Minimum Cybersecurity Expectations
Guidance for Law Practices

Victorian Legal Services
BOARD + COMMISSIONER

To help law practices protect their clients' data and meet their legal and ethical obligations, the following table sets out minimum cybersecurity expectations. It also lists examples of unacceptable cybersecurity practices that we consider capable of amounting to unsatisfactory professional conduct (UPC) or professional misconduct (PM).

Law practice principals should use the table below as a guide to the basic system and behavioural controls you need to implement. This includes the critical system controls without which your practice is most vulnerable. **If there are any critical controls (in the first three rows below) that you are yet to implement, these should be your highest priority.**

System controls and behavioural controls are two types of cybersecurity measures to protect information systems and data:

- **System controls** encompass the technical safeguards implemented within an organisation's information systems to protect against external threats and vulnerabilities.
- **Behavioural controls** focus on influencing and regulating human behaviour to minimise security risks.

Both types of controls work together to protect your law practice from any potential security threats.

Many of them will be straightforward for individuals to implement (e.g. turning on automatic software updates). However, you also need to consider whether your practice requires additional security measures, based on its size and capability, the type of work you perform, and the nature and location of your clients.

If you require support or guidance to understand and implement these controls, or to determine which additional controls are right for your practice, we recommend engaging an IT security consultant. Your professional association may also be able to assist you. Community legal centres can contact the Federation of Community Legal Centres for further support.

	CYBERSECURITY AREA	OUR EXPECTATIONS	CONDUCT CAPABLE OF CONSTITUTING UPC OR PM
CRITICAL CONTROLS	Security updates	• Keep all work devices, apps and software used in your practice up to date with the latest security updates. This includes laptops, servers, operating systems, and network hardware. • Turn on automatic software updates where available, and otherwise manually check for new, improved, or fixed versions at least once a fortnight. • Don't run outdated or legacy software (i.e. software that is no longer updated or maintained by the developer) unless it is genuinely necessary, and only do so with close IT supervision.	• Failing to install security updates and patches. • Failing to install available software updates. • Failing to turn on automatic updates or alternatively manually checking for updates at least fortnightly.
	Passwords and logins	• Set a strong, unique password or passphrase for all devices or accounts used to handle work data. If using a passphrase, it should be long, unpredictable, and use a random mix of unrelated words. • Don't reuse passwords or passphrases across more than one account. • Don't use weak, common or previously compromised passwords, or passwords that include personal information, on work devices and accounts. • Consider using a secure password manager to randomly-generate, autofill, encrypt and store strong and unique passwords for your online accounts. Consider giving staff access to a secure password manager on all their work devices. • For passwords that you need to memorise or type frequently (like your computer login, or the password for your password manager's vault), create a strong and unique passphrase. • If you cannot use a password manager, write your passwords and passphrases in a notebook and secure it in a safe place (i.e. under lock and key in a secure location or in a safe). • Immediately change any passwords that have been compromised or used with an account that has been hacked.	• No passwords or passphrases set for work devices and accounts. • Sharing passwords or passphrases to individual accounts (e.g. your email login) with anyone else. • Reusing passwords or passphrases across more than one account. • Using weak, common or previously compromised passwords, or passwords that include personal information, on work devices and accounts. • Storing passwords and passphrases in insecure locations (e.g. on sticky notes or unencrypted Word documents). • Leaving devices logged-in and unlocked while unattended (including in your office).
	Multi-factor authentication (MFA)	• Turn on multi-factor authentication (MFA) on all online accounts and services where it is available. Follow online guides for common services (such as Microsoft, Google or Apple accounts) by searching online for "how to turn on MFA" for that service. Alternatively check your account settings to enable MFA. Do not disable MFA or ignore the option to turn it on.	• Disabling MFA or failing to activate MFA where it is available. • Sharing MFA codes with others. • Approving unexpected or unknown sign in attempts in your MFA application or device.

