Scenario Playbook Pack

Continuity response cards for the disruptions UK SMEs face most. These keep the business running; if a cyber attack is the cause, run your Incident Response Plan alongside them.

Premises unavailable

Fire, flood, cordon, structural or utility issue. The common problem: you cannot get in.

DO

- Account for staff safety first; confirm nobody should travel to site
- Invoke the plan; move to alternative location or home working
- Sort equipment, access to records, phone rerouting and post/deliveries
- Communicate with staff and customers; notify insurer and landlord
- Plan the return to site once it is safe

> Home working only helps if people actually have the laptops, connectivity and access to do their jobs. Twenty people without kit are still twenty people who cannot work.

Internet or telephony outage

Provider incident or local equipment failure.

- Establish scope (your kit vs a wider provider incident)
- Switch to your alternative connection (second circuit, 4G/5G)
- Move to mobile working; reroute VoIP numbers
- Check which cloud services are still reachable
- Communicate status; escalate against the provider SLA

Microsoft 365 or cloud outage

A PROVIDER outage of Exchange, Teams, SharePoint, authentication or a SaaS app.

- Switch to alternative communications; keep priority work going on manual processes
- Identify which data is unavailable and what will need reconciling later
- Tell staff where the official instructions are coming from

> If you suspect a tenant COMPROMISE rather than a provider outage, treat it as a security incident and switch to your Incident Response Plan.

Major IT / server / data loss

Server failure or data unavailable, at business level.

- Identify affected processes; set restore priority from the BIA
- Use manual workarounds; understand your RPO (data loss) and RTO (time)
- Validate the backup before trusting it; restore in dependency order
- Plan reconciliation of anything done manually

Cyber incident (continuity view)

Keep operating while your Incident Response Plan contains the threat.

- Focus on minimum viable services and safe alternative communications
- Use manual processes; protect finance controls and payment verification
- Meet customer commitments where you can; set recovery priorities

> This card does not contain or investigate the attack. That is the job of your Incident Response Toolkit: systemforce.co.uk/resources/cyber-incident-response-toolkit/

Power / utilities loss

Power cut, water loss, heating failure.

- Safety first; estimate likely duration; know your UPS and generator limits
- Decide whether to relocate or send people home
- Manage the knock-on loss of internet and network; shut down equipment safely
- Protect anything perishable or production-critical; communicate throughout

Key supplier failure

A single-source supplier cannot deliver or ceases trading.

- Identify affected products/services; check current stock or capacity
- Escalate to the supplier; activate a secondary source or alternative product
- Prioritise your own customers; understand contractual and financial impact

Staff shortage / key-person loss

Large-scale absence, or the loss of a single critical person.

- For broad absence: minimum staffing, deputies, cross-training, remote working
- For key-person loss: rely on documentation and deputies prepared in advance
- Protect priority services first; secure any specialist access or knowledge

Full guidance and context: systemforce.co.uk/blog/2026/08/26/business-continuity-plan-template-uk/ · Practical guidance, not legal advice.