Action Point Checklist

Cybersecurity strategy — Checklist for remote working

This checklist has been authored for LexisNexis by the **LexisNexis Legal Writer Team.**

Introductory note:
With cases of the Novel Coronavirus (COVID-19) on the rise, many businesses are taking swift action to curb its spread. Remote working or working from home is pivotal to those efforts. While remote working arrangements may be effective to slow the community spread of COVID-19 from person to person, they present cybersecurity challenges that can be different than on-premise work.

Below is a list of recommendations and tips to help guide organisations and staff through these challenges.

Links to related content:

For further practical guidance on cybersecurity, see Overview — Ensuring data protection compliance.

Also refer to Australian Signals Directorate issues cyber security warning for remote working in response to COVID-19.

See also Australian Signals Directorate.

Action Point Checklist

Cybersecurity strategy — Checklist for remote working

Recommendations for organisations		✓
➢	Review your business continuity plans, IT policies and incident response procedures and update if necessary.	
➢	Ensure that your systems, including Virtual Private Networks and firewalls, are up to date with the most recent security patches.	
➢	Ensure you have procedures in place for regular back-up of data and systems.	
➢	If you use a remote desktop client, ensure it is secure.	
➢	Ensure your work devices, such as laptops and mobile phones, are secure.	
➢	Implement multi-factor authentication as a mandatory practice for remote access systems and resources (including cloud services) including, where possible, replacing the use of platforms/software that do not have an option for MFA.	
➢	Ensure that you are protected against Denial of Service (DoS) threats.	
➢	Ensure that your staff and stakeholders are informed and educated in cybersecurity practices, such as detecting socially-engineered messages.	
➢	Ensure that staff working from home have physical security measures in place. This minimises the risk that information may be accessed, used, modified or removed from the premises without authorisation.	

Recommendations for staff		✓
➢	Avoid using public networks. Connect only to your home network or tether through a mobile work device.	
➢	Change the default password on your home router regularly.	
➢	Do not transfer any work files to personal devices.	
➢	Avoid connecting home printing devices, scanners and USB devices, which can store copies of documents.	
➢	Ensure all devices are physically secure to minimise the risk that information may be accessed, used, modified or removed from the premises without authorisation.	

Action Point Checklist

➢	Keep social media and web browsing on work devices to a minimum. Cybersecurity risks increase in a remote environment.	
➢	Do not allow family members to use laptops and devices. This will reduce the risks from social media use, installation of third-party apps, etc.	
➢	Be alert to scams and malicious links in emails (phishing). For instance, do not respond with haste to any “urgent” email requests. Confirm via non-email communication with the requester before taking any actions.	