BUSINESS CONTINUITY TESTING AND EMERGENCY RESPONSE PROCEDURE

Procedure Title: PRN-011: Business Continuity Testing and Emergency Response Procedure

Company Name: AI Auto-Tech Ltd
Trading/Business Name: Trusted Companionship
Company Registration Number: 15556946
SIC Code: 88100 – Social Work Activities Without Accommodation for the Elderly and Disabled
Email: info@trustedcompanionship.com
Version Number: V01 20260815
Date of Review: (August 2026)

---

1. Purpose

This procedure provides practical guidance for preparing for, responding to, managing, testing, and reviewing emergency situations that may affect the organisation's ability to deliver services.

The organisation recognises that emergencies and disruptive incidents can impact service users, volunteers, employees, information systems, buildings, suppliers, and community activities.

This procedure aims to:

Support the safety of people.

Minimise service disruption.

Protect critical services.

Promote effective emergency responses.

Strengthen organisational resilience.

Ensure business continuity arrangements remain effective.

---

2. Scope

This procedure applies to:

Employees

Volunteers

Managers

Directors

Trustees

Contractors where relevant

The procedure applies to emergencies and disruptive incidents affecting organisational activities.

---

3. Principles

Emergency response arrangements will be:

Safety Focused

Protecting people from harm.

Organised

Providing a structured response.

Proportionate

Reflecting the nature and scale of the incident.

Collaborative

Working with external agencies where necessary.

Learning Focused

Using incidents and exercises to improve preparedness.

---

4. Types of Emergencies

Examples may include:

Severe weather

Flooding

Fire

Major power outage

Telecommunications failure

IT or cyber incident

Pandemic or infectious disease outbreak

Loss of key personnel

Serious safeguarding incident

Community emergency

Security incident

Transport disruption

Loss of premises

This list is not exhaustive.

---

5. Activation of the Procedure

This procedure may be activated where an incident:

Prevents normal service delivery.

Creates significant risk.

Affects critical operations.

Disrupts communication.

Threatens organisational stability.

Activation may be authorised by:

Director

Senior Manager

Designated Emergency Lead

---

6. Initial Emergency Response

Upon becoming aware of an emergency:

Step 1

Ensure immediate safety.

Step 2

Contact emergency services where required.

Step 3

Notify management.

Step 4

Assess immediate risks.

Step 5

Implement emergency arrangements.

Step 6

Record key actions taken.

---

7. Emergency Contact Arrangements

Emergency contact information should be maintained for:

Employees

Volunteers

Key managers

Trustees

Service providers

Emergency services

Partner organisations

Contact information should be reviewed regularly.

---

8. Roles and Responsibilities During Emergencies

Emergency Lead

Responsible for:

Coordinating the response.

Making operational decisions.

Communicating updates.

Liaising with external agencies.

Managers

Responsible for:

Supporting implementation.

Monitoring staff and volunteer welfare.

Reporting developments.

Employees and Volunteers

Responsible for:

Following instructions.

Prioritising safety.

Reporting concerns promptly.

---

9. Communication During Emergencies

Effective communication is essential.

Communication may be required with:

Service users

Families or carers

Employees

Volunteers

Trustees

Emergency services

Partner agencies

Information should be:

Accurate

Clear

Timely

Appropriate

---

10. Service User Welfare Checks

Where service disruption may affect vulnerable individuals:

Welfare risks should be assessed.

Appropriate contact should be attempted.

Alternative support options should be considered.

Safeguarding concerns should be escalated.

Priority should be given to individuals at greatest risk.

---

11. Alternative Service Delivery

Where normal arrangements cannot continue, alternative approaches may include:

Telephone support.

Online support.

Rescheduled visits.

Alternative venues.

Partner support arrangements.

Alternative arrangements should be communicated clearly.

---

12. Premises-Related Emergencies

Where premises become unavailable:

Immediate Actions

Ensure evacuation if required.

Account for individuals present.

Contact emergency services if appropriate.

Follow-Up Actions

Identify temporary working arrangements.

Communicate with affected individuals.

Assess operational impact.

---

13. IT and Cyber Incident Response

Where IT systems are affected:

Notify management immediately.

Follow cyber incident procedures.

Restrict affected systems where necessary.

Assess operational impact.

Activate alternative arrangements.

Relevant cyber security procedures should also be followed.

---

14. Severe Weather Response

Potential actions may include:

Reviewing travel risks.

Postponing activities.

Delivering services remotely.

Communicating cancellations promptly.

Monitoring service user wellbeing.

Safety should remain the primary consideration.

---

15. Infectious Disease and Public Health Incidents

Where public health concerns arise:

Follow official guidance.

Assess service delivery implications.

Implement infection prevention measures.

Communicate changes to stakeholders.

Business continuity arrangements may need to be modified.

