



# Business Continuity & Resilience Policy

Continuity arrangements for client delivery, cloud systems, production assets and key personnel.

|                           |                          |
|---------------------------|--------------------------|
| <b>Document reference</b> | BC-POL-012               |
| <b>Version</b>            | 2.0                      |
| <b>Status</b>             | Approved for publication |
| <b>Approval date</b>      | 08 August 2026           |
| <b>Next review</b>        | 08 August 2027           |

Legal entity: Becks & Clates Ltd | Company number: 15821561  
Registered office: 320 Firecrest Court, Centre Park, Warrington, WA1 1RG  
Approved by: Director, Becks & Clates Ltd

## Document control

|                       |                                                                                      |
|-----------------------|--------------------------------------------------------------------------------------|
| <b>Document title</b> | Business Continuity & Resilience Policy                                              |
| <b>Reference</b>      | BC-POL-012                                                                           |
| <b>Owner</b>          | Director                                                                             |
| <b>Approved by</b>    | Director, Becks & Clates Ltd                                                         |
| <b>Version</b>        | 2.0                                                                                  |
| <b>Effective date</b> | 08 August 2026                                                                       |
| <b>Review cycle</b>   | At least annually and following material legal, operational or organisational change |

Document status: public. Printed copies are uncontrolled. The version published by Becks & Clates is the current controlled version.

## Contents

1. Purpose and objectives
2. Critical activities
3. Roles and escalation
4. Technology and data continuity
5. Production continuity
6. People and premises
7. Supplier and financial resilience
8. Incident process
9. Testing and review

## Purpose and objectives

Becks & Clates maintains proportionate continuity arrangements so that foreseeable disruption can be managed without unnecessary harm to clients, personnel or data.

The policy covers loss of office access, device failure, cyber incidents, key-person absence, supplier failure, cloud outages, travel disruption, equipment loss and significant production interruption.

## Critical activities

| Activity                        | Priority | Target restoration / workaround                                 |
|---------------------------------|----------|-----------------------------------------------------------------|
| Client emergency communications | Critical | Within 4 hours where practicable                                |
| Email / collaboration           | High     | Within 8 hours or approved alternative                          |
| Access to active project files  | High     | Within 24 hours from available backup/redundant service         |
| Time-critical production        | High     | Same day assessment and client communication                    |
| Finance / invoicing / payroll   | Medium   | Within 3 business days or before statutory/contractual deadline |
| Website / general marketing     | Medium   | Restore as reasonably practicable; client                       |

|  |  |                         |
|--|--|-------------------------|
|  |  | delivery takes priority |
|--|--|-------------------------|

*Targets are operational objectives rather than absolute guarantees; severe regional or supplier-wide incidents may require alternative arrangements.*

## Roles and escalation

- The Director leads material business-continuity incidents and determines priorities.
- Project leads maintain client contact and assess delivery impact.
- Technical support/suppliers are engaged where systems or infrastructure are affected.
- Personnel must report incidents promptly and avoid uncoordinated external statements.

## Technology and data continuity

- Important business systems are cloud-based or otherwise capable of remote access where practical.
- Active project data is backed up or stored redundantly proportionate to project risk.
- Account recovery information and administrative access are maintained securely.
- Cyber incidents are managed under the Cyber Security and Data Protection policies.
- Alternative communications channels may be used where normal email or collaboration systems are unavailable.

## Production continuity

- Critical shoots are planned with suitable contacts, access details and contingency time where feasible.
- Replacement or rental equipment can be sourced where owned equipment fails or is unavailable.
- Freelance and supplier networks may provide alternative crew subject to competence, confidentiality and client requirements.
- Weather, travel and site restrictions are assessed early; postponement is preferred to unsafe improvisation.
- If a material deadline is threatened, the client is informed promptly with realistic options.

## People and premises

- Remote working provides a practical alternative where office access is lost.
- Key procedures and project records should not exist solely in one person's memory.
- Work is reassigned where a key person is unexpectedly unavailable.
- Health, safety and welfare take priority over maintaining normal operations during emergencies.

## Supplier and financial resilience

- Material supplier dependencies are identified during project planning.
- Alternative freelancers, equipment hire, hosting/support or production services are used where proportionate.
- Critical subscriptions and insurance are kept current.
- Fraud controls remain in force during disruption; urgency must not bypass payment-verification procedures.

## Incident process

1. Identify and assess the incident, safety impact and affected clients/services.
2. Stabilise people, systems and data.
3. Prioritise critical commitments and activate workarounds.
4. Communicate with affected clients, personnel and suppliers.
5. Restore normal operations in a controlled manner.
6. Review causes, outcomes and improvements after the event.

## Testing and review

- Continuity arrangements are reviewed at least annually.
- Key contact, backup and access assumptions are checked periodically.
- Material incidents and significant supplier/system changes trigger a focused review.
- Lessons from outages, near misses and client feedback are incorporated into updated arrangements.