10 TIPS for Small Businesses Wanting to Work from Home

Responding to COVID-19 (Coronavirus)

Social distancing is a key strategy to flattening the COVID-19 (Coronavirus) infection trend, limiting the potential for the virus to spread so that the most vulnerable in our communities have the best access to Australia's world leading health system. The following 10 tips are to help your business maximise working from home arrangements over a three-month timeline.

1

Take precautions to protect your own health and that of staff and clients.

This includes reinforcing regular handwashing; a minimum social distancing of 1.5m (continually checking for updates on current Health Department requirements); refraining from the 'handshake' culture; use of alcohol-based hand sanitiser containing at least 60% alcohol; use of handkerchiefs/tissues when sneezing and coughing; promoting awareness of 14 days of self-isolation for people returning from overseas; maximising cashless payments and online orders. If the office itself is mission critical, you could consider thermal cameras at the front desk to identify visitors with raised body temperatures who may be showing COVID-19 symptoms. All non-secure doors should be locked open during business hours to reduce contact.

2

Share with your customers your business plans and approach to minimising COVID-19 risks.

3

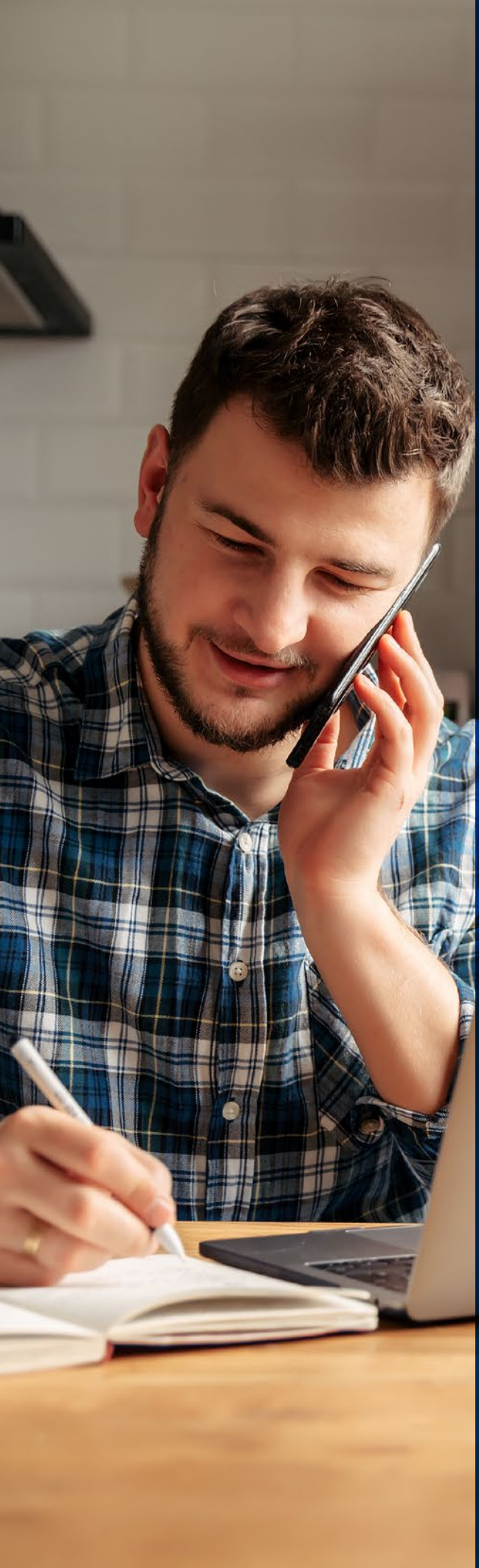
Document your chain of command and key person risk.

If the boss is impacted by the COVID-19, who is the 2IC (second in charge) that will then be delegated day to day business decisions? This should be applied down to three levels and ensure every team member is aware. Expand this approach to your subject matter experts. Who are they, and who do you contact is your primary expert is not available? Again, apply three levels down.

4

Understand your mission critical functions and think through how they could be performed from team members working at home this week.

It may require reallocating desktops, laptops, and mobile phones across team members. If your primary service is break-fix, think through how you will manage contact with your clients/customers.



5

Load testing: Don't leave it until you're forced to work remotely to realise your weaknesses:

☑ Pick a day this week and have as many of your team as possible work from home and see how the network performs.

