How to Implement Safe and Secure Remote Working

In the modern world of work and technological progress, change happens fast, and often unexpectedly. If we are to adapt, it is up to all of us to embrace change and ease transition. A major change that we're having to deal with currently is COVID-19. Lockdown restrictions mean that those who can possibly work from home, should do so. As a result, the number of people working from home is increasing rapidly. Research shows that 1.54 million people in the UK work from home for their main job, and 60% of the UK's adult population are working from home during the coronavirus lockdown. Whilst remote workers tend to be more productive and experience greater job satisfaction, many companies have expressed concern that remote working could pose a threat to cybersecurity.

Coderus has put together some useful tips on how you can implement safe and secure remote working practices by using an effective integrated management system (IMS) process and enforcing appropriate working from home policies.

Connect Networks Through Virtual Private Networks (VPNs)
Remote workers typically need to spend long hours connected to the networks of their organisations, so a virtual private network (VPN) is crucial for your online privacy. A VPN is a tunnel through which data can travel between networks. Traffic goes through the tunnel as *Authentication Header* (AH) or *Encapsulation Security Payload* (ESP) packets. As AH does not provide encryption, you should ensure that ESP protocol is followed. This will render traffic unreadable by anyone who might attempt to intercept it. Likewise, if staff need to use any software-as-a-service (SaaS) resources, they should also access these via the VPN.

Secure Wi-Fi Connections

It is common for householders to take a relaxed approach to Wi-Fi security but when a worker is accessing the company's network remotely, a data breach could spell disaster. To mitigate against this, Wi-Fi users should update their Wi-Fi-enabled devices as soon as a software update becomes available. Wi-Fi enabled devices are anything that connects to the Internet such as laptops, tablets, smartphones, and other smart devices like wearables and home appliances. This will enable any security vulnerabilities to be patched.

In addition, all traffic whether inbound or outbound should be restricted to the highest possible level of encryption. Wi-Fi routers and access points should have encryption set to WPA2 or WPA3.

Set up Firewalls
In order to prevent malicious programs entering your system, firewalls deliver the necessary defence. Since most operating systems include firewall protection, you should instruct your remote workers to ensure that their firewalls are enabled.

For devices that don't include firewalls, or if you just want to enhance levels of protection, search for firewalls from reputable suppliers.

Implement Two-Factor Authentication for Added Security
Two-factor authentication or 2FA, offers an added layer of protection from phishing scams and password leaking. Besides entering a username and password, users must also provide some additional piece of information. This second factor could be an answer to a secret question such as your mother's maiden name, a fingerprint, or perhaps a one-time passcode that is sent to your mobile phone. Whatever it is, it should be something that a hacker can't easily exploit.

Maintain a Comprehensive Filing System on the Cloud
For an IMS to function seamlessly, files need to be instantly accessible whatever the user's location. Remote working can be made much easier by ensuring that any files that are to be shared between several members of staff are stored on the cloud. Minimise frustration by making your filing system easy to navigate by ensuring that all files are kept in one place, arranged by department.

When choosing a cloud company, keep security in mind and choose a company that has its own active security processes.

<u>Special consideration for Apple users</u>
If you're running a Mac, you probably already backup your files through Time Machine. Whilst this is perfectly good for backing up within the same LAN, you will have discovered that doing so over a VPN isn't so straightforward. One solution is as follows:

dns-sd -P DiskStation "_adisk._tcp." "local" "9" Diskstation.local 10.100.15.153 10.100.15.152:9 10.100.15.151:9 10.100.15.150:9 sys=adVF=0x100 dk0=adVF=0x83,adVN=Office\ Backups,adVU=AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEEE dk1=adVF=0x83,adVN=Dev\ Backups,adVU=AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEE2 dk2=adVF=0x83,adVN=QA\ Backups,adVU=AAAAAAAA-BBBB-CCCC-DDDD-EEEEEEEEEEE1

dns-sd -P DiskStation _afpovertcp._tcp. local 548 Diskstation.local. 10.100.15.153 10.100.15.152:548 10.100.15.151:548 10.100.15.150:548dns-sd -P DiskStation _smb._tcp. local 445 Diskstation.local. 10.100.15.153 10.100.15.152:445 10.100.15.151:445 10.100.15.150:445

Provide the Necessary Resources

Under normal circumstances, you wouldn't leave cybersecurity to the individual user. Ultimately, your highly-trained IT team should be in full control of tools and processes. It is their responsibility to maintain the security of your data, and the integrity of your IMS. They must ensure that anyone accessing your systems has authority to do so, and they should communicate the rules and procedures clearly to remote workers.

It is also within the remit of the IT department to establish the legitimacy of online services, approve cloud storage and file sharing tools, and set up services like Google G Suite, Zoom, Slack, Microsoft Teams, and other online tools that facilitate productive remote working.

Likewise, if USB drives are used to share files between devices, IT should thoroughly vet these to avoid cross-contamination.