Lawcover®

CYBER SECURITY **SNAPSHOT**

PROTECT YOUR DATA

Identify what data you have, what it is used for, who uses it and where it is stored

Schedule regular data backups and test the integrity of these backups periodically

Manage user accounts and control access to sensitive information and files

Create awareness and train staff in safe internet practices

Protect against the risks of remote working and never access sensitive information or emails using public WiFi, and use an enterprise VPN that is configured to ensure a secure internet connection

STEP BY STEP

IDENTIFY YOUR DATA

To safeguard your law practice, it's essential to understand your valuable assets. A crucial step is creating a comprehensive data asset registry. This registry helps identify, categorise, assess, and protect sensitive data like client information, employee records, financial data, and intellectual property. By having a clear inventory of your data assets, you can implement tailored security measures to mitigate risks, build a robust data protection strategy and ensure compliance with regulations.

Heading	Description	Example Data
Data	Specific type of data	Client personal information, financial records, employee records, intellectual property etc.
Location	Where the data is stored	On-premises servers, cloud storage, paper documents, etc.
Critically	Importance of the data to the organisation	High (critical to business operations), Medium (important but not critical), Low (less important).
Owner	Responsible individual or team	Legal department, HR department, IT department, etc.
Use	How the data is used	Client management, financial reporting, employee managment, research and development, etc.
Users	Who has access to the data	Specific individuals or groups within the organisation who have or need access to the data.
Protective Controls	Security measures in place	Encryption, access controls, firewalls, antivirus software, backup and recovery procedures, etc.
Retention Time	How long the data should be retained	As per legal and regulatory requirements or organisational policies.

Below is an example of an Asset table. The column headings in the Asset table below are described in the table above.

Data	Location	Critically	Owner	Use	Users	Protective Controls	Retention Time
Personal Information	CMS	High	Sales	Client Contact Details	All Users	MFA to sign in	3 years
Database							
Privileged Data							
Banking Information							
Accounts							
Case Details							

STEP BY STEP
IDENTIFY YOUR DATA

- Regularly review and update this registry to ensure its accuracy and completeness
- Seek input from employees to identify any additional data assets or security concerns
- Train employees in data security best practices, including password security, phishing awareness, and data handling procedures
- Encourage a culture of data protection to safeguard sensitive information and comply with relevant regulations
- Ensure appropriate access management controls are in place to ensure users only have access to the minimum number of files and folders they need to complete their job. For further guidance please see our Guide to Cyber Security.

STEP BY STEP

DATA BACKUP AND RESTORATION

A data backup is a copy or archive of the important information stored on your devices such as a computer, phone, or tablet, and it's used to restore that original information in the event of a data loss.

DATA BACKUP AND RESTORATION - SAMPLE ACTION PLAN

ACTION	STEPS TO BE TAKEN
What data?	Back up any data that is essential for running your law practice. The backup should include your practice data and configuration data required to operate your systems. As a baseline, you should back up anything sensitive or confidential in nature, is essential to the running of your practice or that can't be replaced if it's lost.
Back up regularly	Develop and maintain a schedule to conduct regular backups of data. This should occur at a convenient time for the practice (weekends or overnight will avoid disruptions to work during practice hours) and can be automated through your operating system. Retain backups for every month, rather than just a single rolling backup. A single backup does not provide much protection if an infection isn't noticed before the backup is overwritten.

As a baseline, you should back up anything sensitive or confidential in nature, essential to the running of your practice or that can't be replaced if it's lost.

STEP BY STEP
DATA BACKUP AND RESTORATION

Storage and maintenance of backed up data	Consider both a physical backup method of storage (like an external hard drive) and a cloud based option. For instance, if your office is flooded, a physical data backup like an external hard drive might be lost. But data that's backed up on the cloud will not. Maintain multiple backups of important files and store these in different locations. The '3-2-1' rule is a popular strategy used in most scenarios; at least three copies on two devices and one offline backup (kept separate from your network – e.g. cloud). Multiple backups ensure that at least one other copy is intact if one is compromised.
Access to backups	Restrict access to credentials and servers used for backups as these can be targeted by attackers, either to obtain your data or to destroy your ability to recover it. Use version control, native access control lists, roles, or permissions to ensure that previous versions of files are protected from accidental or malicious deletion, especially when using cloud synchronisation services for backups.
Testing backups	Test the quality of data backups through restoration exercises. The integrity of the data that has been backed up needs to be ensured if the practice is to resume normal operations from a cyber incident or IT disruption as soon as possible.
Restoring backups	Data backups may contain unwanted malware. To ensure any malware is eliminated in any backups, files should be scanned using up to date antivirus software when they are being restored. Reduce the risk of re-infection when restoring backed up data by re-installing executables from trusted sources. Ensure operating systems and application software are up to date.