☑ If you are expecting staff to log in using their own internet plans, assessments need to be done straight away to test whether the home plans are capable of supporting business applications. Upload speed is more important than download speed. Adding 4G to the business for remote laptop access needs to be decided earlier rather than later.

☑ This might be the first time that a couple works from home at the same time. Watch out for children coming home from school and jumping onto Netflix, Disney or other streaming services. If your internet is crawling, refrain from video during web conferencing. If the participants know each other, then you may need no video at all.

☑ Have standard operating times and designated work areas for how the household will function to accommodate working from home.

☑ If you need to ramp up internet bandwidth at a team member's home, options to consider include:

- Enterprise Grade Mobile Broadband Hotspot devices capable of supporting 20 users/devices – Nighthawk (Netgear) M1 approx. $350 each.
- Huawei Optus E5573 4G Personal Mobile Broadband Hotspot devices capable of supporting 5 users/devices –Personal Mobile Broadband Hotspot approx. $70 each.
- Entry level smartphones with hotspot capabilities can be issued to team members who don't have a personal mobile phone/plan suitable to support your work practices such as the Samsung Galaxy A20.
- A dual SIM model smartphone so team members can have a company and personal SIM in the same device. Cost approx. $279 each. Consider OVO Voice/Data and Mobile Broadband SIMs as they have generous data allowances and are prepaid and you can control spend risk.
- For home offices there is the 4G LTE Router with switch, Firewall, VPN and wireless network, for less than $400.

