CONTROLLED COMPANY DOCUMENT

Business Continuity Plan

Maintaining safe, secure and accountable delivery through disruption.

Document owner: Max Pocock, Lead Consultant
Version: 1.0
Issued: 23 July 2026
Review due: 23 July 2027, and after every activation, exercise or material dependency change
Applies to: Managed Services Ltd's critical business operations and active client engagements

The continuity priority is to protect people and information, establish control, communicate early, preserve decision-ready work and restore the most important service first.

1. Purpose and operating context

This plan provides a proportionate continuity framework for a founder-led consultancy delivering through Max Pocock as Lead Consultant and, where required, separately confirmed human specialists or suppliers.

It does not assume a large permanent workforce, an automatically available deputy, duplicate specialist capacity or a certified business-continuity system. Each engagement must convert this company framework into a contract-specific continuity record based on its deadlines, data, dependencies, locations and impact.

No client delivery will rely on an unnamed or unconfirmed substitute. Access, confidentiality, competence, buyer approval and conflict checks apply before any substitute or recovery support receives client information.

2. Objectives

During disruption, Managed Services Ltd will:

- protect life, welfare and safeguarding;
- contain security, privacy and contractual harm;
- maintain or restore essential client communication;
- preserve critical records, evidence and decision history;
- prioritise accepted deliverables and time-sensitive obligations;
- give clients accurate information and options;
- use secure alternative working methods;

- recover in a controlled sequence; and
- learn from the incident and improve resilience.

3. Activation

Max Pocock may activate this plan where an incident threatens a critical activity, deadline, person, system, location, supplier or information asset beyond routine workarounds.

Anyone acting for the company must escalate a potentially material disruption immediately. If Max is unavailable, the confirmed contract-specific continuity contact may initiate protective and communication actions within their documented authority.

The incident record must state:

- what happened and when;
- immediate safety or security action;
- affected clients, activities, information and deadlines;
- incident lead and authorised support;
- continuity level and priorities;
- communications made and due;
- decisions, assumptions and owners; and
- recovery and review status.

4. Continuity priorities and planning targets

The following are default design targets, not a claim of a contractually guaranteed service level. Each engagement must confirm whether they are achievable, sufficient and tested.

Priority activity	Default recovery target	Maximum tolerable data gap	Continuity approach
Life safety, safeguarding and emergency action	Immediate	Not applicable	Stop unsafe work; use emergency, host and statutory routes
Client incident contact and delivery control	Within 4 business hours	Latest verified contact and decision record	Alternative device, connection and authorised contact list
Secure access to critical active engagement records	Within 1 business day	Up to 24 hours unless contract requires less	Approved backup, version history and restoration check

Priority activity	Default recovery target	Maximum tolerable data gap	Continuity approach
Time-critical analysis and deliverables	Within 2 business days or agreed contract target	Up to 24 hours for working files	Prioritised work package, recovery copy and controlled reassignment
Finance, supplier and ordinary administration	Within 3 business days	Up to 5 business days where lawful	Alternative records and deferred non-critical processing

Where a buyer requires a shorter target, the company must design, resource, price and test that stronger arrangement before committing to it.

5. Critical dependencies

The contract-specific continuity record will identify:

- Max Pocock's availability and authority;
- confirmed human specialists, suppliers and substitution constraints;
- client decision-makers and emergency contacts;
- secure devices, accounts, authentication and software;
- internet, telephone and alternative communications;
- active project records, source evidence and deliverable versions;
- backup location, frequency, access and restoration test;
- premises, travel, venue and remote-working needs;
- banking, invoicing and essential supplier services;
- contract notice, data-breach and regulatory obligations; and
- information that a recovery person would need to understand the current position.

Credentials must not be placed in the plan. The plan records how authorised access is recovered, not the secrets themselves.

6. Preventive controls

Managed Services Ltd will apply proportionate controls including:

- small, accepted delivery stages rather than a single final dependency;
- current action, decision, risk and version records;

- clear file naming and controlled source-to-output traceability;
- supported devices, security updates and multi-factor authentication where available;
- approved secure cloud or backup arrangements appropriate to the data;
- regular backup and proportionate restoration testing;
- alternative secure connectivity and working location;
- accessible offline copies of essential non-secret contacts and procedures;
- supplier due diligence and exit or substitution planning for critical services;
- time contingency before fixed buyer deadlines; and
- contract-specific handover information that can be released only to an authorised recovery person.