Windows

Windows

Refer to your operating systems user guide or website for specific instructions on how to conduct a backup and restore.

Apple

Apple

Refer to your operating systems user guide or website for specific instructions on how to conduct a backup and restore.

STEP BY STEP

DATA LOSS PREVENTION

Data Loss Prevention (DLP) policies in Microsoft and Google platforms are designed to help you identify sensitive data in your environment and stop unauthorised transmission of these types of data.

CUSTOMISE YOUR DLP POLICY

DLP policies can be tailored to your practice needs. For example you can receive an alert when sensitive information like credit card details have been shared with someone outside of your practice.

Microsoft 365

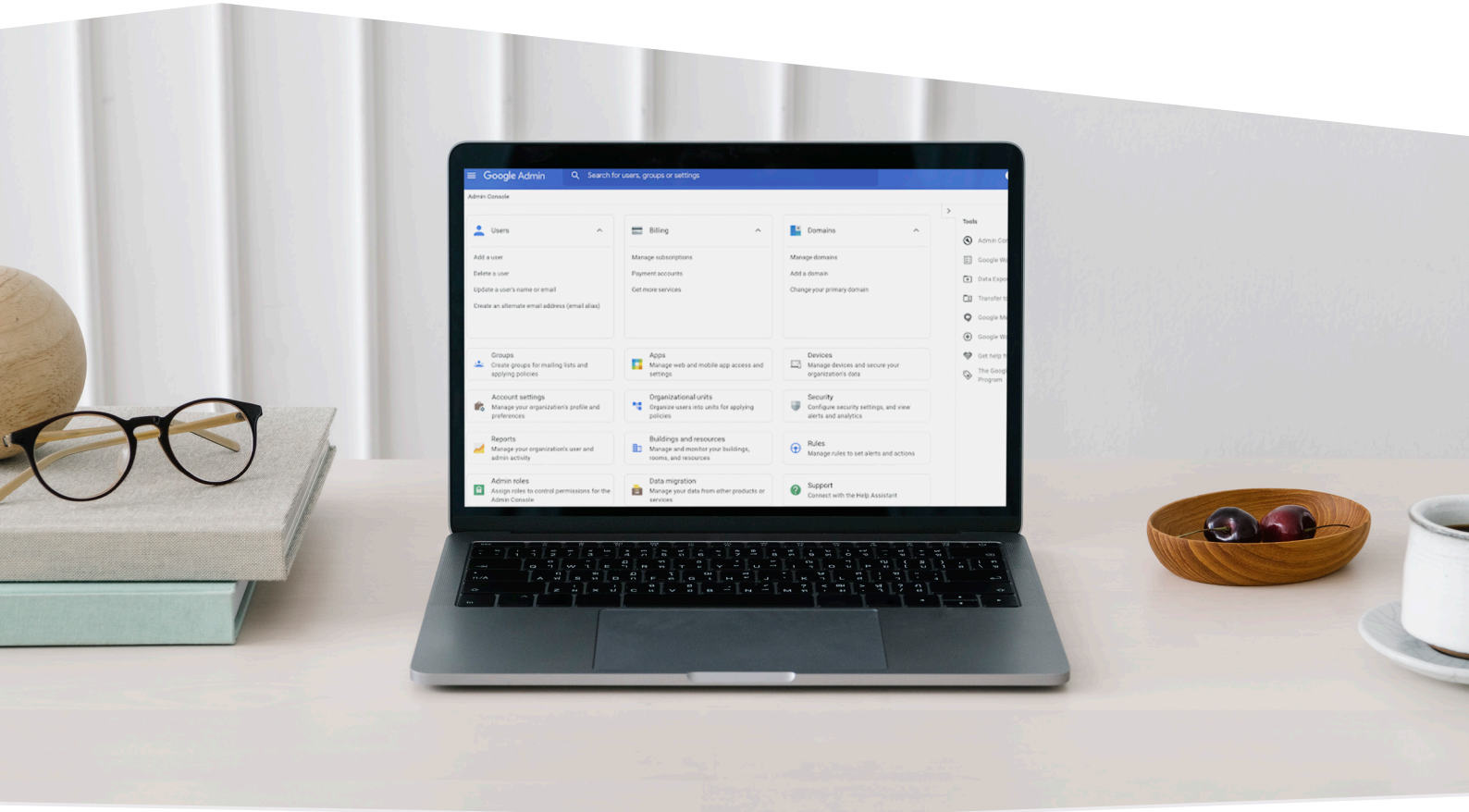
Through the Security & Compliance Centre, you can refine the DLP policy to:

