the Incident Coordinator manages response; IT and Engineering perform technical investigation; Privacy Coordinator manages personal data incidents; Communications coordinates customer notifications where required.

5. Incident Lifecycle

Preparation → Detection & Reporting → Triage → Containment → Eradication → Recovery → Post-Incident Review.

6. Detection & Reporting

Personnel must report suspected incidents immediately through approved reporting channels. Security events should be logged and assessed without undue delay.

7. Triage

Incidents should be classified by severity, business impact, affected assets and urgency to determine the required response.

8. Containment

Short-term and long-term containment measures should be implemented to minimise business impact while preserving evidence where practical.

9. Eradication

Malicious software, compromised accounts, vulnerable services or unauthorised access shall be removed before systems return to normal operation.

10. Recovery

Affected systems shall be restored from trusted sources, validated and monitored to ensure secure operation before returning to production.

11. Evidence Handling

Logs and other relevant evidence should be preserved to support investigation, legal requirements and customer obligations.

12. Customer & Regulatory Notification

Customers and regulators shall be notified when required by contractual obligations or applicable law.

13. Lessons Learned

Following significant incidents, a post-incident review should identify root causes, corrective actions and opportunities for continuous improvement.

14. Testing

Incident response tabletop exercises and technical simulations should be conducted periodically to validate readiness.

15. Compliance

This plan aligns with ISO/IEC 27035, ISO/IEC 27001:2022, NIST SP 800-61 Rev.2, NIST CSF 2.0 and applicable contractual requirements.

16. Review

This plan shall be reviewed annually or after any major incident, organisational change or significant technology update.