Business continuity does not justify weakening confidentiality, data protection, safeguarding, buyer approval or evidence controls.

7. Scenario responses

Max Pocock unavailable

Protect immediate safety and deadlines, activate the contract-specific contact route, tell the client what is known, identify decisions only Max can make, preserve records, and assess delay, authorised support or buyer-approved substitution.

A separately engaged human specialist may continue only within their confirmed role and authority. They do not automatically assume client communication, commercial decisions, final approval or contract accountability.

Human specialist or supplier unavailable

Stop assigning new work, secure and recover company or client records, assess confidentiality and access, identify the minimum affected work, and use a pre-assessed alternative only after competence, conflict, contract and buyer requirements are satisfied.

Cyber incident or personal-data breach

Disconnect or contain affected access where safe, preserve evidence, change compromised credentials, use a clean communication route, activate the Privacy and Data Protection Policy, notify the client promptly where required, and restore only from a trusted state.

Cloud, software or device outage

Confirm whether the failure is local or supplier-wide, use the approved alternative device, connection or offline work package, protect version integrity, avoid copying sensitive data into unapproved services, and reconcile all work after restoration.

Premises, power, weather or travel disruption

Move to the approved remote or alternative location, reschedule non-essential travel, protect paper and equipment, confirm participant and staff safety, and switch to remote delivery only where the method remains accessible, safe and contractually acceptable.

Client-side delay or access loss

Record the dependency and effect, protect the team from unproductive effort, re-sequence independent tasks, present options and decision dates, and use contract change control where scope, price or milestone impact is material.

8. Incident response sequence

1. **Protect:** address life safety, safeguarding, data exposure and immediate harm.
2. **Control:** appoint the incident lead, open the record and stop unsafe or unreliable work.
3. **Assess:** identify affected services, people, information, deadlines, dependencies and obligations.
4. **Communicate:** notify relevant clients and partners with verified facts, impact, current action and next update.
5. **Continue:** use the safest approved workaround for the highest-priority activity.
6. **Recover:** restore people, systems, records and delivery in a controlled order.
7. **Validate:** check security, completeness, calculations, versions and approvals before normal use.
8. **Learn:** record causes, effects, decisions, lessons and improvement owners.

9. Communication

Incident communications must be early, accurate and proportionate. They will state:

- what is known and not yet known;
- service or deadline impact;
- immediate protection and continuity action;
- decisions or support needed from the recipient;
- alternative contact route; and

- time of the next update.

Speculation, blame and unsupported assurance are prohibited. Only authorised people may communicate externally about the incident.

10. Recovery and return to normal

Before declaring recovery, the incident lead will confirm:

- people are safe and safeguarding concerns are managed;
- compromised access is removed and required notifications are complete;
- restored information is current, complete and trusted;
- calculations, evidence links and deliverable versions have been checked;
- clients understand the revised position;
- temporary workarounds are closed or formally accepted;
- missed obligations and commercial effects are recorded; and
- improvement actions have owners and dates.

11. Exercises, tests and maintenance

The plan will be:

- reviewed at least annually;
- checked when a critical supplier, system, delivery model or legal obligation changes;
- exercised proportionately before a high-impact or time-critical engagement;
- tested through restoration of a representative critical file or system;
- reviewed after every material incident or near miss; and
- updated where an action, contact or recovery assumption fails.

An exercise must be recorded as an exercise, not a live incident or proof of full operational resilience.

12. Contract-specific continuity record

Before a material engagement starts, the record will confirm:

- critical deliverables and dates;
- impact and maximum tolerable outage;
- recovery and data-gap objectives;

- Max's availability and protected capacity;
- authorised continuity contacts and their limits;
- confirmed human-specialist or supplier dependencies;
- client contacts and notice requirements;
- critical systems, data, backup and restoration evidence;
- alternative equipment, connectivity and work location;
- security, privacy and safeguarding overlays;
- manual work the buyer requires;
- last review or exercise; and
- unresolved gaps and stop conditions.

13. Official references

Official sources checked on 23 July 2026:

1. National Cyber Security Centre, Small Business Guide - Response and Recovery - View official source
2. National Cyber Security Centre, Prepare for incidents - View official source
3. National Cyber Security Centre, Small organisations guide to cyber security - View official source
4. Information Commissioner's Office, Personal data breaches - a guide - View official source

14. Document control

This plan is reviewed at least annually and after activation or exercise. Tender-specific copies must be reconciled with the contract, service criticality and actual tested controls before issue.