

TekGenio Inc.
Business Continuity Plan (BCP)
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This Business Continuity Plan (BCP) establishes the framework for maintaining and restoring critical business operations following disruptive events while protecting employees, customers, information assets and contractual commitments.

2. Scope

Applies to all TekGenio business operations, personnel, customer projects, cloud platforms, software development, AI/ML services, ERP implementations, data analytics, managed services and supporting infrastructure.

3. Objectives

Minimise business disruption, protect critical information, ensure continuity of customer services, and enable timely recovery of essential operations.

4. Governance

Executive Management is responsible for approving the BCP. Business unit leaders, IT teams and project managers are responsible for implementing continuity procedures within their respective functions.

5. Business Impact Analysis

Critical business processes shall be identified, prioritised and periodically reviewed. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) should be established for essential services.

6. Risk Assessment

Business continuity planning shall consider cyber incidents, cloud service outages, natural disasters, utility failures, pandemics, supplier failures, human error and other operational disruptions.

7. Response & Continuity Procedures

Personnel shall follow documented procedures for incident escalation, emergency communications, continuity of customer support, remote working and restoration of critical services.

8. Alternate Working Arrangements

Where practical, personnel should be capable of securely performing critical business activities through approved remote working arrangements or alternate locations.

9. Communication

Internal and external communication procedures shall ensure timely notification to employees, customers, suppliers and other stakeholders during significant disruptions.

10. Dependencies

Critical suppliers, cloud providers, telecommunications services and technology platforms supporting business operations should be identified and periodically reviewed.

11. Training & Exercises

Business continuity awareness shall be provided to relevant personnel. Continuity plans should be tested periodically through tabletop exercises or simulations.

12. Plan Maintenance

The BCP shall be reviewed following significant organisational, technological or regulatory changes and after major incidents or exercises.

13. Compliance

This plan aligns with ISO 22301, ISO/IEC 27001:2022, NIST Cybersecurity Framework and applicable contractual obligations.

14. Review

This Business Continuity Plan shall be reviewed at least annually and approved by Executive Management.