



**Majlis Peguam
Bar Council**

www.malaysianbar.org.my

Wisma Badan Peguam Malaysia
2 Leboh Pasar Besar
50050 Kuala Lumpur, Malaysia
Tel : +603-2050 2050
Fax : +603-2050 2019
Email : council@malaysianbar.org.my

Circular No 393/2024

Dated 21 Nov 2024

To Members of the Malaysian Bar

Guidance Notes on Cloud Services | Ensuring High Cybersecurity Standards for Law Firms

With technological advancement via the use of cloud services by advocates and solicitors, the duty to ensure that clients' information and data are kept confidential and secure now extends beyond physical measures to include measures for cybersecurity. Globally, the increase of cybersecurity incidents and personal data breaches involving law firms in recent years has shed light on the necessity for cybersecurity standards in the legal profession.

Following this, the Bar Council Cyber and Privacy Laws Committee has prepared “**Guidance Notes on Cloud Services | Ensuring High Cybersecurity Standards for Law Firms**” (“Guidance Notes”) which specifies the considerations when deciding whether to use cloud services as well as the issues that may arise, possible steps to address them, and best practices and recommendations.

The Guidance Notes do not have any force of law, are merely advisory, and are not legally binding upon or enforceable against advocates and solicitors. However, since most, if not all, Members are utilising some form of cloud services to enhance efficiency in the delivery of their legal services, Members are encouraged to thoroughly understand the details of using cloud services, including reviewing the relevant agreements.

Please click [here](#) (see pages 3 to 21) to view the full “Guidance Notes on Cloud Services | Ensuring High Cybersecurity Standards for Law Firms”.

Please click [here](#) (see page 22) to view the first of a series of infographics summarising the information in this circular.

Should you have any inquiries, please contact Corina Robert Mangharam, Officer, by e-mail at corina@malaysianbar.org.my; or Jasintrawni Ravichandran by email at jasintrawni@malaysianbar.org.my.

Thank you.

Sarah Yong Li Hsien
Chairperson
Bar Council Cyber and Privacy Laws Committee

Guidance Notes on Cloud Services | Ensuring High Cybersecurity Standards for Law Firms

TABLE OF CONTENTS

PART A: OVERVIEW OF THE GUIDANCE NOTES

- (1) Preamble
- (2) Interpretation
- (3) Characteristics, Service Models and Deployment Models of Cloud Services

PART B: UNDERSTANDING CLOUD SERVICES

- (1) Potential Benefit
- (2) Potential Risks
- (3) Best Practices
- (4) Cessation of Practice
- (5) Recommended Practices

APPENDICES

APPENDIX A: Technology by firm size

APPENDIX B: Organisational processes by firm size

APPENDIX C: Security controls by firm size

APPENDIX D: Awareness and training programme

APPENDIX E: Cybersecurity staff training

PART A: OVERVIEW OF THE GUIDANCE NOTES

(1) Preamble

- 1.1 These Guidance Notes specify what advocates and solicitors should consider when deciding whether to use cloud services, and the issues that may arise, possible steps to address them, and the best practices and recommendations to adopt.
- 1.2 These Guidance Notes do not have any force of law, are merely advisory, and are not legally binding upon or enforceable against advocates and solicitors.
- 1.3 These Guidance Notes provide information to advocates and solicitors about using cloud services. Advocates and solicitors are encouraged to thoroughly understand the details of using cloud services, including reviewing the relevant agreements.
- 1.4 Advocates and solicitors may use cloud services to store data as part of the provision of legal services by them.
- 1.5 Advocates and solicitors must be cognisant that the use of any cloud services is done in accordance with and do not infringe the following:
 - (a) Rules and Rulings of the Bar Council, including with specific reference to Ruling 17.11;
 - (b) Legal Profession (Publicity) Rules 2001;
 - (c) Legal Profession (Practice and Etiquette) Rules 1978;
 - (d) Legal Profession Act 1976;
 - (e) Personal Data Protection Act 2010;
 - (f) Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001; and
 - (g) all applicable laws, as amended, re-enacted or replaced from time to time, including (a) to (f) above.
- 1.6 The Bar Council does not object to the informed use of cloud services, provided that advocates and solicitors are aware of the issues raised in these Guidance Notes.
- 1.7 The Bar Council does not regulate cloud service providers. However, it may, at its discretion, inform advocates and solicitors that specific cloud service providers have been blacklisted based on investigated and verified complaints received by the Bar Council. Advocates and solicitors should then decide whether to proceed with such cloud service providers.
- 1.8 The Bar Council does not endorse or prohibit the use of any particular cloud service provider(s).

