Disaster recovery plan

A plain-English template for small architecture, engineering and construction firms

How to use it: fill in all eight sections. Grey italic text is an example for a made-up 20-person engineering firm; replace it with your own. Keep one printed copy and one copy away from the office, because the server you saved it on might be the thing that is down.

1 Plan basics

Firm name	
Plan owner	*Office manager*
Backup plan owner	*Senior project engineer*
Last updated	
Where copies are kept	*Printed in the office manager's desk, and a copy in the cloud*

2 Emergency contacts

ROLE	NAME	PHONE	EMAIL
Plan owner			
Backup plan owner			
IT support			
Internet provider			
Building manager			
Key software vendor	*Autodesk reseller*		

3 Critical systems and data, in recovery order

Back within = the longest it can be down. Can lose = how much recent work you could live without.

ORDER	SYSTEM OR DATA	OWNER	BACK WITHIN	CAN LOSE
1	*File server and project files*	*Office manager*	*4 hours*	*1 hour of work*
2	*Microsoft 365 email*	*Office manager*	*4 hours*	*None*
3	*CAD and BIM software, licences*	*BIM lead*	*1 day*	*Not applicable*
4	*Accounting software*	*Bookkeeper*	*2 days*	*1 day of entries*

4 Backups

WHAT IS BACKED UP	WHERE THE COPIES ARE	HOW YOU KNOW IT RAN	LAST TEST RESTORE
Servers and file storage	*Office copy and cloud copy*	*IT support checks*	
Microsoft 365			
Staff laptops			
Project archives			

5 Who does what

JOB	PERSON	THEIR BACKUP
Decides it is a disaster		
Leads the recovery		
Calls IT support		
Keeps staff updated		
Talks to clients about deadlines		

6 The first hour, step by step

- [ ] **1** If ransomware is suspected, disconnect the affected computers from the network.
- [ ] **2** Call the plan owner and IT support, even if it might be nothing.
- [ ] **3** Work out what is affected and what still works.
- [ ] **4** Tell staff what to do, and what not to touch.
- [ ] **5** Restore systems in the order from section 3.
- [ ] **6** Check restored files open and save before everyone starts working again.
- [ ] **7** Tell clients about any deadline at risk, early.
- [ ] **8** Write down what happened, when, and what you would change.

7 Working while systems are down

Where will staff work?

How will they reach the files they need?

Which deadlines are at risk, and who calls each client?

8 Testing and review

Review the plan whenever your people, systems or offices change.

DATE	WHAT WAS TESTED OR REVIEWED	RESULT	NEXT REVIEW