TekGenio Inc.
Disaster Recovery Plan (DRP)
Version 1.0

Document Classification: Internal Use
Review Frequency: Annual

1. Purpose

This Disaster Recovery Plan (DRP) establishes the procedures required to restore critical IT services, applications, infrastructure and customer environments following a disaster or major service disruption.

2. Scope

Applies to TekGenio-managed servers, cloud infrastructure, applications, ERP platforms, AI/ML solutions, databases, networking components, development environments and supporting services.

3. Objectives

Restore critical systems within agreed Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), minimise downtime, protect customer data and maintain business continuity.

4. Disaster Recovery Governance

Executive Management provides strategic oversight. IT & Infrastructure teams coordinate technical recovery. System owners validate restored services before returning them to production.

5. Disaster Scenarios

Recovery procedures should address cyber attacks, ransomware, cloud outages, hardware failures, software corruption, database failures, power outages, natural disasters and loss of key facilities.

6. Recovery Priorities

Critical services shall be prioritised according to business impact analysis, contractual obligations and operational dependencies.

7. Backup & Restoration

Approved backups shall be maintained and restoration procedures tested periodically to verify recoverability of business-critical information and systems.

8. Recovery Procedures

Recovery activities include infrastructure restoration, operating system recovery, application deployment, database recovery, network validation, identity services restoration and functional verification.

9. Communication

Internal stakeholders, customers and relevant suppliers shall be informed in accordance with the Business Continuity Plan and Incident Response Plan where appropriate.

10. Testing & Validation

Disaster recovery exercises should be conducted periodically to validate recovery procedures, RTO/RPO objectives and technical readiness.

11. Documentation

Recovery procedures, system inventories, architecture information, contact details and recovery results should be maintained and reviewed regularly.

12. Continuous Improvement

Lessons learned from recovery exercises and actual incidents shall be incorporated into future revisions of the Disaster Recovery Plan.

13. Compliance

This plan aligns with ISO 22301, ISO/IEC 27001:2022, NIST SP 800-34 Rev.1, NIST Cybersecurity Framework and applicable customer contractual obligations.

14. Review

This Disaster Recovery Plan shall be reviewed annually or following major infrastructure, business or regulatory changes.