POLICY DOCUMENT

Business Continuity

Policy

Organisation: [Organisation Name]
Version: 1.0
Effective Date: [Date]
Review Date: [Date + 12 months]
Policy Owner: [Name / Role]

Prepared by [IT Provider Name]

IMPORTANT — KEEP ACCESSIBLE OFFLINE
A printed copy of this document must be held by the Business Continuity Coordinator and stored in a secure location accessible without IT systems.

---

1. Purpose

[Organisation Name] depends on its people, systems, premises, and suppliers to deliver services to clients. Disruptions — whether from a cyber incident, natural disaster, pandemic, power failure, or supplier failure — can cause significant harm if not managed effectively.

This Business Continuity Policy establishes the framework within which [Organisation Name] will prepare for, respond to, and recover from disruptions to maintain or rapidly restore critical functions and meet its obligations to clients, staff, and regulators.

---

2. Scope

This Policy applies to all business functions, services, and processes delivered by [Organisation Name]; all staff, contractors, and volunteers; and all premises, systems, and suppliers on which the organisation depends.

---

3. Business Continuity Objectives

In the event of a disruption, [Organisation Name] will prioritise:

- The safety and wellbeing of staff, clients, and visitors

- The protection of client data and personal information in accordance with the Privacy Act 2020
- The continuation of critical services to clients
- Compliance with all legal and regulatory obligations
- The protection of the organisation's reputation and financial position

---

4. Business Impact Analysis

A Business Impact Analysis has been conducted to identify the organisation's critical functions and the maximum tolerable period of disruption for each. The analysis is reviewed annually.

Critical Function	Dependencies	Max Downtime	Recovery Priority
[e.g. Client communications]	[Systems / people]	[e.g. 4 hours]	1 — Critical
[e.g. Financial processing]	[Systems / people]	[e.g. 24 hours]	2 — High
[e.g. Reporting]	[Systems / people]	[e.g. 5 days]	3 — Medium

---

5. Disruption Scenarios

Cyber Incident

Including ransomware, data breach, or extended system outage. Response procedures are set out in the Cyber Incident Response Plan.

Loss of Premises

Including fire, flood, or earthquake rendering the primary workplace inaccessible. The organisation will activate remote working arrangements and, where required, alternative premises at [location].

Loss of IT Systems

Including extended outage of core business systems, cloud services, or internet connectivity. The organisation will activate offline working procedures and manual workarounds.

Loss of Key Personnel

Including sudden unavailability of key staff due to illness or emergency. Succession plans and cross-training must ensure critical functions can continue.

Supplier Failure

Including the failure of a critical supplier or service provider. The organisation maintains a register of critical suppliers and alternative arrangements for key services.

Pandemic or Public Health Emergency

Remote working capability is maintained as a standing arrangement for all staff whose role permits it.

Natural Disaster

The organisation is located in [region] and has assessed the relevant hazards. Emergency supplies and contact lists are maintained at [location].

---

6. Recovery Strategies

Remote Working

All staff whose roles permit remote working must be capable of doing so at short notice. [IT Manager / IT Provider] maintains remote access capability for all applicable staff.

Alternative Premises

In the event the primary premises are unavailable, the organisation will operate from [alternative location]. [IT Manager / IT Provider] will restore minimum IT capability within [target time].

Manual Workarounds

Process	Normal System	Manual Workaround
[Process name]	[System]	[Manual procedure]
[Process name]	[System]	[Manual procedure]

Backup and Data Recovery

Data backup and recovery is managed by [IT Manager / IT Provider] using Veeam Backup and Replication for on-premises workloads and Veeam Backup for Microsoft 365 for cloud data.

Emergency Communications

If primary communication systems are unavailable, the organisation will use staff mobile phones (maintained in the contact list in section 7), and where necessary personal email for temporary external communications containing no confidential data.

---

7. Business Continuity Team

Role	Name	Mobile	Responsibility
Business Continuity Coordinator	[Name]	[Mobile]	Overall coordination of continuity response
IT Lead — [IT Provider Name]	[Name]	[IT Provider Phone]	IT systems, backups, remote access
Operations Lead	[Name]	[Mobile]	Core service delivery and staff coordination
Finance Lead	[Name]	[Mobile]	Financial transactions and payroll continuity

Communications Lead	[Name]	[Mobile]	Client and external communications

---

8. Critical Suppliers

Supplier	Service	Contact	Alternative if Unavailable
[IT Provider Name]	IT support, backups, security	[IT Provider Phone]	[Alternative IT provider]
Microsoft	Microsoft 365, Azure	microsoft.com	Backup comms via personal email
[Supplier]	[Service]	[Contact]	[Alternative]

---

9. Invoking Business Continuity Arrangements

Upon invocation, the Business Continuity Coordinator will:

1. Assess the nature and likely duration of the disruption
2. Notify the Business Continuity Team via phone or alternate communication method
3. Activate the relevant plan for the affected function(s)
4. Notify affected clients and stakeholders as appropriate
5. Establish a regular status update cadence — at minimum every four hours for critical disruptions
6. Document all actions and decisions throughout the response

---

10. Privacy During Disruption

The Privacy Act 2020 continues to apply during a disruption. Staff must not store personal information on personal devices without approval, share personal information with unauthorised parties, or discard physical records without secure destruction. Where a disruption results in a notifiable privacy breach, the Privacy Officer must be notified immediately.

---

11. Insurance

Policy Type	Insurer	Policy Number	Broker Contact
Cyber Liability	[Insurer]	[Policy No.]	[Contact]
Business Interruption	[Insurer]	[Policy No.]	[Contact]

Professional Indemnity	[Insurer]	[Policy No.]	[Contact]

12. Testing

Business continuity arrangements must be tested at least annually through tabletop exercises, IT failover tests, communication tests, and remote working tests. Test outcomes will be documented and improvements actioned within 30 days. [IT Manager / IT Provider] will assist with planning and facilitation of annual tests.

13. Related Documents

- Cyber Incident Response Plan
- Acceptable Use Policy
- Artificial Intelligence Acceptable Use Policy

Acknowledgement

I confirm that I have read and understood the Business Continuity Policy and my responsibilities within it.

Full Name

Role

Signature

Date

Document Control

Version	Date	Author	Summary of Changes
1.0	[Date]	[IT Provider Name]	Initial version

Prepared by [IT Provider Name] | [IT Provider Website] | [IT Provider Phone]