(2) Interpretation

For purposes of these Guidance Notes:

- 2.1 “Advocate and solicitor” has the meaning ascribed to that expression in the Legal Profession Act 1976 as amended or re-enacted from time to time;
- 2.2 “Advocate and solicitor” shall include a law firm, unless the context shall otherwise require;
- 2.3 “Approved information” has the meaning attributed to that expression in the Publicity Rules;
- 2.4 “Cloud services” refers to application and infrastructure resources that exist on the Internet. Subscribers contract with third party providers for these services, allowing subscribers to leverage

computing resources without having to purchase or maintain hardware and software.¹ This facility is most commonly used for storing and transferring files across several devices, and for sharing data access to selected individuals / organisations.

- 2.5 “Cloud service providers” shall hereafter be referred to as provider(s);
- 2.6 “Etiquette Rules” refer to the Legal Profession (Practice and Etiquette) Rules 1978 as amended, re-enacted or replaced from time to time;
- 2.7 “Laws” shall include guidelines, directives, directions, Rules and Rulings, whether or not having the force of law.

(3) Characteristics, Service Models and Deployment Models of Cloud Services

3.1 Essential Characteristics²

- (a) On-demand self-service: Users can easily and automatically request server time and network storage without needing to interact with the provider directly.
- (b) Broad network access: The cloud services can be accessed over the Internet using devices like mobile phones, tablets, laptops, and workstations.
- (c) Resource pooling: The provider combines and manages computing resources to serve multiple users. Users may not know the exact location of the resources but can specify a general location (e.g., country or data centre). Examples of resources include storage, processing power, memory, and network capacity.
- (d) Rapid elasticity: Users can quickly scale up or scale down their usage of cloud resources as needed. Unlimited resources are available, and they can be accessed in any quantity and at any time.
- (e) Measured success: Cloud systems automatically monitor and optimise resource usage. Usage is measured and can be controlled and reported, providing transparency for both the provider and the user. This includes tracking storage, processing, bandwidth, and active user accounts.

3.2 Service Models³

- (a) Software as a Service (“SaaS”): Using applications provided through a web browser or programme interface. The user has no control over the underlying infrastructure, such as servers or storage, except for limited application configuration settings.
- (b) Platform as a Service (“PaaS”): When the user deploys their own applications onto the cloud infrastructure. The user does not manage the underlying infrastructure but may have control over the deployed applications and some configuration settings.
- (c) Infrastructure as a Service (“IaaS”): This means accessing fundamental computing resources like processing power, storage, and networks. The user can deploy and run their own software, including operating systems and applications. They do not manage the infrastructure but have control over operating systems, storage, and applications, and limited control over networking components like host firewalls.

3.3 Deployment Models

¹ What are Cloud Services? Overview, Hewlett Packard Enterprise [Accessed 11 June 2023].

² New Zealand Law Society Cloud Computing Guidelines for Lawyers, June 2017, pages 3 and 4

³ New Zealand Law Society Cloud Computing Guidelines for Lawyers, June 2017, page 4

- (a) Private cloud: Exclusively used by a single organisation, such as a law firm, it can be owned, managed, and operated by the organisation or a third party, or a combination. It can be located on-site or off-site.
- (b) Community cloud: Specifically used by a community of users who have shared concerns, such as security or compliance requirements, it can be owned, managed, and operated by one or more organisations within the community, a third party, or a combination. It can be located on-site or off-site.
- (c) Public cloud: Available for use by the general public, it is owned, managed, and operated by a business, academic, or government organisation, or a combination. It is located on the premises of the provider.
- (d) Hybrid cloud: This is a combination of two or more different types of clouds (private, community, or public) that are connected using standard or proprietary technology. Each cloud remains separate but can share data and applications. For example, it can be used for load balancing between clouds.

