IT business continuity plans

A comprehensive guide

Fires and floods

1. The preparation

For starters, make an emergency contact list that includes local authorities, IT technicians, and managers. This way, you and your staff will be able to reach the right people and services quickly in a crisis. Secondly, contact state emergency services to find out if you are in a disaster-prone area. Asking about flood maps and bushfire levels will help you determine what disaster recovery solutions you need.

If there's a high probability that fires or floods will render your main office inoperable, for example, consider setting up a secondary facility that houses backup servers, networks, and workstations. This is particularly vital for organisations that need to recover instantly after a disaster. Another solution is to move documents and apps to remote cloud servers that can be accessed via the internet. Not only are these solutions more cost-efficient, but they also guarantee faster recovery times and are maintained by a team of experts.

However, no matter what plan you have, test it regularly with simulations and role-playing exercises. It can make the difference between a full recovery and your business closing its doors for good.

2. The response

When disaster strikes, call local authorities and your IT technician about your situation. Staff members, business partners, and customers must also be informed to prevent widespread panic and ensure everyone knows what to do next.

Afterwards, have employees turn off all electronics and evacuate the building in a quick yet orderly fashion. If you have a secondary facility, make sure everyone knows how to get there and what's expected of them once they've arrived. Otherwise, you can let staff work remotely in the cloud, assuming they're in a safe location.

3. The recovery

Until your headquarters has been fully restored and deemed safe by professionals, your business will need to operate in a temporary work site. Contact your managed services provider to restore any lost documents and repair faulty software and equipment. You'll also need to record what was lost for insurance purposes, including the serial numbers of electronics. Finally, it's important to reassess your plans with key decision-makers to improve your disaster recovery process.

Power outages

1. The preparation

Power outages are a common occurrence in Australia, especially during a heatwave. As such, you need to prepare well ahead of time. This involves setting up an uninterruptible power supply (UPS) to give everyone enough time to safely shut down their systems. If you can't risk having a single minute of downtime, it may be worth investing in a backup generator that kicks in when the main power fails.

More importantly, you must regularly back up your critical documents in a cloud-based system like Office 365. Keeping business documents, contact lists, and other critical information in the cloud enables employees to work remotely as long as they have an internet connection.

2. The response

In the event of a blackout, save your work and turn off any equipment before the UPS runs out. If there are any urgent tasks that require web access, enable personal wireless hotspots. Also, make sure to unplug all devices because they are prone to short-circuiting when the power comes back on.

Then, call your utility's designated line to report the outage, when it occurred, and whether there are any damaged lines or other hazards. It pays to check power outage updates and nearby offices to see the extent of the problem. Once you've assessed the situation, notify key stakeholders about the service disruption and give them constant updates about what you're doing to remedy the issue.

3. The recovery

When the power comes back, have a technician check for faulty wiring and reset the circuit breaker before turning on devices and network routers. This will minimise potential hazards and prevent further damage to your systems. Next, use your PC's system file checker function to repair any missing or corrupted local data. Of course, you can always restore your files using cloud backups if this doesn't work.

Data breaches

1. The preparation

Preparing for breaches — whether they're caused by malicious actors or negligent employees — requires several steps. First, install advanced threat prevention and email filtering software to detect and mitigate malware, network-based attacks, and online scams. Then, back up your files in a separate location outside your company network to keep them safe from attacks.

If your company employs remote workers, register the devices they use for work into a mobile device management system. This allows you to set access restrictions on sensitive files and remotely wipe devices in case they're lost or stolen.

Employees must be trained to recognise and report breaches as soon as they occur so you can quickly respond to the situation. It's also a good idea to appoint a security expert to coordinate the response and recovery, like Empower IT Solutions.

2. The response

If you detect a breach, the best response is to contain the threat. This means disabling your network, running anti-malware software, and applying the latest patches to limit the spread of cyberattacks. On the other hand, if data was leaked intentionally or accidentally by an employee, modify access privileges and reset passwords to minimise further damage.

When waiting for experts to confirm the breach has been secured, everyone should use backup workstations and devices. Administrators should also keep activity logs from the time of the breach for forensic analysis.

3. The recovery

To recover from a data breach, perform a last-minute scan for any remaining traces of malicious programs with anti-malware software. When you're certain that your device is clean, restore clean copies of your data with cloud backups.

Data breaches must be reported to the Office of the Australian Information Commissioner (OAIC) and affected parties. As such, send an email to all customers and stakeholders that explains what data was compromised, how it occurred, and what actions you've taken to fix the issue to effectively manage expectations.

