

13 POINT

SECURITY RISK CHECKLIST

REMOTE
WORKER
EDITION

13 common remote workplace vulnerabilities that are putting your data at risk.



68%

of business
leaders feel their
cybersecurity
risks are
increasing with
remote workers.

- Office Tech Insider



ALLIED
BUSINESS SOLUTIONS

allied. tech

13 POINT

SECURITY RISK CHECKLIST

REMOTE WORKER EDITION

- 1. Unauthorized Access to Data on Your Home Device**
Encrypting data on devices helps prevent unauthorized access to data by making it difficult to decipher and protects against lost or stolen devices. ☐
- 2. Unpatched Software**
Update operating system and application software with the latest versions to eliminate vulnerabilities used by cybercriminals. ☐
- 3. Automatic Logins**
Unattended devices enabled for automatic logins are easy targets to prying eyes – disable so unattended devices require a password, PIN or biometric alternative to turn them on or resume from sleep. ☐
- 4. Easy to Guess PIN or Password**
Don't use one password for all logins, or lazy ones like 123456 – use one that looks random to anyone but you or consider using a password manager to ensure that each destination login uses a unique, difficult password. ☐
- 5. Identity Theft, Fraud, Data Loss**
Enable two-factor authentication that requires a password and one-time codes generated by authenticator apps to verify your identity and prevent access to sensitive data. ☐
- 6. Lost or Stolen Devices**
Enable "Find my Device" and remote wipe all data on your mobile devices if lost or stolen. ☐
- 7. Discarded Devices**
It's important to wipe hard drive data and reset devices to factory settings when giving, selling or throwing them out. ☐
- 8. Public or Untrusted Networks**
Use a VDI to establish a secure and encrypted connection to your company's network to keep your data safe from being intercepted. ☐
- 9. Unsecure Document Destruction**
Confidential paper documents need to be shredded or disposed securely to prevent a breach. ☐
- 10. Avoid Suspicious Emails or Websites**
Knowing that the cyber threat landscape is real, practice good judgement when clicking on links in emails or visiting suspicious websites. ☐
- 11. Using Your Home Computer for Work**
Business devices often have business class antivirus and threat management tools that most home computers don't have. Example; Windows 10 Home version doesn't have the same security options that Windows 10 Pro does. ☐
- 12. Unsecure Work Space**
Multiple users and proximity to windows can cause security risks. Ask yourself, can other people in the home view confidential information? Is your screen visible through a window? Are you locking your device when you're not working? ☐
- 13. Vulnerable Data on Local Devices**
Remote users often save critical documents on their local device instead of the company server because it's easier or they don't want to use VPN connection. Proper training on how, where and why to save information on a company server will ensure your data is more secure and backed up where as most home computers are not. ☐