- Send you an incident report email when users share sensitive information with people outside your organisation
- Add other users to the email incident report
- Block access to the content containing the sensitive information but allow the user to override and share or send if they need to.

STEP BY STEP
DATA LOSS PREVENTION

Google

- Sign in to your Google Admin console
- Sign in using an administrator account, not your current account
- From the Admin console Home page, go to Security and then Data protection
- Under Rule recommendations, click Review Recommended Rule
- Review the rule summary page, which shows the rule configuration settings. Click Create to implement the rule with the default recommended settings. Click the Edit rule to navigate to the first step in the rule configuration flow. Or, you can click Back to navigate to rule settings and change them as needed. Go to Create new DLP for Drive rules and custom content detectors for details on creating and working with DLP rules
- After creating the rule, you return to the Data protection Homepage and receive a confirmation message
- As you implement a recommended rule, the rule is removed from the list of recommendations. Other rule choices may be added for your consideration.



STEP BY STEP

OPERATING SYSTEMS AND USER ACCOUNTS

A user account exists when you have an established relationship with a system. Most systems that use the internet or a computer/smart device require a user account. Generally, you must sign in to use the account. Examples include: operating systems (Windows or Apple iOS), data bases, email, internet banking, document or file sharing, online subscriptions.

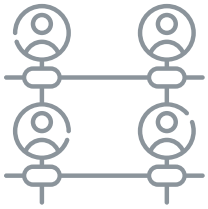
OPERATING SYSTEMS

There are usually two main types of user accounts in an operating system: standard and administrator. Administrator accounts are special accounts that have all privileges to perform tasks, install or change software, and manage other user accounts. Standard accounts are for general everyday use. As a standard user you can still perform necessary tasks, however you cannot change or install anything on the computer without administrator permission.

Administrator accounts are the 'keys to the kingdom'. They give the user full control of the computer.

Cybercriminals will target administrator accounts in order to take full control of a user's computer. Not using an administrator account for everyday use will help limit what a virus or exploit can access if your computer becomes infected.

STEP BY STEP
OPERATING SYSTEMS AND USER ACCOUNTS



Check, change, audit or remove user accounts on your operating system

Microsoft Windows 10

1. Click the Windows icon, type “Control Panel,” and click on the Control Panel app
2. Click User Accounts. Please note that you will need to be on or have access to an administrator account to make any of these changes
3. Select Add or Remove user accounts
4. Check to see if there are any unusual accounts. You should only have one administrator account, and your daily use account should not be the administrator account

Apple macOS

Check user accounts:

1. Click on the Apple icon in the top-left of your screen and click on System Preferences
2. Click User and Groups
3. Check to see if there are any unusual accounts. You should only have one administrator account, and your daily use account should not be the administrator account

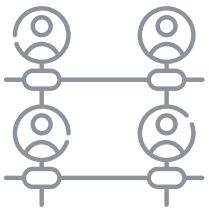
Change the account type:

1. You may need to unlock the User & Groups preference pane by clicking the padlock icon in the bottom-left of the System Preferences window, entering your administrator password, and clicking Unlock
2. Select the account you want to change from the list of accounts on the left
3. Check or uncheck the box ‘Allow user to administer the computer’
4. When changing the user type, you will need to restart the computer for your changes to take effect

Removing user accounts:

1. Select the account you want to remove from the list of accounts on the left
2. Click on the – icon on the bottom left
3. Choose between deleting all the files of the user you are removing or keeping the files
4. Click Delete User to confirm you are removing the account

STEP BY STEP
OPERATING SYSTEMS AND USER ACCOUNTS



Implement strong user access controls to ensure that employees can only access the data and systems necessary to perform their specific roles. By restricting access, you can significantly reduce the impact of a cyber security breach.
For example, if an employee's device becomes compromised by ransomware, appropriate access controls can confine the attack to a limited set of files which prevents widespread damage to the entire practice.