PART B: UNDERSTANDING CLOUD SERVICES

(1) Potential Benefits

The key benefits of using cloud services, as opposed to internal on-site or offsite data storage facilities such as servers are:

- (a) Reduced infrastructure and technology staff costs resulting in better economies of scale;
- (b) Flexibility in subscription packages and storage capacity;
- (c) Better quality servers with better data handling capacity and security;
- (d) Reduced document management cost and not having to manage software / hardware update and upgrade issues;
- (e) Improved backup and disaster recovery services; and
- (f) Easy access to files and applications from any location and device as long as there is an Internet connection.

(2) Potential Risks

Despite its potential benefits, cloud services also presents risks that advocates and solicitors must consider, particularly since advocates and solicitors owe fiduciary duties to their clients including confidentiality, and the management of client personal data, amongst others.

This non-exhaustive list of risks includes examples of using cloud services by advocates and solicitors⁴:

- (a) Speed and space (bandwidth): for example, while you are subscribing for an annual fee, as your bandwidth needs increases, you may be locked-in to a single provider;

Example A:

Provider A offers different subscription plans with varying amounts of storage space and bandwidth. The basic plan provides 100GB of storage and 10Mbps of bandwidth, while the premium plan offers 1TB of storage and 100Mbps of bandwidth. As your business grows and

⁴ All examples cited in (2) are referenced from chat.openai.com accessed on 3 June 2023

needs more bandwidth, you can upgrade to a higher-tier plan within the same provider for a higher fee. You do not have to switch to a different service provider.

Example B:

Provider B offers an annual subscription that includes unlimited space and bandwidth. This means that no matter how much your bandwidth needs grow, you will not face any restrictions or additional costs. This provides flexibility and scalability for your legal practice without being limited by a specific bandwidth limit.

Example C:

Provider C offers a set storage space, for example, 500GB, but allows you to increase your bandwidth as required. They may charge additional fees for higher bandwidth levels, such as 10Mbps, 50Mbps, or 100Mbps. While your storage space stays the same, you have the flexibility to adjust your bandwidth to match your changing needs.

- (b) Lack of control over any customisation or integration;

Example A:

Some providers offer Application Programming Interfaces (“APIs”) that let you connect their services with your applications or systems. However, these APIs may have limitations on customisation options or lack support for specific features you need. This can restrict your ability to fully customise the integration or create custom solutions that meet your business requirements.

Example B:

Cloud services often have predefined storage structures, such as folders and file hierarchies. You may have limited control over modifying or customising these structures to align with your specific organisational requirements.

Example C:

Some providers may not provide options for extending or customising their functionality beyond what is offered out of the box. This can be problematic if you have unique business processes or specific requirements that necessitate customisations or integrations with other systems.

Example D:

When relying heavily on a specific provider, you may face challenges when trying to integrate or migrate your data to another service. Lack of standardisation and interoperability between different providers can result in vendor lock-in, making it difficult to switch to a different provider or integrate with other systems seamlessly.

Example E:

Cloud services typically provide their own security measures, such as encryption and access controls. While these measures ensure the safety of your data, you may have limited control over customising or implementing additional security protocols according to your specific requirements.

- (c) Risk of security and privacy breaches;

Example A:

Data breaches: *Providers store large amounts of data from many users, making them attractive targets for hackers. If a provider experiences a data breach, there could be unauthorised access to sensitive information stored in the cloud, such as confidential documents, client data, or intellectual property.*

Example B:

Inadequate security measures: Some providers may have weak security measures in place, leaving vulnerabilities that attackers can exploit. This could include poor encryption protocols, insufficient access controls, or inadequate security monitoring and response capabilities.

Example C:

Insider threats: Cloud services involve multiple parties, including provider employees who may access user data. Without proper safeguards, there is a risk of insider threats where an employee intentionally or accidentally compromises the security or privacy of the stored data.

Example D:

Insufficient privacy controls: Providers may have privacy policies that allow them to access or share user data for various purposes. In some cases, these policies may not align with the privacy requirements of advocates and solicitors, potentially exposing sensitive information to unwanted access or disclosure.

Example E:

Data loss or corruption: Although cloud services usually have backup measures, there is still a risk of data loss or corruption. Technical failures, natural disasters, or human errors can permanently delete or make data inaccessible.

