CYBER RISK MANAGEMENT CHECKLIST

☑ Payment processes and email fraud

- ☐ Before acting on directions for payment that are provided by email, your law practice verifies the payment details by phone (not using the phone number included in the same email as the directions for payment).
- ☐ You inform your clients in writing that you will never send them an email changing your trust or office account details.
- ☐ You advise your clients in writing to contact you urgently if they receive an email from the practice purporting to change payment details.
- ☐ You regularly check your email set up to ensure that there are no unexpected redirection rules in place (in Outlook, you can check this on the Home screen under Rules, then Manage Rules & Alerts).
- ☐ Multi-Factor Authentication (MFA) is required and enabled for all email and email administrator accounts.

☑ Software and virus protection

- ☐ You have a process in place to ensure that new software patches are applied to your IT system and software.
- ☐ All operating systems and browsers in the network have security updates applied and a process exists to do this in a timely manner.
- ☐ Applications and systems that are unsupported by vendors have been decommissioned with an exceptions recorded in a risk register.
- ☐ You have antivirus protection in place and it is kept up to date.

☑ Data storage and back-ups

- ☐ You complete daily data back-ups.
- ☐ You check at least monthly, that your back-ups are readily accessible and able to be used/not corrupted upon retrieval.
- ☐ Where data is backed up in the cloud, you know what authentication procedures are required by the cloud provider to ensure that unauthorised users are not able to access your law practice data.

A joint initiative of THE LAW SOCIETY OF NEW SOUTH WALES OMNIUM JURA DEFENDIMUS Lawcover

☑ Staff risk-awareness and training

□ You have incorporated cyber risk awareness in your staff policies and training.

□ Your firm has a "BYO device" security policy for staff who are able to access work files on non-company devices such as smart phones, tablets or home computers.

□ You have advised all staff in writing of the importance of using passwords that are unique to the workplace only.

□ You and your staff automatically/regularly change your passwords every few weeks.

□ You have discussed with staff the risks associated with clicking on attachments or hyperlinks in emails that look unusual or suspicious, and which could contain viruses, ransomware or other malware.

□ You have discussed with staff the risks associated with using free or unsecured WiFi, importing material onto the practice's computer network through a USB drive, and taking confidential material outside the workplace via USB, mobile phone or laptop.

□ Cyber risk awareness is included in your induction material for new staff.

☑ Data security breaches and privacy protection

□ You have considered whether the Mandatory Breach Reporting regime under the Privacy Act 1988 (Cth) applies to your firm.

□ Your policies and procedures note the importance of reporting relevant data breaches.

☑ Planning ahead

□ You have an emergency response plan for what to do in the event of a cyber-attack.

□ The plan includes seeking crisis assistance from your practice's IT consultant with their contact details recorded for immediate response.

□ The plan is being regularly tested (e.g. in tabletop exercises which involve all key stakeholders for various scenarios). Any opportunities for improvement are identified and acted upon.

□ In the instance of a cyber breach, call the Lawcover cyber response team to access your cyber risk insurance cover on **1800 4 BREACH (1800 427 322).**