Cyber Resilience Checklist:

Cyber POA for Hybrid Workers

Hybrid workers have quickly become the number one target for cybercriminals, which is why we've put together a checklist of best practices to help you maintain a strong security strategy, regardless of where or how you get your work done.

Some of these points might be the basics, but they're easy to forget when mixing up where you work, whether that's at home, on the commuter train or in a coffee shop. So why not refresh with our checklist?

1. Install essential security protection

Ensure all your devices, whether company-issued or personal, are protected by actively licensed antivirus and antimalware solutions.

2. Keep hardware and software updated

Cybercriminals will exploit security vulnerabilities in your hardware and software systems. To keep your systems as secure as possible, you need to install updates right away.

3. Secure your home network

When working from home, make sure you're using a wireless network that is secure and password protected. Never use the default internet router credentials. Always change them to maximise security.

4. Use a VPN to access company resources

Using a VPN (virtual private network) while accessing company data or applications helps protect your privacy by encrypting all traffic and data being transmitted.

5. Enable multi-factor authentication

Multi-factor authentication enforces strict control over who logs in to company systems and applications, ultimately protecting against unauthorised access of confidential data should your individual credentials be compromised.

6. Secure personal devices

If you have permission to work and access company systems with your personal device, it's critical that you implement encryption for all data assets and internet traffic and make sure your device is password-protected.

7. Follow company password policies

Weak and bad passwords will spoil even the tightest security strategies. Make sure you are adhering to your company's password policies and criteria requirements.

8. Learn about and adhere to all company security policies

An essential security practice when working remotely is to follow your company's IT and security policies. This helps you securely access your company's data, networks and resources, and minimise risks.

9. Beware of phishing scams

Read emails carefully before responding and avoid malicious links. Be aware of the context, who the email is from and look out for any key giveaways, like poor grammar and spelling.

10. Back up everything

Data loss can result from a variety of incidents, such as system failures or accidental deletions, and can cause costly downtime. Make sure all files and data are backed up regularly and securely according to your company's backup policies.

11. Avoid using public Wi-Fi

Multi-factor authentication enforces strict control over who logs in to company systems and applications, ultimately protecting against unauthorised access of confidential data should your individual credentials be compromised.

12. Lock your device or log out when not in use

An unlocked device is an invitation for trouble. Make it a habit to lock your device when unattended.

13. Never share passwords or account credentials

Never share your passwords or login credentials with anyone – colleagues, family members or friends.

14. Company-issued devices are for your use only!

Never allow family or friends to use your company-issued devices or any devices that contain private, sensitive or restricted company data or systems.

15. Avoid printing or writing down sensitive information

Avoid the risks that come with protecting documented, confidential information by never printing or writing down any sensitive or private data. If necessary, keep records securely put away and out of view.

16. Company devices are not for personal use

Using company-issued devices for personal activities, such as online shopping, gaming or social networking, puts your company's sensitive data at risk and could introduce malware into the devices.

17. Stick to company-approved communication resources

Don't use personal emails for business communication. Always use company-provided resources, such as corporate emails, to communicate or share documents and other information.

18. Complete security awareness training

Make sure you complete the training programs to learn the strategies, measures and actions needed to protect yourself and your company.

If you need help securing your hybrid working environments, devices or data, contact us today.