

READY OR NOT: YOUR BUSINESS AND COVID-19

Have you thought about how your business would cope with COVID-19? We have. Remote-working plan and IT systems are vital if you want to survive and thrive in these uncertain times. In this checklist, we'll break down the IT challenges your business might face and how to prepare for them. If you have the correct IT systems in place, you have the best chance of continuing business as usual – even if your staff are stuck at home.

CHALLENGE 1: SYSTEM ACCESS

By using cloud systems (internet connection required), staff can access their desktop and data anywhere in the world, on any device. It's the best approach for seamless remote working, giving your people full access to digital business systems from wherever they are. If you've already joined a cloud-based IT system, like Microsoft 365, then you'll need to make sure your team can access all the same tools they'd use in the office.



Our tip: Make sure all team members understand how your cloud system works, how to log in remotely and have a secure internet connection in their homes.

TO CONSIDER:

- Access to all systems, software and data storage
- Availability of Customer Relationship Management, HR and Enterprise Resource Planning systems
- Any other systems and tools that are specific to your business (line of business applications)
- Is secure and easy to access
- A central hub where people can access, edit and instantly sync files

CHALLENGE 2: COLLABORATION

Ensuring your team can seamlessly collaborate will keep work flowing smoothly and efficiently.

Video conferencing and phone services are hugely helpful for meetings and team catch-ups. You'll need to make sure that your business has access to a team's package, with options for multiple users. Your Intranet system can also help send company messages, bolster communication between staff from different teams and keep company culture alive. It's important to remember that this is a new scenario for most employees and guidance is needed.

TO CONSIDER:

- Be clear on the right mode of collaboration to use and when, i.e. when to email, when to use Teams or Slack, etc.
- If on Microsoft 365, use Teams for instant messaging, crystal clear audio calls or video conferencing.
- If not on Microsoft 365 environment, Microsoft Teams is now free and can be quickly implemented in your company.
- When holding online meetings, remember to make video participation optional
- Record calls so other team members can catch up on the information

CHALLENGE 3: BUILDING REMOTE INFRASTRUCTURE

If all your equipment is in the workplace, how do you help people set up a productive home office? In a poll by Gartner, 54% of HR leaders indicated that poor technology and infrastructure is the biggest barrier to effective remote working.



Our tip: Preparation is key. Find solutions, like mobile WIFI hotspots, hiring laptops, etc., for people who do not have proper IT infrastructure in their homes.

ASK YOUR EMPLOYEES:

- Do they have a strong WIFI connection?
- How much bandwidth do they need to be productive and do they have access to it?
- Do they have the necessary equipment; a computer, headset and monitor?
- Have they got a guide for setting up their home office?

CHALLENGE 4: KEEPING A BUSINESS RUNNING

Once you've got systems and structure in place, you need to consider business processes. Beyond day-to-day output, there's many behind the scenes tasks that need to be managed to keep your organisation running smoothly.

ASK YOUR EMPLOYEES:

- How will phones be answered and calls transferred?
- Can you quickly deal with a customer enquiry?
- Are staff emergency contact details up to date?
- How will you communicate with your team to keep them in the loop?
- How will your team communicate with each other?
- How will the devices used meet performance specifications and security standards for your software?
- Can you still raise invoices, process the banking, reconcile accounts, or do month-end reports?

CHALLENGE 5: SECURITY

Your business information is one of the most, if not the most, important asset of your company. The Opportunity for cybercriminals grows when you introduce remote work because people are not working on a network that's controlled by a business. Make sure you protect your employees and organisation by making sure that all endpoints are secure, cyber-security programs are updated, and only authorised applications are used.

TO CONSIDER

- Add two-factor authentication to any system logins. Authentication by SMS is a quick and easy fix
- Setting up secure remote working for large organisations takes time. prioritise the services and people that are critical for keeping things running.

Above all, remember that the unknown is stressful for people. Open communication and support will help your team be productive when working from home. We're here if you have any questions about setting your staff and organisation up for successful remote work.

Get the latest COVID-19 advice for employers [here](#).