Last but not least, review how well your company handled the incident and discuss what you've learned from the breach. You may find that retraining your employees and upgrading your security software could reduce your exposure to future threats.

The most important element of BCP

Each crisis requires a different business continuity strategy, but the most important aspect of keeping a business operational hinges on the effectiveness of data backups. Merely keeping one set of backups on-premises is a recipe for failure. Instead, businesses should have multiple backups, preferably one stored onsite, one in an external hard drive, and another in the cloud. This way, if your onsite backups fail, there are other copies in the cloud you can fall back on. As a cloud provider, we go to great lengths to guarantee your data's survival no matter the incident.

Data backups are so crucial to business continuity that we recommend you test them and your recovery procedures as often as possible. Because if your backup protocols fail on the day you need them, your business might never recover.

Insert Your Business Name

Business Continuity Plan

Date: _____

Distribution list

An up-to-date list of all plan locations and persons supplied with a copy of the plan should be included.

Copy Number	Name	Location
001		
002		
003		
004		
005		

References and related documents

Include all documents that have a bearing on your Business Continuity Plan.

Document title

Risk management plan

Prepared by.:……Date: ……

Reviewed by: …….. Date: ……

Key:

VH = Very High
H = High
M = Medium
L = Low

Risk Description:	Likelihood	Impact	Priority	Preventative Action	Contingency Plans

Insurance

Determine what types of insurance are available and put in place the insurance your business needs.

Insurance type	Policy coverage	Policy exclusions	Insurance company and contact	Last review date	Payments due

Data security and backup strategy

How have you protected your data and your network? (e.g. virus protection, secure networks and firewalls, secure passwords and data backup procedures)? Detail your backup procedures in the table below.

Data for backup	Frequency of backup	Backup media/ service	Person responsible	Backup procedure steps

Business impact analysis

Critical Business Activity	Description	Priority	Impact of loss *(financial, loss of reputation etc.)*	RTO *(critical period before business losses occur)*

Incident response checklist

Information to include when planning your critical incident response as part of your Incident response plan.

Incident response	✓	Actions
Have you: Assessed the severity of the incident?	❑	
Evacuated the site if necessary?	❑	
Accounted for everyone?	❑	
Identified any injuries to persons?	❑	
Contacted Emergency Services?	❑	

Implemented your Incident Response Plan?	❑	
Started an Event Log?	❑	
Activated staff members and resources?	❑	
Appointed a spokesperson?	❑	
Gained more information as a priority?	❑	
Briefed team members on incident?	❑	
Allocated specific roles and responsibilities?	❑	
Identified any damage?	❑	
Identified critical activities that have been disrupted?	❑	
Kept staff informed?	❑	
Contacted key stakeholders?	❑	
Understood and complied with any regulatory/compliance requirements?	❑	
Initiated media/public relations response?	❑	

Evacuation procedures

Your evacuation procedures should cater for both staff and visitors and be stored in a place accessible to all staff. In the event of a critical incident. You should:

- Start with a floor plan of the site.
- Clearly identify the location of emergency exits.
- Develop strategies for providing assistance to persons with disabilities.
- Make sure that everyone knows what to do if evacuation is necessary.
- Select and indicate a meeting place (evacuation point) away from the site.
- Test the plan on a regular basis.

Emergency kit

If a building is damaged or must be evacuated, operations will need to be moved to an alternative location. The emergency kit should be able to be easily carried off-site or alternatively stored securely off-site. Document within your plan what is contained within your emergency kit and when it was last checked. Items that you may wish to include are:

Documents:

- BCP - your plan to recover your business or organisation in the event of a critical incident.
- List of employees with contact details - include home and mobile numbers, and even e-mail addresses. You may also wish to include next-of-kin contact details.
- Lists of customer and supplier details.
- Contact details for emergency services.
- Contact details for utility companies.
- Building site plan (this could help in a salvage effort), including location of gas, electricity and water shut off points.
- Evacuation plan.
- Latest stock and equipment inventory.
- Insurance company details.
- Financial and banking information.
- Engineering plans and drawings.
- Product lists and specifications.
- Formulas and trade secrets.
- Local authority contact details.
- Headed stationery and company seals and documents.

Equipment:

- Computer back-up tapes/disks/USB memory sticks or flash drives.
- Spare keys/security codes.
- Torch and spare batteries.
- Hazard and cordon tape.
- Message pads and flip chart.
- Marker pens (for temporary signs).
- General stationery (pens, paper, etc).

