13 STEPS TO SECURING YOUR ORGANISATION FOR REMOTE WORKING

cyberEase
keeping IT safe

In the mad rush to get everyone setup to work from home, have you stopped to consider the security implications for your organisation? We're tried to make it easy for you by producing this handy 13 step checklist to help you ensure you've got all the key points covered.

If you want more detail on what or how for any of the points please just reach out and ask.

□ **1. Asset List in place & up-to-date**

With a distributed IT Infrastructure, it's vital you keep a track of where all your machines and where your company data is being stored and processed.

□ **2. Security Patches applied and monitored**

Cybersecurity is a massive concern at the moment. Attacks have spiked over 800% in some instances. The simplest way to protect yourself is to stay up to date.

□ **3. Appropriate Virus Protection Installed & Active**

Staff may be using temporary machines or their home machines – do they have the same level of virus protection you have in your business?

□ **4. Enhanced Web Protection against malicious links and sites**

Staff will now be operating outside the office firewall, how are you protecting what they visit on the web?

□ **5. Ransomware Protection installed and monitored**

We're expecting ransomware attacks to rise sharply, how are you ensuring your IT estate stays protected?

□ **6. Deployed MFA on all relevant systems**

The most common way of getting hacked is through a leaked password. Multi-Factor-Authentication helps significantly reduce that risk

□ **7. Verified Security of Remote Access Procedures**

With so many people now working remotely, Remote Access tools are a prime target for cyber criminals. Have you reviewed what you have in place and how they are secured properly?

□ **8. Security Awareness Training deployed to staff**

The Human factor is the weakest link in almost every security chain. People are more likely to revert to bad habits at times of stress like we're experiencing right now. What additional Security awareness are you delivering to your staff to stop them being the weakest link in your security?

□ **9. Educated staff on Best Practice for their home Internet security**

Are you staff following best practice with their home internet by changing the default router password and making sure WPA2 encrypted WiFi is in use?

□ **10. Reviewed Backup Procedures and data risks**

How and where is your Data stored now? Do tapes need changing at the office? Do you need to backup data on staff laptops? Have you started storing new data in the cloud that needs to be backed up?

□ **11. Implemented Hard Drive Encryption for any sensitive data**

What data is being stored on your staff's home machines? If you're using something like Dropbox that's still storing data locally and is at risk if the machine gets stolen. You should implement hard drive encryption to protect it.

□ **12. Provided Video Conferencing Guidelines**

Some staff will be using video conferencing for the first time, and may forget they are actually at work. Have you given behaviour guidelines and checking if there is any sensitive material in the background before broadcasting video?

□ **13. Checked Insurance Cover for Remote Working**

Does your insurance cover you if all your computers are at home with your staff? Or is it reliant on them having contents insurance for it?

FURTHER HELP

I've produced a detailed guide on each of **the 13 steps**, to get that or to book a free consultation on any of the above point's just visit https://brokenstones.co.uk/lp/13-steps

brokenStones
your best friend in IT