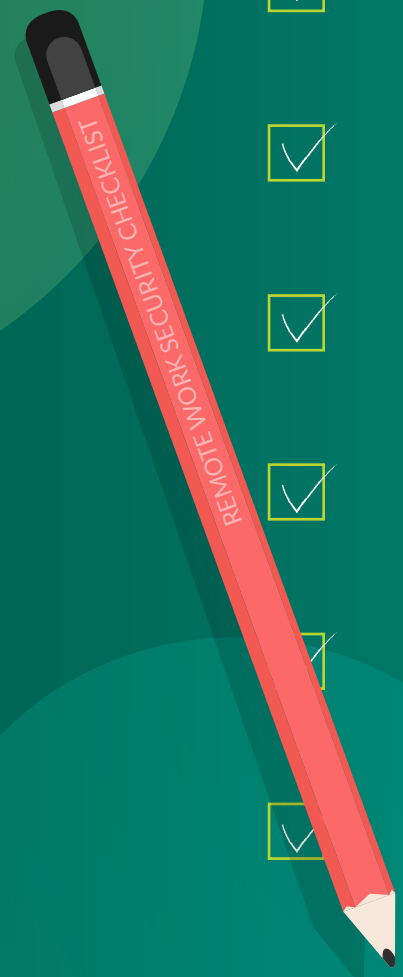
REMOTE WORK

SECURITY CHECKLIST

- [x] Ensure home networks have **current firewalls installed** that provide similar levels of protection to corporate networks.
- [x] Ensure every device has **up to date antivirus software** that offers the same level of endpoint protection that corporate network attached devices have.
- [x] Ensure all relevant data is being **backed up**, including work-in-progress files on remote devices.
- [x] Make sure all devices are being **patched** to maintain a baseline of security.
- [x] Enable **administrator visibility across all devices** with tools such as Microsoft Intune and Microsoft Endpoint Manager to understand what is installed and running on each device.
- [x] Ensure every asset is **secure from being lost or stolen** by enabling Bitlocker on Windows 10 devices.
- [x] Ensure you have **a complex password policy** within your organisation i.e. Minimum password lengths, use of pass phrases including the use of special characters, numbers and symbols. *****



As part of our Desktop as a Service (DaaS) offering in partnership with HP and Intel®, we can ensure your workers' desktops are safely secured, regularly patched and possess the latest anti-virus software to thwart the growing number of threats. Get in touch with us today to find out how we can give you peace of mind for your remote workforce.

Call +64 9 918 3712

Visit softsource.co.nz

softsource®
computing a better way