A Quick Check of Pandemic Preparedness

Do you have a BCP Plan?

A Business Continuity Plan is an important artefact in any business. It is the 'go-to' for any event that impacts the way you provide services to your internal and external clients.

Typically, a full BCP Plan will consider the following scenarios. In a Pandemic more than one scenario may apply.

Loss Type	Strategy Examples
Area / Building (unavailable) – Denial of Access or Evacuation	Operations staff are relocated to BCP site, or home with secure remote access available for all
People (unavailability – due to sickness, transportation)	Increase support levels at required site, and engage contractors for critical functions
Tools or Data (loss of access to)	Move to the BCP site, and/or manual restore.
Technology Access (Telco and/or Infrastructure at primary site)	IT recovery procedures, client comms, staff follow manual admin processes.

The desired outcome is a safe working environment for your staff and the continuation of services to your clients and customers.

This brief does not intend to replace a BCP Plan, but instead presents a quick consideration of the checks and controls you should have in place specifically for the current virus threat.

For a Pandemic, what do you need to consider?

In general, the scenarios are:

- Working Well - all staff are available, just not in the same place at the same time.
- Surviving Sick - some or all staff are ill / unable to perform duties.

Local, state or federal actions may impact your plan, so, perform daily or weekly 'BCP team' meetings to collate any news, update any learnings from other organisations, (trusted) web sites and news events.

What should you communicate to staff?

You know best the message style that is appropriate to manage your teams.

Be practical and pragmatic.

Keep the messages short, but frequent.

You can follow up with links to acknowledged websites and Twitter feeds for further reading but stay clear of 'toilet-paper-panic' sites.

If staff are working from home, ensure you have a collaboration capability, such as Office 365 Teams, Video Conference facility or even WhatsApp for individual or teams conversations.

Communications & Media Escalation

In general, staff should not answer any media queries and should refer these to a nominated senior manager (such as CEO).

Validate your Assumptions

As there may be factors that change outside of your control or planning, such as local, state or national lock-downs it is important that you identify your assumptions.

Some examples of reasonable assumptions are as follows – please validate these for your organisation:

1. All staff have Internet at home.
2. All staff have access to a work laptop or home PC at any time.
3. Staff using home PC/laptops are up to date with security patching, and the device is physically secure (not used by other family members).
4. You have direct control of the physical security of your office (i.e. you can lock it during business hours).
5. You have up to date contact details for all staff (physical address, mobile and email).
6. Passwords to systems and tools are personalised, or if a shared password that this is kept in an online password safe and available only to relevant personnel.
7. You can access all of the tools and systems you need to do your job remotely. Examples are using Office 365 for email, collaboration or shared files.

Do you know what you Need to perform your Critical Functions?

Make a list. You need to consider organisational tools, systems and procedures and the risk to each. For example, your Finance system may be only accessible to on-site connected users. Additional security may be needed to protect the data being accessed remotely e.g.

Team	Process	App	Who	IT Needs	Third Party	Vital Records	Special requirements
Finance	Payroll	Xero (Cloud)	CFO Acct'nt	Laptop + Internet	MicroPay	Xero	Security

What else do you need to consider?

This is a good time to also consider your organisations HR Policies and Procedures in relation to Sick Leave availability, requesting a doctor's certificate before returning to work (even if tested to not be coronavirus).

Your partners and suppliers – are they ready with their own BCP Plan? Have they communicated their plan to you? Consider your Payroll provider in particular - to ensure staff are not unduly impacted (or create a manual workaround).

What aspects of your business can you reduce or shut down for a short period? Can you redirect staff to help cover other roles? Can you start this training now?

Does your organisation have more than one location? If so, consider the loss of one group or area.

Most Importantly

Remember everyone handles stress differently. We don't always know what goes on at home for some staff – health, dependants, cash flow, lack of social engagement may all be factors. These may continue to influence after return to 'normal' operations.