	CYBERSECURITY AREA	OUR EXPECTATIONS	CONDUCT CAPABLE OF CONSTITUTING UPC OR PM
SYSTEM CONTROLS	**Security software**	• Install and turn on security and antivirus software on all work computers and devices. You should enable the default antivirus programs built-in to your current devices as a starting point, but you may require third-party or more robust solutions depending on your security needs. • Run a full antivirus scan on work devices to detect malware and viruses, and to ensure that your program is properly configured. This should be done when work devices are set up or reconfigured, as well as after a change in user. • Perform regular virus and malware scans on your work devices, ideally once a week. Configure the software to do automatic scans if it can do so. Otherwise, you should manually run the scans. • Configure all work devices to use a secure Domain Name System (DNS) provider (such as Quad9, OpenDNS, or dns0.eu) to block malicious websites using DNS filtering or security software.	• Leaving devices unprotected by not using any security software, not running any virus and malware scans, and/or not enabling built-in security features (e.g. the system firewall). • Using pirated software which may contain vulnerabilities. • Ignoring or disabling security alerts or warnings without good reason (e.g. on the advice of your IT department or service provider).
	Access control	• Put in place a procedure for granting staff different levels of access to programs, websites, computers, and client information, based on job roles and responsibilities. This is known as 'role-based access control'. Limit staff access to what is necessary for their role. • Ensure contractors, temporary staff, interns, and trainees are only given access to the information and systems they need to do their job for as long as you employ or engage them. Provide them with their own individual login details, or with temporary guest access. • Record access permissions, and monitor staff access to sensitive information (i.e. check that information is only accessed by appropriate persons with the correct level of access). Consider using access control software to keep track of who has access to what. • Regularly review who has permission to access sensitive information, preferably once a month. Promptly update access for staff who change roles; revoke access for staff who leave your practice at the time of their exit. • Don't use accounts with administrator access (i.e. complete and unrestricted access to create, delete, and modify files, folders, and settings) for everyday tasks. Set up standard user accounts for everyday work, and reserve administrator access for IT administration (e.g. installing software). • Only use shared accounts (i.e. accounts owned by the organisation rather than a staff member, such as library accounts and social media accounts) where there is no other option.	• Giving users access to work systems and data beyond what is required to do their job. • Inappropriately devolving access to, and responsibility for managing, online accounts (e.g. to an assistant). • Not promptly revoking temporary access, or reusing login accounts (e.g. 'intern1') for temporary staff.
	Devices	• Turn on full disk encryption for all work devices that store or work with sensitive, confidential, or privileged data. • Change the default passwords when first setting up all hardware on your network, including servers and routers. • Set devices to automatically lock when inactive. • Ensure work and personal devices are physically secure (i.e. locked away) and stored safely, especially when not in use. • Only use USB sticks and external hard drives on work devices if they are from sources you are confident are secure. • Consider whether to allow staff to use personal devices such as smartphones, tablets, or home computers to access work files or connect to the office network. If you decide to allow this, you are responsible for giving staff assistance and detailed guidance on securing their personal devices and home networks (e.g. through providing a secure Virtual Private Network (VPN)).	• Leaving work devices physically unattended in a public place (even if locked or shut down). • Allowing unprotected personal devices to access confidential information. • Using unknown devices or accessories (e.g. promotional USB sticks or scavenged drives) with work devices and networks. • Not having a clear policy on whether staff can use personal devices to access work data or networks. • Not training staff who use their own devices for work purposes on how to secure their devices or home networks. • Not establishing and enforcing device security rules or policies for staff.

