BUSINESS AS USUAL

Your urgent Coronavirus checklist

Helping to ensure your team can work as normally as possible from home

net technical solutions

HOW TO MAKE SURE YOUR TEAM CAN WORK SAFELY AND EFFECTIVELY FROM HOME

On the 3rd March, the Government published their Coronavirus (COVID-19) action plan which provided guidelines on what to expect across the UK, as well as how businesses should react.

As of 10th March 2020 the UK remains in containment phase. A total of 321 people have been diagnosed with the virus in the UK, 18 of whom have now recovered and the rest are still being monitored. Sadly there have been 5 deaths to date.

Despite the relatively low figures, The World Health Organisation has declared that this is a public health emergency of international concern. And the UK chief Medical Officers have raised the risk to the UK from low to moderate.

The advice – as stated in the Government's action plan and the guide to employers and businesses – is to self-isolate should you suspect symptoms of Coronavirus.

Because of this, Boris Johnson has said that up to a fifth of UK workers "could be off sick at the same time" and it is "highly likely that we will see a growing number of UK cases".

In the past week we have seen a sharp increase in customer requests to assess the ability of users to work from home, including looking at equipment, security and VPN access. As a result, our technicians have created a **4-step checklist** to ensure that your business is prepared for the possibility that your team is not able to come into the office.

Protecting your business from cybercrime has become a high priority when it comes to IT strategy and you probably have security covered in your office already. All of your servers, PCs and laptops should have anti-virus software, your network should be protected behind a firewall, and your data should be backed up safely and securely, ideally with a copy both on site and in the Cloud.

But if your team starts to work from home, you're widening your exposure to potential threats and cracks can quickly appear in your business's protection.

When preparing for a potential office shut down, you may need to provide your employees with equipment and infrastructure in order for them to complete their duties from home. At the very least you'll need to assess the equipment they are using for remote access. When doing this, it's best to take the approach that: **If it's not secure, there's no point in having it.**

If an employee requires a computer to work from home, especially if they need access to shared networks or data, this should ideally be provided through the business. For security reasons, it is better that staff do not use personal machines and for the business to provide employees with a device that they can use strictly for work purposes. This is a great way to immediately minimise risks to your business, especially from ransomware, but of course this is not always possible.

Here's a quick overview of what else should be considered:

- Ensure your employees are using approved devices for work purposes, especially if you use a VPN which is the safest way to work remotely.
- Educate employees on device use whilst at home (not using work devices for game downloads, being extra-careful when clicking on links etc).
- Ensure all devices have anti-virus software installed, ideally through the business.
- Make sure wi-fi passwords are secure before using home wi-fi for business purposes.
- Set up MFA (multi-factor authentication) either through Office 365 or other providers.

#2

Access to data

If your employees need to work from home, it's important that they are able to access everything they need to fulfil their responsibilities.

This means that you need to consider how and where you are saving data and files and our advice is that this should be in one secure location that is regularly backed up. This may be an on-premise server, or hosted space in a datacentre or a Cloud application such as Teams or SharePoint which are part of Office 365.

Another thing to think about is how your employees can access business applications and how your remote workers can access your server/data remotely. Can they access the server directly via a VPN, is there a Terminal Server in place or can they use Remote Desktop Services (RDS) to access their PC remotely?

All of this can seem quite daunting, but here's a really easy way to figure out what your employees need and how to ensure they have it. **For each department in your business, think of all the different applications that are needed and create a list like this:**

System	How do we access?	Who needs access	Actions / Options
Email / Office 365	Online/Outlook	All staff	Assess Laptops and Mobile Devices
Documents	File Server	All staff	Ensure secure VPN access Advise staff on process

Once you have done this, you can then create a list for each member of your team:

User	Device	Access Required	Actions
Chris	Laptop and mobile phone	Just emails and phone	Set up Office 365 on all devices
Alex	MacBook	Emails, phone and file data	Set up secure VPN

This is a great way to figure out exactly what applications are required, who needs them and how they can get access safely.

#3

Home office set up

If your employees have to work from home because of a Coronavirus lockdown, the obvious question to ask is: does your team have the equipment they need to work remotely?

With the majority of office devices being desktops, it's important to consider sooner rather than later if your staff have the right equipment to work from home. Especially, as the best advice is to provide employees with safe and secure devices, should they need to access shared networks via a VPN.

This sort of decision needs to be thought through carefully and made in advance, to ensure that the devices required are available. We are already seeing an increased demand for devices such as laptops and desktops, and some supply restrictions due to manufacturing issues in China.

You must also consider your telephony systems. Are your staff able to work remotely using mobile phones and diverts? If your team requires access to an internal phone system, could Microsoft Teams (built into Office 365) be a better way to minimise costs if you are already using Office 365.

Here's a quick overview of what should be thought about:

- Whether you require additional work laptops for employees?
- Do your employees have the right Internet access at home?
- What telephony systems do your employees require and do they have a suitable telephone device to work from?
- Do your employees require any other additional equipment to fulfil work responsibilities at home?

Some of your employees may find working from home difficult. This is why every effort should be made to ensure your staff have an appropriate work space in the home environment.

We do not suggest that you go out and buy everyone a desk and a chair. But we do advise that you clarify with your employees what their home working environment is, particularly in relation to the IT setup and offer support where it is possible and appropriate.

#4

Communication, collaboration and management

For any business owner or manager, there is always the worry that employees aren't as productive working from home, as they would be if they were in the office.

This is why clear communication, collaboration and management channels should be implemented to ensure your employees stay focused and productive while working from home.

This could be a great opportunity to look at your current processes, with the view to improve them regardless of the Coronavirus situation. If you are already part of the Office 365 ecosystem, there are lots of applications in there that you already have access to and could use.

Here's a quick overview of what should be considered:

- Project management software
- Video conferencing
- Instant messaging / chat
- Reporting and time management
- Office 365 applications including:
    - Teams
    - SharePoint
    - OneNote
    - Planner

HOW CAN WE HELP?

You may feel like this much preparation is a bit too much, considering the current threat levels to the UK.

However, it is crucially important to ensure that your business can continue operating in the wake of a Coronavirus emergency if the situation escalates. The earlier you plan for such an eventuality, the more prepared and protected your business will be.

For many of our clients, this type of planning can seem quite daunting, which is why we can work with you to ensure your business and employees have everything they need to continue working safely and securely.

Don't leave this too long.
Let's talk now and get your business prepared.

01252 235 235
sales@ntsols.com
www.ntsols.com

net technical solutions