Recommendations – A bit of a Checklist

Description	Check
IT, Systems and Technology Security	
If staff have a work laptop they should start taking it home (with power pack!), as the situation could change at any time and they may not be able to get back into the office to pick it up.	
Do a practice run – get each team to work from home for a half-day. Can they access all tools and systems?	
If you have any dedicated systems, e.g. need to use a remote desktop (RDP), VDI, VPN or other secure application to access your systems, check with your IT service provider that there is sufficient capacity for all staff to use them at the same time.	
Are there systems that can only be accessed by people physically in your office? (It may be geo-fenced, or blocked from external access). Talk to your IT service provider about secure remote access.	
Discuss options for Multi-Factor Authentication with your IT service provider. This enables a secure code in addition to passwords for some applications. This may be important where staff are using home PCs to access business systems.	
Review your password safe. Who has access to it, and what level of access	
Do you know what and where your Vital Records are? These will be your HR files, Finance records, CRM records, BCP Plan (!). Are these available offline? Is there a paper copy (preferably not) or soft copy on a thumb drive (better) held by 1-2 people (in case of an Internet outage).	
Are there routines that are performed on your IT systems that require access to the office e.g. changing backup tapes.	
If you are locking the office, can your IT service provider access it if any systems fail?	
If working from home, can your staff work from a laptop screen for long periods of time, or do they need a monitor and external keyboard/mouse.	
If you intend to engage contractors, volunteers or casual staff, create instructions (now) to instruct your IT service provider of the levels of access they are to be assigned. Your, and your clients, data security remains critical.	
Communications	

Description	Check
Ensure all staff are aware of the process that will be used to notify them should you require them to stay at home or divert to an alternate location. It is critical that you know where all of your team is at any time as you are still responsible for their working environment (even when at home).	
Create a list of all staff mobiles (corporate or personal). Ensure all staff are covered and contacted by the most universal service available e.g. text. If you don't have a SMS Broadcast tool, a calling tree will do this (each nominated manager assigned to call a nominated group of staff).	
Follow up with group conference call, or collaboration session (e.g. Office 365 Teams) so that there is a consistent message. Welcome ideas or comments, so you can understand the concerns in general, or any specific risks.	
Ensure your BCP team includes representation from different groups, so that any messages are relevant to all groups, and that there is representation, not just management.	
Ensure that, if you do invoke a BCP that you communicate with all staff within 2 hours as a group (group email at a minimum, but preferably open a audio conference bridge or Teams meeting so that the collective attention, feedback and support for each other is recognised (also you can do a head-count at this point).	
Communicate a high-level view of the Plan with your customers or clients. Keep it simple and consistent. Ensure your staff are aware of the communications that are being sent. This could be as simple as: • If you are experiencing delays in delivery of goods or services • If you intend to meet virtually, instead of physically • If Key Personnel, such as Escalation personnel are available	
Notify your key partners and supplier of any changes in business operations so they can best assist.	
Health and Safety	
At all times, the safety and welfare of your people comes first. Employees should be encouraged to dial in to the audio bridge, chat room, WhatsApp or other social forums	
Do you have agreed transport arrangements, such as Taxi chit or Uber corporate account (make sure the staff know the rules for use).	
If staff report a flu (we are heading towards Winter) then ensure they don't come to work without a clearance certificate. At the moment this needs to be from the doctor, although drive-thru testing centres or other options may be available to certify)	
Is your cleaning company able to provide specialist cleaning, or do you need to engage another company?	
Does your organisation have an EAP program, where staff can access confidential counselling?	

Description	Check
Personnel	
Understand who your Key Personnel are. This is not the loudest or the busiest, but should consider a person to pay bills, pay staff, service clients, keep technology lights on.	
Check you have position descriptions, or role briefs, for all positions. Ensure you have a personnel contracting organisation at hand, should you need to boost staff in some groups.	
Do you have an alternate person agreed for all Key Personnel e.g. if CFO is unavailable, does the CEO or CIO have Delegated Authority? If you have a client Service Manager / Account Manager, is there a peer who can take over the assignment.	
Do you have a list (company, contact email and phone and person) of: • All Suppliers • All critical partners (e.g. IT service provider & Telco) • Your building /strata manager • Your alarm / security provider	

END