Business Continuity and Disaster Recovery Plan

for Subcontractors and Employees

Author

Mark Taylor

Date Issued

18th September 2026

Version
1.1

Business Continuity and Disaster Recovery Plan

CF POL 07 | Version 1.1 | Issued 18 September 2026

Owner and approver: Changing Footprint Director | Status: Issued
Reviewed and approved: 18 September 2026
Effective date: 18 September 2026 | Review date: 18 September 2027

PURPOSE ACTIVATION AND PRIORITIES

PURPOSE AND AUDIENCE

Changing Footprint will protect people and information and maintain or restore priority consultancy activities during disruption. This shareable plan explains responsibilities, decision-making and recovery steps for clients, employees, associates and subcontractors. Account credentials, personal contacts and system recovery details belong in a separate restricted operational schedule.

ACTIVATION

Activate this plan when illness, loss of key people, cyber incident, device loss, premises disruption, severe weather or supplier failure threatens safe delivery, information security or a material deadline. Anyone identifying disruption must notify Changing Footprint's Director immediately. Changing Footprint's Director acts as incident lead.

AUTHORITY AND LIMITS

The incident lead assesses impact, sets priorities, authorises proportionate expenditure within recorded delegated limits and coordinates communications. A nominated associate is not automatically authorised to access all client records.

WORKING PRIORITIES

First protect people and contain security risks. Next preserve evidence, identify urgent client and regulatory obligations and stabilise communications. Recover the information and systems needed for priority delivery, then restore lower-priority work. Do not reconnect compromised systems or bypass security simply to meet a deadline.

RECOVERY ACTIONS AND TARGETS

FIRST RESPONSE

Record the incident start time, known facts, affected people, systems and deadlines. Contact emergency services where necessary. Use a verified alternative communication channel if email may be compromised. Secure devices and accounts with competent support and preserve evidence. Apply the personal data breach process in CF POL 06 in parallel; continuity targets do not override legal notification deadlines.

SYSTEM OR DEVICE FAILURE

Isolate unsafe equipment. Use an approved replacement device and securely recover authorised access. Restore from a known clean backup, verify completeness and integrity and confirm essential applications operate correctly. Do not restore malware or overwrite useful evidence. Reconcile work completed since the last recovery point.

SUPPLIER OUTAGE OR PREMISES LOSS

Assess the supplier’s status and available exports. Use a previously assessed alternative only where contractual, privacy and security requirements are met. Work remotely from a safe approved location where possible. If access to a specialist platform cannot be restored, explain the delivery implications and agree a revised method or timetable with the client.

PLANNING TARGETS

Initial impact assessment and incident lead assignment: within four working hours of awareness. Initial affected-client update: within one working day, sooner where the impact requires it. Restore priority communications and access to essential project records: target one working day. Restore priority delivery capability: target two working days; remaining work: five working days. Target maximum loss of actively changing critical records: one working day, supported by at least daily backups when work changes. These are internal planning targets to validate, not guaranteed service levels.

COMMUNICATIONS TESTING AND RESTRICTED SCHEDULE

COMMUNICATIONS

The incident lead approves factual updates covering known impact, interim arrangements, client actions and the next update time. Avoid speculation and unnecessary personal or security information. Verify unexpected payment or bank-detail changes through an established independent channel. Maintain a communication log and coordinate supplier, insurer, regulator and contractual notifications as applicable.

RETURN TO NORMAL

Before resuming normal service, verify system security, restored data, access permissions and work quality. Reconcile outstanding actions and revised commitments with clients. Record the decision to stand down, unresolved risks and owners. Hold a lessons review within ten working days of stabilisation and update the plan and controls.

TESTING AND REVIEW

Test backup restoration at least quarterly using a representative critical file or system and record recovery time and data loss. Conduct an annual exercise covering a system or cyber incident. Record failures, actions and retests. Review contacts and dependencies quarterly and after changes.

RESTRICTED OPERATIONAL SCHEDULE

Maintain a separate access-controlled schedule containing business, emergency and out-of-hours contacts; client priority and deadline register; system owners and support routes; backup locations, frequency and test evidence; secure recovery instructions; insurance and specialist support; delegated spending and contractual authority; and fallback arrangements. Record credentials only in an approved secure vault, never in this shareable plan.

EVIDENCE AND REVIEW

Maintain the completed schedule, incident logs, communications, backup test results, exercise reports and corrective actions. Changing Footprint's Director reviews this plan annually and after incidents or material changes. Share relevant instructions with those expected to act and provide clients with accurate information about capability and any material limitations.

Reviewed and approved by: Mark Taylor, Changing Footprint Director
Approval and issue date: 18 September 2026