	CYBERSECURITY AREA	OUR EXPECTATIONS	CONDUCT CAPABLE OF CONSTITUTING UPC OR PM
SYSTEM CONTROLS	**Information security**	• Ensure all copies of sensitive, confidential, or privileged data are encrypted when storing that data (including on external drives and cloud services) and when transferring that data to other organisations. • Only use unencrypted communications (e.g. email) to send or receive high-risk information (e.g. health information, financial details, identity documents) from clients at their request and only if strictly necessary. • When you stop using a hard drive or device, ensure that it has been securely and completely erased, or that the drives have been completely destroyed. • Review client files and data regularly (we recommend every two years) to determine whether it is necessary or advisable to retain the files or data beyond the minimum required period. • When keeping documents to use as a precedent, extract them from client files and store them separately, after redacting any confidential or sensitive information.	• Storing your client data on unencrypted drives. • Retaining client files indefinitely, without good reason.
	Backups	• Consider what information needs to be backed up based on its importance and potential impact of loss (e.g. important files, client details, and financial records). • Choose and set up a backup service that meets your needs. This might be a cloud backup service (i.e. Microsoft OneDrive or Apple iCloud), an external storage device, or a combination of both. You could also work entirely in the cloud with a commercial provider that allows recovery of deleted documents and previous versions. • Back up your files regularly to avoid permanent data loss due to cyberattack, system failure, or accidental deletion, and maintain a routine depending on how frequently your data changes and how important that data is. You can also enable automatic backups. We recommend backing up at least once a fortnight. • Encrypt backups and store any physical copies in a secure location. Don't store backups in the same location as primary devices, so they are not vulnerable to the same physical incident (e.g. a fire). Ensure recent backups can be accessed quickly. • Regularly check that backups are being made as scheduled, including after any change. Test that the backups can be successfully restored at least once a year. If a backup test fails, investigate the issue and take corrective action immediately. • Retain backups and logs for an appropriate period and ensure that they are accessible when needed (i.e. when requested by regulators). The retention period for logs will depend on what type of logs are kept (from 18 months to seven years) and previous backup versions should be retained for two years (unless the information is particularly sensitive and no longer needed).	• Not either backing up your data, or alternatively storing your data in a secure cloud service which allows recovery. • Storing backup data unencrypted, whether on a drive or in the cloud. • Failing to retain data, documents, and logs for compliance, auditing, and forensic purposes, as needed (subject to the **information security** expectations above).

	CYBERSECURITY AREA	OUR EXPECTATIONS	CONDUCT CAPABLE OF CONSTITUTING UPC OR PM
BEHAVIOURAL CONTROLS	Training	• Provide all staff with comprehensive cybersecurity training relevant to their specific roles and responsibilities, on topics such as phishing emails, social engineering, password best practices, safe web browsing, and other risks. Also complete this training yourself. • Require new staff to undergo training as part of induction and provide existing staff with refresher training at least once a year. • Update cybersecurity training as required to address relevant and emerging threats, at least yearly. • Ensure all staff understand their role in maintaining cybersecurity, and their obligations in the event of a cybersecurity incident. • Share with your staff any cybersecurity updates you receive that are relevant to your practice.	• Not educating staff who use work devices and networks on how to identify, report, and respond to cyberattacks. • Not providing your staff with up-to-date cybersecurity training.
	Client or bank verification	• Ensure daily trust account transactions are monitored by someone with appropriate seniority and experience. • Implement procedures to verify client details, such as account numbers and email addresses, before actioning requests or sending correspondence. • Scrutinise client instructions, emails, and requests for funds or confidential information for red flags such as unusual requests, changes in payment instructions, or urgent demands. • Verify all payment details by a pre-established alternative communication method (i.e. phone, video chat, or in person) before making money transfers. • Explain cybersecurity risks to clients and warn them not to send sensitive or confidential information via email where possible. • Ensure that all staff are familiar with the procedures and quickly flag any breaches so that remedial action can be taken.	• Failing to regularly inspect (or review) trust account transactions to promptly identify defalcations/deficiencies (principals with trust authorisation). • Not training staff who handle client instructions or money transfers on the client verification process, or not enforcing compliance with that process. • Not verbally verifying written client instructions and emails regarding money transfers. • Not having a way to communicate with your client other than email. • Not taking reasonable steps to warn clients about cyber-risks and the risks of insecure communications.
	Incident response and reporting	• Create and implement an incident response plan with clear procedures to identify an incident, understand its scope, mitigate, document, and report it. We recommend following the basic action lists adapted from the Law Council of Australia and the LPLC. • Ensure all staff are aware of the incident response plan and know what to do if they become aware of a potential cybersecurity incident. • Regularly update and test your incident response plan. We recommend doing so at least once a year. • Ensure that you have up-to-date direct contact details for your bank's security team, and make sure they are readily available to all staff who may need to report an incident to the bank. • Immediately report any cyber-incidents to the Australian Cyber Security Centre, the security team of any involved banks, and (if relevant) PEXA. Also inform the LPLC, police, and the VLSB+C. • Promptly inform your clients if their information has been affected by a cyber-incident. • Encourage a culture of reporting within your practice, and establish a process for information sharing, incident reporting, and post-incident discussion.	• Not establishing a cyber-incident response plan with assigned roles and responsibilities. • Not reporting and managing security incidents promptly. We will take into account if you have reported incidents to us promptly when considering whether disciplinary action is warranted. • Underreporting or covering up incidents.