

CYBER SECURITY SNAPSHOT



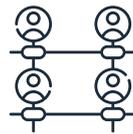
PROTECT YOUR DATA



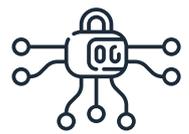
Identify what data you have, what it is used for, who uses it and where it is stored



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



Manage user accounts and control access to sensitive information and files



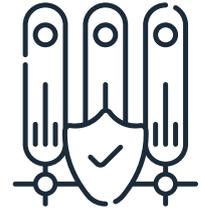
Use a VPN to ensure a secure internet connection



Never access sensitive information or emails using public WIFI



Create awareness and train staff in safe internet practices



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?	<p>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.</p> <p>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.</p>
Back up regularly	<p>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.</p> <p>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</p>

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.

Storage and maintenance of backed up data	<p>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.</p> <p>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.</p>
Access to backups	<p>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.</p> <p>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.</p>
Testing backups	<p>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.</p>
Restoring backups	<p>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.</p> <p>Reduce the risk of re-infection when restoring backed up data by re-installing executables from trusted sources.</p> <p>Ensure operating systems and application software are up to date.</p>



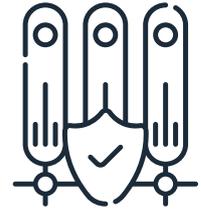
Windows

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



Apple

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



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

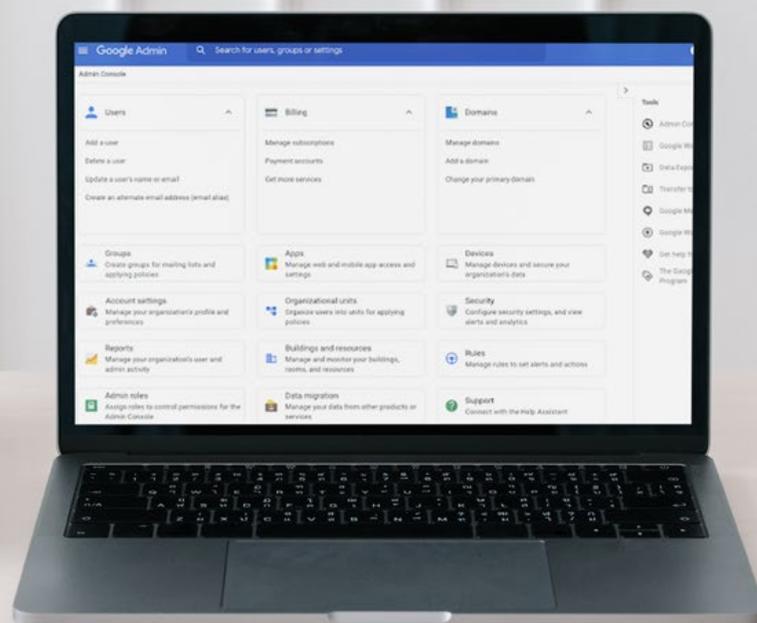
Through the Security & Compliance Centre, you can refine the DLP policy to:

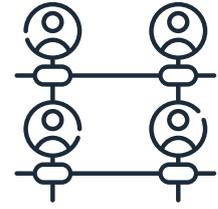
- Send you an incident report email when users share sensitive information with people outside your organisation.
- Add other users to the email incident report.
- Block access to the content containing the sensitive information but allow the user to override and share or send if they need to.



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.





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.

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:

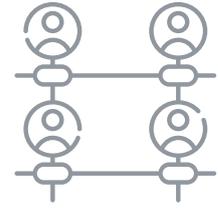
1. Click on the Apple icon in the top-left of your screen and click on System Preferences
2. Click User and Groups
3. Check to see if there are any unusual accounts. You should only have one administrator account, and your daily use account should not be the administrator account.

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.



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 gear icon for the member you want to make an admin
5. Select Add admin permissions from the menu
6. Confirm you've selected the correct admin permissions level in the pop-up window.

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.

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 gear icon beside the member's name and select either Remove admin permissions or Delete user
5. If you're deleting a user, select whether or not you'd like to use remote wipe to remove any files from the user's linked devices the next time they come online, and then click Delete.

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.

Change admin permissions:

1. Sign into Dropbox with your admin credentials
2. Click Admin Console
3. Click Members
4. Click the gear icon next to the member's name
5. Click Add admin permissions or Change admin permissions.

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.





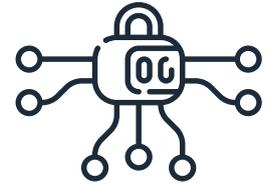
Never access your emails from public Wi-Fi in cafes, airports, hotels etc, as skilled cybercriminals can intercept these connections and compromise your device and data.

WHEN USING PUBLIC WI-FI

- Avoid sending or receiving sensitive information while connected to public Wi-Fi networks.
- 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.
- 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.



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.



INTERNET USE

Cybercriminals spy on weak internet connections in airports, bars, hotels or cafés 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 systems that enable remote access are secure. You can achieve extra internet security by installing and using Virtual Private Network (VPN) software. VPN software establishes a secure private connection by creating an encrypted tunnel between your computer and the internet.

A VPN can ensure secure Wi-Fi connections, encrypt your data traffic, download files safely, disguise your location and safeguard your privacy online.

There are a number of VPN providers to choose from. Research your options and assess which provider is the best fit for your needs.



HAVE YOU
EXPERIENCED
A BREACH?

CALL
1800 4BREACH
(1800 427 322)