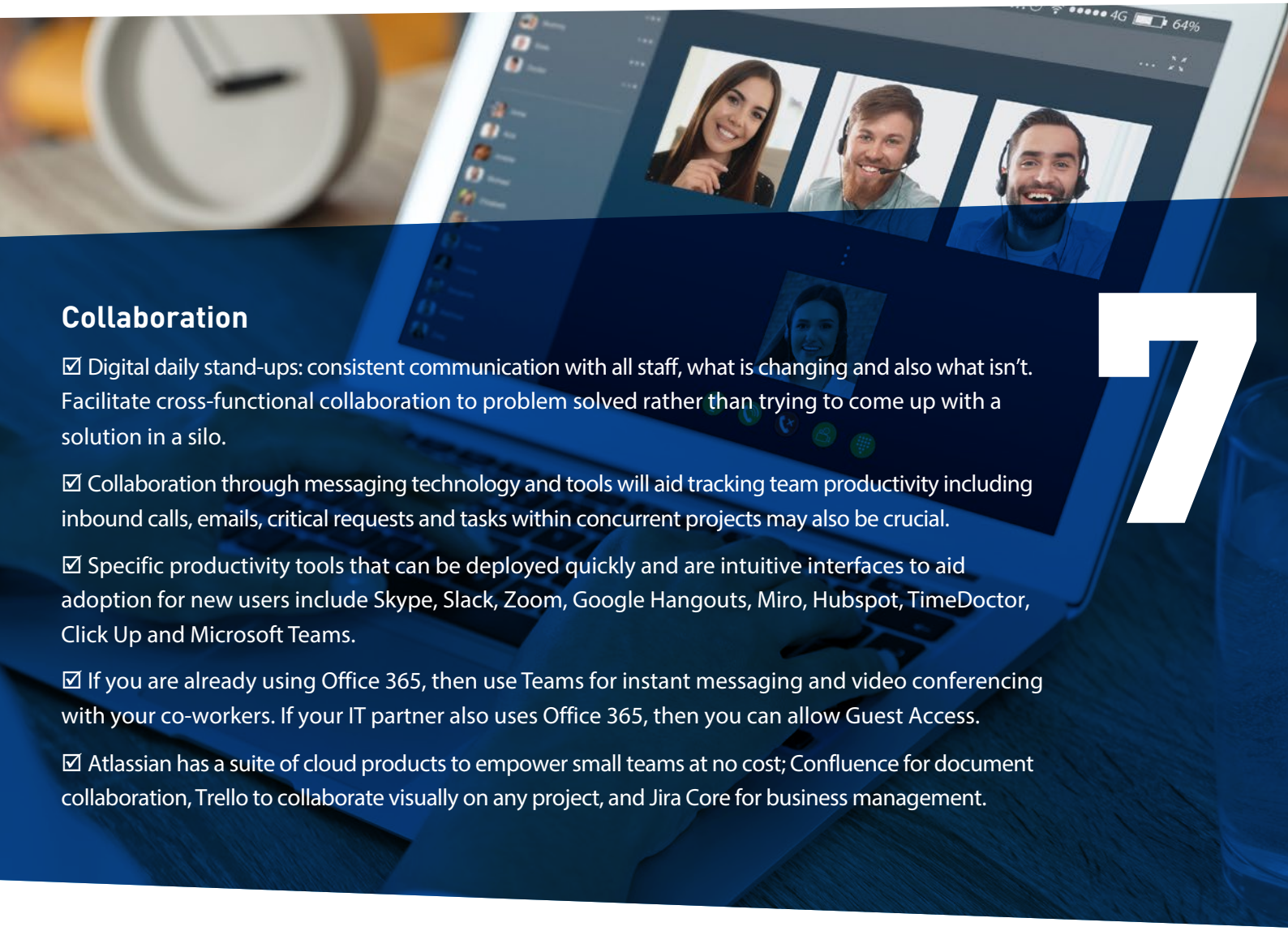
6

Mobility and hardware. If you do not have already, and where financial capacity enables, provide:

☑ Laptops to team members.

☑ A headset for audio conferences, and optionally a web camera for video. One tip is that audio and video conferences tend to work better using a phone app, than a computer.

☑ Pay for a licensed cloud remote access platform. Don't be tempted with free versions and pay to legally use the platform. Examples include TeamViewer or Real VNC Professional.



7

Collaboration

☑ Digital daily stand-ups: consistent communication with all staff, what is changing and also what isn't. Facilitate cross-functional collaboration to problem solved rather than trying to come up with a solution in a silo.

☑ Collaboration through messaging technology and tools will aid tracking team productivity including inbound calls, emails, critical requests and tasks within concurrent projects may also be crucial.

☑ Specific productivity tools that can be deployed quickly and are intuitive interfaces to aid adoption for new users include Skype, Slack, Zoom, Google Hangouts, Miro, Hubspot, TimeDoctor, Click Up and Microsoft Teams.

☑ If you are already using Office 365, then use Teams for instant messaging and video conferencing with your co-workers. If your IT partner also uses Office 365, then you can allow Guest Access.

☑ Atlassian has a suite of cloud products to empower small teams at no cost; Confluence for document collaboration, Trello to collaborate visually on any project, and Jira Core for business management.

8

Business as usual (when business isn't usual)

☑ Quality employees will be your greatest assets. Look after them and check in regularly to see how they are travelling.

☑ Accept normal business operations may quickly become abnormal. Accept that team members won't be able to achieve the same level of productivity and ergonomic working from home as in the office.

☑ Don't panic. Expand your business if your competitors vacate the market. Keep in touch with your clients.

☑ Directly connect with all your key customers on your preferred social channels such as Linkedin, Facebook, Twitter.

9

Cyber security

☑ Company owned devices are preferred as they should be compliant with your corporate security policy.

☑ Data on all devices should be encrypted.

☑ Anti-virus software is installed, up to date and monitored.

☑ A compliant, supported and up-to-date operating system is installed.

☑ The latest security updates are installed.

☑ Monitoring equipment so the organisation can respond to identified threats.

☑ Use 2 factor authentication. Enable multi-factor authenticator 2 Factor Authentication on Real VNC or TeamViewer.

☑ Ensure your team has a heightened vigilance for phishing emails and scams.

☑ Avoid using public WiFi.

☑ Ensure that staff connect to Extranets via a VPN. (a VPN can also simplify remote access).

☑ Ensure your team have a working etiquette around password strength and rotation policies.

See the Essentials 8 for recommendations of the Australian Defence Force Directorate when it comes to cyber security hygiene.

10

Back-up plans

☑ Ensure any internal servers in your workplace have redundant power supplies so systems stay operational in instances of power outages or other interruptions.

☑ Data loss prevention (DLP) should include having all files needed to stay productive in the cloud. For example, everyone with a Microsoft Account has OneDrive Storage, every Gmail account has Google drive, every Apple account has iCloud.

☑ If you have on premises servers, where are you keeping your off-site back-ups? Is it time to use two off-site backs ups to maximise recovery should there be a site closure without notice?