OTHER USER ACCOUNTS

There are numerous subscription services, document sharing applications and the like that are used in everyday practice. It is important that the security around these services and applications is reviewed and updated regularly. This includes staff access and use.

Check, change, audit or remove user accounts on subscription services or document sharing applications (for example)

Dropbox

Change an admin:

1. Sign in to Dropbox with your admin credentials
2. Click Admin Console
3. Click Members
4. Click the "..." (ellipsis) next to the member you want to make an admin
5. Click Make Admin
6. Select the correct admin permissions level in the pop-up window and click Add
7. Click OK

Often, the principle of least privilege is the safest approach. This gives users the minimum access they need to perform their work. You can always change access levels if required.

STEP BY STEP
OPERATING SYSTEMS AND USER ACCOUNTS

> A cyber breach can occur at any time while using an application, program, database, website etc. Maintaining user safety and conducting regular audits of user accounts and permissions can help mitigate the risk of a cyber breach.

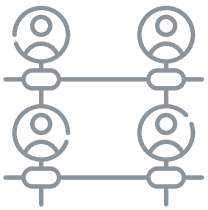
Remove an admin:

1. Sign into Dropbox with your admin credentials
2. Click Admin Console
3. Click Members, and then locate the member whose account you'd like to delete
4. Click the "…" (ellipsis) next to the member you want to remove as admin
5. Click Change Role
6. Click Remove Admin Role
7. Click OK

Change admin permissions:

1. Sign into Dropbox with your admin credentials
2. Click Admin Console
3. Click Members
4. Click the "…" (ellipsis) next to the member whose admin permissions you want to change
5. Click Change Role
6. Select the correct admin permissions level in the pop-up window and click Change
7. Click OK

STEP BY STEP
OPERATING SYSTEMS AND USER ACCOUNTS



LexisNexis:

Edit User Product Access:

1. Select the Product Access tab to see the products to which the user whose name is displayed has access
2. Click Edit to edit product access
3. Make desired changes using the checkboxes and then click Save

Check Individual User Functions:

a) Status. Select this drop-down list to change the status

b) Role. Select this drop-down to change the user's role. Choices include end-user and admin

c) Reset Password. Select this to issue the user a new temporary password

d) Details. Select this tab to view and edit the general information for the user

e) Product Access. Select this tab to view and edit the user's product access

Google

1. Sign in to your Google Admin console using an administrator account, not your current account

2. In the Admin console, go to Menu and then Rules

3. Click Templates

4. Click one of the templates in the list

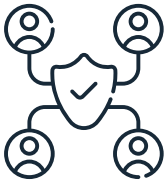
5. Choose your rule's scope. You can apply to all in your domain (the default setting), or you can apply to specific organisational units or groups

6. Click Continue

7. Click Create and activate

STEP BY STEP

REMOTE WORKING



Public Wi-Fi amenities may be convenient but are laden with risk. It's easy for information sent on a public Wi-Fi network to be intercepted and used by cyber criminals. Setting up a personal hotspot on your mobile means that your cellular data can be used on multiple or other devices securely (e.g. your tablet or laptop). Or alternatively you can use your mobile cellular data and check your email on your phone, without connecting to any external Wi-Fi.

IF YOU MUST USE PUBLIC WI-FI

- Never send or receive sensitive information while connected to public Wi-Fi networks
- Never access your emails if using public Wi-Fi
- When online banking or shopping, sending confidential emails or entering passphrases/passwords or credit card details into websites, switch to your cellular data connection or wait until you're on a secure home or office connection
- Always try to confirm the 'official' hotspot name from venue staff and manually connect your device to it
- Do not let your device automatically connect to public Wi-Fi networks by disabling this option in your device's Wi-Fi settings
- Remember to disconnect from the Wi-Fi network and clear it from your device after using it
- Use an appropriate VPN when sending or receiving information while connected to public Wi-Fi networks.