Example F:

Compliance and regulatory risks: Depending on the type of data stored by advocates and solicitors, there may be compliance requirements and industry-specific regulations to meet. If the provider fails to comply or provide necessary assurances, it can result in regulatory violations and legal consequences.

- (d) Concerns about cross-border privacy legislation as servers may be located anywhere in the world and the advocate and solicitor must ensure that their cloud-based operations comply with the laws of such jurisdictions;

Example A:

Data protection laws: Different countries have different laws and regulations regarding data protection. When your data is stored in servers located in another country, it can be challenging to ensure compliance with the relevant regulations that govern the collection, storage, and processing of personal information or data in general.

Example B:

Jurisdictional conflicts: Legal disputes or investigations involving data stored in a different country can lead to conflicts regarding which country's laws apply. This can complicate legal proceedings and create uncertainties about the protection and privacy of your data.

Example C:

Government surveillance and access: Governments in different countries have varying surveillance laws and intelligence capabilities. Storing your data in a country with less strict privacy protections may expose your information to potential government access or surveillance without your knowledge or consent.

Example D:

Lack of control and oversight: When your data is stored in another country, you may have limited control and oversight over how it is handled, secured, or accessed. This would raise concerns about the level of protection for your data and your ability to enforce privacy measures.

Example E:

Data transfer restrictions: Some countries have restrictions on transferring personal data outside their borders. This can impact your ability to store or process certain types of data in specific locations, potentially limiting your options when choosing a cloud storage provider.

- (e) Reliability of the provider and access to customer service;

Example A:

Uptime and availability: A reliable provider ensures that your data is consistently available and accessible. They have strong infrastructure and backup systems in place to minimise any downtime and ensure that your data is always accessible when you need it.

Example B:

Performance and speed: A reliable provider offers fast and consistent performance for uploading, downloading, and accessing your files. They have optimised networks and efficient data transfer protocols, ensuring that you can store and retrieve your data quickly without any significant delays.

Example C:

Data durability and backup: A reliable provider safeguards the integrity of your data. They have backup systems, data replication, and error detection mechanisms in place to prevent data loss or corruption. This ensures that even in case of hardware failures or disasters, your data remains secure and accessible.

Example D:

Service level agreements (“SLAs”): A reliable provider offers clear and well-defined SLAs that outline the level of service they guarantee. This includes commitments regarding uptime, performance, data protection, and customer support response times. SLAs provide assurance and accountability for the reliability of the service.

Example E:

Responsive customer support: A reliable provider has a responsive and knowledgeable customer support team. They offer various channels of communication and provide timely assistance to questions, issues, or technical support needs. They address concerns promptly and offer reliable solutions to ensure a positive user experience.

Example F:

Proactive communication and updates: A reliable provider keeps customers informed about any maintenance activities, updates, or service disruptions that may impact data access. They have effective communication channels and provide regular updates on the status of their service to minimise any potential disruption to your operations.

- (f) How to assure your clients that the data is secure;

Example A:

Encryption: Advocates and solicitors can protect their data by using encryption. This converts the data into a secret code that can only be understood with a special key. Even if someone gets access to the data, they cannot read or use it without the key.

Example B:

Strong access controls: Advocates and solicitors should use strong measures to control who can access their data. This includes using strong passwords, adding extra layers of security like fingerprint or face recognition, and carefully managing who has access. Only trusted individuals

should be able to access the data, and their access should be regularly checked and removed if needed.

Example C:

Choose reputable providers: *Advocates and solicitors should select trustworthy providers with a strong reputation for keeping data safe, i.e., providers who have certifications, comply with data protection rules, and have clear security policies. Doing some research can help ensure that the provider is reliable and trustworthy.*

Example D:

Regular security audits: *Whenever possible, advocates and solicitors should regularly review the security of their cloud setup. This means checking the provider's security measures, looking at access records, and identifying any potential risks or weaknesses in the system.*

Example E:

Data backup and disaster recovery: *Advocates and solicitors should regularly backup their data and prepare for any emergencies to ensure that even if there's a problem or data loss, the information can be recovered and accessed again. Backup data should be kept separately to provide extra protection.*

Example F:

Transparent communication: *To build trust with clients, advocates and solicitors should openly communicate about data security including, possibly, sharing information about encryption, access controls, backup processes, and how they comply with privacy laws. Clients should know what steps are being taken to keep their data safe and should feel comfortable reaching out for support or any questions about security.*

(3) Best Practices

Advocates and solicitors currently using or intending to move their data to the cloud must do so with a clear understanding of their priorities. They should evaluate the risks in line with their fiduciary responsibilities to their clients and the Courts, as well as their business goals.