- Mobile telephone with credit available, plus charger.
- Dust and toxic fume masks.
- Disposable camera (useful for recording evidence in an insurance claim).

Notes:

- Make sure this pack is stored safely and securely on-site and off-site (in another location).
- Ensure items in the pack are checked regularly, kept up-to-date, and in good working order.
- Remember that cash/credit cards may be needed for emergency expenditure.

This list is not exhaustive, and you should customise it to suit your business.

Roles and responsibilities

Assign a role, or multiple roles, to one or more staff members and assign back-up staff as appropriate. The staff members involved should be given this table in order to understand their roles. You should customise this table to suit your business's needs and structure. Emergency responsibilities:

Role	Designated employees	Alternate
Title	Name: Contact information:	Name: Contact information:
Title	Name: Contact information:	Name: Contact information:
• Ensure the Business Continuity Plan has been activated. • Oversee smooth implementation of the response and recovery section of the plan. • Determine the need for and activate the use of an alternate operation site. • Communicate with key stakeholders as needed. • Provide important information to the Communication Officer for distribution. • Keep key staff apprised of any changes to situation.		

Contact list - Internal

Use this table to document your staff emergency contact details. Each business will have different positions identified in its contact list.

Person	Contact number/s	Email	Responsibilities

Contact list - External

Use this table to document external services (including emergency services) contact details. Each business will have different external suppliers and stakeholders.

Key contacts	Contact number/s
Police (emergency)	000
Police attendance (all states except Victoria)	132 444
SES (floods and storms)	132 500
Ambulance	
Police (local)	
Medical	
Security	
Insurance company	
Suppliers	
Water and sewerage	
Gas	
Electricity	

Event log

Use the event log to record information, decision and actions in the period immediately following a critical event or incident.

Date	Time	Information / Decisions / Actions	Initials

Recovery plan

Critical Business Activities	Preventative Recovery Actions	Resource Requirements/ Outcomes	Recovery Time Objective	Responsibility	Completed

Incident recovery checklist

Customise this list to include information specific to your business. Now that the crisis is over have you:

Incident response	✓	Actions
Refocused efforts towards recovery?	❑	
Deactivated staff members and resources as necessary?	❑	
Continued to gather information about the situation as it affects you?	❑	
Assessed your current financial position?	❑	
Reviewed cash requirements to restore operations?	❑	
Contacted your insurance company?	❑	
Developed financial goals and timeframes for recovery?	❑	
Kept staff informed?	❑	
Kept key stakeholders informed?	❑	
Identified information requirements and sourced the information?	❑	
Set priorities and recovery options?	❑	
Updated the Recovery Plan?	❑	
Captured lessons learnt from your individual, team and business recovery?	❑	

Recovery contacts

Include all of the organisations/people that will be essential to the recovery of your business.

Contact Type	Organisation Name	Contact	Title	Phone Number
Insurance				
Telephone/internet services provider				
Bank/building society				
Supplier (Main)				
Supplier (Backup)				
Accountant				
Lawyer				
DEEDI Regional Development Officer				

Insurance claims

What insurance policies have you claimed for?

Insurance company	Date	Claim details	Follow-up actions

Market assessment

List any areas of you market that have changed due to the incident.

Market changes	Impact to business	Business options

Rehearse, maintain and review

It is critical that you rehearse your plan to ensure that it remains relevant and useful. This may be done as part of a training exercise and is a key factor in the successful implementation of the plan during an emergency. You must also ensure that you regularly review and update your plan to maintain accuracy and reflect any changes inside or outside the business. The following points may help:

- Prepare a training schedule for all people involved in an emergency at the site.
- Pay attention to staff changes.
- Use staff titles rather than names.
- If you change your organisational structure or suppliers/contractors this must be amended in your plan.
- After an event it is important to review the performance of the plan, highlighting what was handled well and what could be improved upon next time.

Training schedule

Record details of your training schedule in the table below:

Training Date	Training type	Comments

Review schedule

Record details of your review schedule in the table below:

Review date	Reason for review	Changes made

How we can help

Empower IT Solutions have the enterprise-grade solutions and services to keep your operations running. Just talk to one of our many IT professionals today, and we'll customise a BCP that meets your needs and budget. Call us on: 1300 797 838

DISCLAIMER

The Business Continuity Procedure template provided by Empower IT Solutions is for reference only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk.

Template information supplied by: QLD Government https://www.publications.qld.gov.au