Victorian Bar

Technology Minimum Standards

☑ Does your operating system have current vendor support and is it upgraded to the latest version?

(a) Members are permitted to use any device to maintain their practice provided they are supported by the relevant vendors.
   i. Windows devices need to be in line with Microsoft's Product Life Cycle Policy (https://support.microsoft.com/en-au/hub/4095338/microsoft-lifecycle-policy)
   ii. Apple devices need be within Apple's maintenance period (https://support.apple.com/en-au/HT201624).

(b) For barristers with chambers within Barristers' Chambers Limited (BCL), all network connectivity within chambers needs to be accessed using BCL equipment only. Personal network devices such as routers, firewalls, hubs, and switches are not permitted on the BCL Network as specified in the BCL Technology Usage Terms and Conditions.

☑ Are your devices updated for anti-virus, lock screens and have in place automatic updates for vendor security patches?

Barrister computers and related devices need to be in accordance with Victorian Bar's minimum standard of security.

(a) All devices using technology services need to have an up-to-date antivirus subscription.
(b) Any device containing data or has access to member's data is required to have a lock screen configured. This includes computers, smartphones, and tablets.
(c) To ensure security patches are installed, all devices are required to have updates automatically applied. At a minimum, vendor updates need to be installed on computers every 90 days.

☑ Are you using a free cloud storage solution (e.g. Drop Box, iCloud)? Data sovereignty, security and retention may not be guaranteed with these solutions.

The use of cloud-based services needs to be closely evaluated by all subscribing members. This includes being aware of:

(a) The physical location of the data. Victorian Bar and BCL recommend against the use of cloud services hosted outside of Australia.
(b) Backup measures supplied by the service and the physical location of the backup service.
(c) Security measures of the product, including vendor employee and third-party access.
(d) The use of shared accounts and the flow-on effect of security concerns.

☑ Can you recover your data in the event of accidental deletion or the failure of a device?

Backup

All barrister data needs to be recoverable in the event of a failure or deletion. The use of cloud products does not guarantee the recoverability of lost data. It is the members responsibility to ensure all critical data is adequately backed up and recoverable upon request.

Business Continuity Planning (BCP)

It is the responsibility of all members to ensure client information and practicing data is always available. Business continuity and data needs be available:

(a) In the event of an asset failure. This may include the loss of a computer, tablet, or smartphone.
(b) In the event of a property failure such as lost access to an office or chambers.
(c) In the event of a technology failure such as virus infection or corrupted hard drive.
(d) Any other event affecting barrister's ability to practice.

☑ How do you access your emails? There is an increase in security risks and backing up emails with legacy email accounts. Consider migrating to Outlook.

It is the members responsibility to ensure all selected systems and application are fit for purpose. The support of third-party application may be limited within BCL's Service Desk offering.

Email applications need to be within the product's lifecycle and supported by the vendor. These applications are to be configured using best practice and recommended methods. This includes:

(a) Ensuring emails are not being deleted from Vicbar's services as a result of misconfigured applications.
(b) Ensuring calendars and folders are shared with adequate security measures.

Vicbar recommends against the use of POP and IMAP configurations along with local archives such as PST's, or "On My Computer".