Working from home or away from the office checklist

The following is a list of business requirements that an organisation needs to implement if they require their staff to work away from the office for any reason.   Anyone who needs to work away from the office (Road warriors, sick or injured) needs to comply with this checklist.

The first section is compulsory.

If these conditions cannot be met, then the users should not be allowed to connect to the corporate network / cloud-based system.

Info	**Do Not** share corporate laptops, smart devices and tablets with family or friends
Info	**Do Not** share itineraries, corporate info, daily routines etc on social media
Info	**Do Not** tell people that you are working from home
Info	**Do** Lock your laptop, smart device and/or tablet when not using it
	Complete remote access education lessons from our learning platform.
	Change the default password on your home router to a complex password.
	Enable WPA2 Wi-Fi security and only connect with a strong pre shared key or password.
	All digital devices connecting to the home network need to use WPA2 encryption, have their firmware updated and their default passwords must be changed.
	Only use a local, non-administrator user account or corporate login on the laptop / remote session / Cloud based system
	Make sure Anti-Virus is installed, updated and active.
	Make sure the firewall is active and updated
	When connecting to the remote server do not save corporate credentials on your laptop / home computer
	2 Factor / multi factor authentication enabled on all cloud-based systems.
	All business activity must be done only on corporate systems
	Read and sign internet policy document.
	If you are connected to a access point / hot spot make sure that your screen cannot be seen by passers-by or outside traffic.
	If using Wi-Fi in a café, corporate lounge or someone else's access point only connect if it requires a WPA2 username and password or a pre shared key.
	Always check for duplicate access points and if you see one do not connect to either
	If in doubt hot spot your smart device using your own complex password

These are additional components (important) that should be implemented but will not stop a person from working away from the office.

	Update your router firmware as required
	Read the breach policy
	Implement a VPN policy to ensure all traffic between the device and the digital world is encrypted

These are nice to be done components (routine)

	Create and use a secure workspace to work in at home where possible.