---

16. Loss of Key Personnel

Where critical personnel become unavailable:

Activate contingency arrangements.

Reassign responsibilities.

Review service priorities.

Inform relevant stakeholders.

Succession planning should support operational resilience.

---

17. Emergency Decision Log

During significant incidents, a decision log should be maintained.

The log should record:

Date and time.

Key decisions.

Decision-makers.

Actions taken.

Rationale for decisions.

Accurate records support accountability and learning.

---

18. Business Continuity Priorities

The organisation should identify priorities such as:

Priority 1

Safety and welfare.

Priority 2

Safeguarding responsibilities.

Priority 3

Critical service delivery.

Priority 4

Communication.

Priority 5

Organisational recovery.

---

19. Recovery Phase

Following an emergency, the organisation should:

Review operational status.

Restore disrupted services.

Support affected individuals.

Assess ongoing risks.

Update stakeholders.

Recovery actions should be proportionate to the incident.

---

20. Business Continuity Testing

Business continuity arrangements should be tested periodically.

The purpose of testing is to:

Assess preparedness.

Identify weaknesses.

Improve response capability.

Increase confidence in procedures.

Testing should be proportionate to organisational size and complexity.

---

21. Types of Testing

Testing methods may include:

Desktop Exercises

Scenario-based discussions.

Tabletop Exercises

Structured emergency simulations.

Communication Tests

Testing emergency contact arrangements.

Practical Exercises

Testing operational response arrangements.

System Recovery Tests

Testing critical technology arrangements where appropriate.

---

22. Frequency of Testing

Business continuity arrangements should normally be reviewed and tested:

At least annually.

Following significant changes.

Following major incidents.

Following identified weaknesses.

Additional testing may be undertaken where risks increase.

---

23. Conducting a Test Exercise

A test exercise should:

Step 1

Identify objectives.

Step 2

Select a scenario.

Step 3

Conduct the exercise.

Step 4

Record observations.

Step 5

Identify lessons learned.

Step 6

Implement improvements.

---

24. Example Testing Scenarios

Scenarios may include:

IT system failure.

Volunteer shortage.

Severe weather disruption.

Cyber attack.

Loss of office access.

Pandemic response.

Communication system failure.

Testing should reflect identified organisational risks.

---

25. Recording Test Results

Records should include:

Exercise date.

Participants.

Scenario used.

Strengths identified.

Weaknesses identified.

Improvement actions.

Responsible persons.

Records should be retained securely.

---

26. Learning and Improvement

Following testing or real incidents:

Lessons learned should be documented.

Improvement plans should be developed.

Policies and procedures should be reviewed.

Training needs should be identified.

Continuous learning strengthens resilience.

---

27. Emergency Response Flowchart

Emergency Identified

↓

Ensure Immediate Safety

↓

Emergency Services Required?

Yes → Contact 999

No → Continue Assessment

↓

Notify Management

↓

Activate Business Continuity Arrangements

↓

Communicate With Stakeholders

↓

Implement Alternative Service Arrangements

↓

Monitor Situation

↓

Recovery and Service Restoration

↓

Review and Learning

---

28. Case Study

Scenario: Severe Snowfall Disruption

Heavy snowfall affects travel across the local area, preventing volunteers from undertaking planned companionship visits.

Action Taken

Travel risks are assessed.

Community visits are temporarily suspended.

Welfare telephone calls are arranged.

Service users and volunteers are informed.

Priority welfare concerns are reviewed.

Outcome

Service user welfare is maintained while travel risks are reduced.

Learning Point

Alternative service arrangements can help maintain continuity during significant disruption.

---

29. Responsibilities

Board of Trustees

Responsible for:

Oversight of organisational resilience.

Reviewing major incidents.

Supporting business continuity planning.

Directors

Responsible for:

Activating continuity arrangements.

Coordinating major responses.

Providing leadership during incidents.

Managers

Responsible for:

Implementing response actions.

Supporting teams.

Recording incidents and actions.

Employees and Volunteers

Responsible for:

Following emergency instructions.

Reporting concerns promptly.

Supporting safe service delivery.

---

30. Monitoring and Quality Assurance

The organisation will monitor:

Emergency incidents.

Business continuity tests completed.

Recovery times.

Communication effectiveness.

Lessons learned.

Improvement actions.

Staff and volunteer preparedness.

Findings will be reported through governance and quality assurance arrangements.

---

31. Review Arrangements

This procedure will be reviewed:

Annually.

Following major incidents.

Following business continuity exercises.

Following legislative or regulatory changes.

Following organisational restructuring.

Related Policies

Business Continuity and Emergency Planning Policy

Health and Safety Policy

Incident Reporting Policy

Information Governance and Cyber Security Policy

Risk Assessment Policy

Lone Working Policy

Adult Safeguarding Policy

Governance, Board and Trustee Responsibilities Policy