



TMPPM CORPORATE DOCUMENT

BUSINESS CONTINUITY PLAN

2026 – 2027

GOVERNANCE WITH
CLARITY, CARE AND
INTEGRITY.

DOCUMENT CONTROL AND PURPOSE



- **Document: Business Continuity Plan (BCP)**
- Author: Taylor Made Project Management Ltd (TMPPM)
- Version: 1.0
- Date: 17 April 2026
- Approved by: Chris Taylor, TMPPM Director

CONTENTS

- 01 Purpose, Scope and Key Objectives**
- 02 Critical Business Functions**
- 03 Risk Assessment and Business Impact**
- 04 Continuity Strategies**

- 05 Incident Response Structure**
- 06 Communication and Recovery**
- 07 Testing, Review and Responsibilities**

PURPOSE, SCOPE AND KEY OBJECTIVES



- **Continue critical services during and after disruption.**
- Maintain consultancy delivery, stakeholder engagement and contractual commitments across NHS, local government and wider health and care.
- Applies to staff, associates, contractors, consultancy services, digital systems and client-facing activity.
- Protect people, minimise impact, maintain compliance and enable rapid recovery.

CRITICAL BUSINESS FUNCTIONS



- **Priority 1 – within 24 hours: programme leadership, client communications, critical milestones and safeguarding advice.**
- Priority 2 – within 48-72 hours: governance reporting, bids and stakeholder workshops.
- Priority 3 – within 5-7 days: business development, marketing and internal improvement.

RISK ASSESSMENT AND BUSINESS IMPACT



- **Key risks: loss of personnel, cyber or IT failure, loss of site/data access, associate supply disruption, reputation and regional/national emergencies.**
- Client programme delivery and client communications: critical, tolerable downtime under 24 hours.
- Bid submissions: high priority, 48 hours. Internal operations: medium priority, 3-5 days.

CONTINUITY STRATEGIES



- **Workforce: flexible associate cover, cross-training, current contacts and escalation routes.**
- Remote delivery: cloud collaboration, secure access and fully remote capability.
- Client continuity: named leads/deputies, agreed contingencies and regular communications.
- Data and IT: secure cloud backup, MFA, cybersecurity controls and recovery testing.

INCIDENT RESPONSE STRUCTURE



- **Incident Lead: Director / Managing Consultant.**
- Response team: programme leads, business support and IT/data support where applicable.
- Identify -> assess -> activate BCP -> communicate -> implement continuity actions -> monitor and review.

COMMUNICATION AND RECOVERY



- **Internal notification via email / Teams with daily situation updates where required.**
- Clients informed within 4-24 hours according to severity, including impact, mitigation and revised timelines.
- Restore critical services first, reallocate resources, use the associate network and complete a post-incident review.

TESTING, REVIEW AND RESPONSIBILITIES



- **Review annually and test scenarios such as IT failure or staff absence.**
- Improve continuously using client feedback, delivery experience and system pressures.
- Director accountable; programme leads manage continuity and client liaison; associates provide flexibility; business support coordinates communications.
- Aligned to resilience, partnership, delivery excellence and Fit for the Future.