STEP BY STEP

VPN USE

Cybercriminals spy on weak internet connections and can steal information or install malware on your system. Protecting your internet connection, especially when dealing with sensitive client data or using banking applications is essential.

A law practice should ensure that remote workers can work securely. While the use of an appropriate Virtual Private Network (VPN) is preferable to no protection at all, they do come with vulnerabilities. Remember if all your work is cloud based you should not need to connect to a network or office at all. The information you need is stored and can be accessed securely in the cloud.

To reduce risks associated with insecure networks such as public Wi-Fi, a VPN can be used. VPN software establishes a secure private connection by creating an encrypted tunnel between your computer and another device, across the Internet. There are two categories of client **VPN – Public and Enterprise.**

- **Public VPN** services are offered by many providers, but they come with certain risks. These services are more focused on masking IP addresses and locations and encrypting Internet traffic. There are often security vulnerabilities, like weak encryption or vulnerabilities within the service itself that puts users at risk.
- **Enterprise VPN** services are designed for businesses. They help users connect securely to their office network, another remote site, or a particular system. They also offer everything a public VPN does, but with added benefits including built in software, more robust security and managed solutions.

There are numerous VPN providers to choose from. A law practice should research options and assess which provider is the best fit for their needs.

STEP BY STEP
VPN USE

Enterprise VPN needs to be configured securely to avoid exposing your office network and connected device(s). Multi-factor authentication should always be used, and the device and/or software must be from a trusted source and must be kept updated with security patches.

PURE VPN ALTERNATIVES THAT OFFER ENHANCED SECURITY

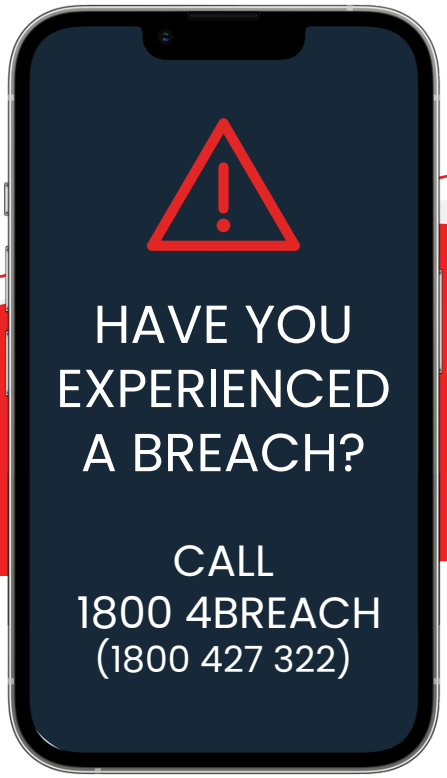
While VPNs mainly offer encryption and secure tunnelling, solutions exist that do that, and more.

Some of the larger antivirus vendors offer an all-in-one solution that is suitable for smaller legal firms. For example, Norton 360 provides antivirus protection, identity theft monitoring, and a VPN for secure Internet connection and work across Windows, macOS, iOS, and Android. While the built-in VPN in Norton 360 also typically needs to be manually toggled on to work, it also offers an Auto-Connect VPN feature that can automatically turn on the VPN when it detects a compromised network. This can be convenient if you must connect to public Wi-Fi networks.

Note: Microsoft Defender for Individuals used to offer an equivalent product, but the Privacy Protection (VPN) feature was deprecated on February 28, 2025.

For larger firms, enterprise-ready, always-on VPNs or Secure Access Service Edge (SASE) technology can be considered. Both provide seamless, always-on security for remote workers using insecure networks, with full encryption of network traffic, enhanced security features, and central management. SASE goes a step further by combining networking and security into one cloud service, ensuring all devices and applications are secure and follow a ‘zero trust’ approach, meaning they don’t trust anything by default. Major SASE solutions include Palo Alto Prisma Access, Zscaler, Netskope, and Cisco Umbrella. A good example of an enterprise-ready always-on VPN is Norton Secure VPN.

Every law practice is different, and each practice should consider its own circumstances when deciding what might work for them.



Lawcover®

Lawcover Insurance Pty Ltd | ABN 15 095 082 509
Phone (02) 9286 8877 | practicesupportservices@lawcover.com.au | lawcover.com.au