

Business Continuity Plan

A simple plan to keep serving clients when systems, power or the building are not available. Fill in each section, share it with your team, then test it.



ORGANIZATION

LAST UPDATED

PLAN OWNER

1 Critical systems, in order of priority

#	System	What it supports	Owner	Longest we can be without it	Workaround while it is down	Who to call
1	Email (Microsoft 365)	Staff and client communication	Operations manager	4 hours	Phone tree and text group. Webmail from any device.	IT provider
2						
3						
4						
5						
6						
7						

2 Who gets notified, and how often

Who	Who tells them	How	How often during an outage
Leadership			
Staff			
Clients			
Board			
Funders and partners			
Insurer and key vendors			

Business Continuity Plan, continued

3 Downtime checklists

Power outage

- ☐ Know which systems have battery backup, and for how long.
- ☐ Save work and shut down safely before batteries run out.
- ☐ Move critical work to charged laptops and phones.
- ☐ Post a notice for clients and update the phone message.

Internet outage

- ☐ Switch to the backup connection or a phone hotspot.
- ☐ Confirm which cloud systems still work from phones.
- ☐ Call the provider and record the ticket number.
- ☐ Tell staff what works and what does not.

Email or Microsoft 365 down

- ☐ Check the service status page before troubleshooting.
- ☐ Use the phone tree or text group for staff updates.
- ☐ Keep a printed list of key contacts.
- ☐ Hold urgent messages and send them once service is back.

Client system down

- ☐ Switch to paper intake forms prepared in advance.
- ☐ Write down every client served during the downtime.
- ☐ Enter paper records once the system is back.
- ☐ Call the vendor and record the ticket number.

Building not usable

- ☐ Know where staff will work: home, another site or a partner.
- ☐ Have laptops and remote access ready ahead of time.
- ☐ Forward the main phone line.
- ☐ Update the website and voicemail with how to reach you.

Cyberattack

- ☐ Switch to the Incident Response Plan.
- ☐ Do not restore anything until the cause is known.
- ☐ Follow your insurer and legal counsel.
- ☐ Use the workarounds above while systems are offline.

4 Keep it working

Test a restore from backup	Every quarter	<u>Last done</u>
Walk through one scenario as a team	Every year	<u>Last done</u>
Update contact lists and the phone tree	Every six months	<u>Last done</u>
Review this plan	Every year and after any big change	<u>Last done</u>

5 Where to find what you need

Backups, and how to restore them

Vendor account numbers

Domain, website and phone accounts

Admin and emergency access

Insurance policy and hotline

Printed forms and contact lists

Want a second pair of eyes? Ask for a free first look.

One conversation and a straight answer about where your organization stands. No cost, no commitment, no pitch.

akrom@zakhidov.ai
zakhidov.ai