3.1 Data storage

- (a) To ensure client confidentiality, advocates and solicitors should:
 - (i) Categorise stored data as high or low risk;
 - (ii) Clearly define how data is stored;
 - (iii) Educate all law firm employees about these policies;
 - (iv) Prohibit employees from using personal cloud services for work-related data, especially high-risk information; and
 - (v) Inform employees who work remotely about the risks of data communication, management, and storage, and how it can threaten client confidentiality and data security.
- (b) Take reasonable steps to prevent crime or fraud within the law firm, such as regularly updating passwords and revoking access for former employees.
- (c) Take reasonable steps, especially before any employees leave the firm, to prevent unauthorised data deletion or modification of account access.

- (d) Keep backups of important documents outside the cloud to ensure access, in case of service disruptions or data loss.
- (e) If the provider's data centres are located outside the jurisdiction, inform clients in writing about this and relevant data protection laws. Include a clause in client appointment letters explaining that cloud services are used, and that the law firm will provide details of the provider, upon request.
- (f) Educate users of cloud services about best practices when accessing the service outside the law firm's premises.
- (g) Encrypt devices (laptops, tablets, mobile devices) used to access cloud storage. Additionally, consider encrypting sensitive files with an extra layer of security, ensuring only authorised users with the encryption key or password can access the data.
- (h) Maintain an updated inventory of authorised accounts and devices.

3.2 Cloud Service Contracts

- (a) Local and international providers offer different contracts for users;
- (b) Consider established providers for cost-effective and secure options. These providers offer fixed contract terms with added benefits such as better security and the ability to upgrade seamlessly;
- (c) While working with smaller and newer providers may be cheaper and offer flexibility and lower subscriptions, however, there may be risks regarding the quality of services and level of security they can provide;
- (d) When choosing a cloud service provider, reliability is crucial. Always:
 - (i) Check their track record and reputation, including client testimonials on contract duration, reliability, security, service standards, and hidden costs;
 - (ii) Consider their position in the cloud services market and prioritise your legal and fiduciary responsibilities as advocates and solicitors;
 - (iii) Confirm that the provider has appropriate security measures in place, such as accreditations and encryption technology meeting current international standards like ISO27001 and multi-factor authentication; and
 - (iv) Be prepared for various possibilities, including data loss, provider discontinuation, and other issues. Have a backup plan and ensure data stored in the cloud is backed up. Evaluate the provider's data retention and restoration methods as well.

3.3 Additional considerations:

- (a) Contracts for cloud services are governed by service level agreements (SLAs), which provide guarantees on the operational time of the service. Carefully review the SLA to understand:
 - (i) Their overall impact and ensure the terms are reasonable;
 - (ii) The provider's redundancy arrangements for continued operation in various situations;
 - (iii) Whether the provider backs up data and how frequently it is done;
 - (iv) If you can access backed-up data if you cannot access your cloud services; and

- (v) That the provider cannot delete any stored documents without your written consent.
- (b) Service charges are important. This includes subscription fees and whether the provider is obligated to inform you about:
 - (i) Structural changes to the business;
 - (ii) Termination clauses and associated penalties;
 - (iii) Handling of data in case of the provider's insolvency;
 - (iv) Contract changes and whether they require written notification, and whether you have the power to terminate the contract, if you disagree; and
 - (v) Whether suspension of services can happen without prior written notification, including for non-payment.
- (c) Providers often work with third-party vendors for hardware and software. The SLA should include clauses ensuring:
 - (i) Third-party vendors do not have access to your stored data;
 - (ii) Your prior written consent is required for any assignment or novation of rights and obligations;
 - (iii) Safeguards to ensure that third party vendors do not have access to your data; and
 - (iv) Notification requirements if your data has been damaged, lost or stolen, and avenues for privacy breach complaints.
- (d) Knowing the physical location of the provider's data centres is important as they must comply with privacy laws in that jurisdiction. If the provider cannot provide this information, you need binding contractual commitments to protect privacy.
- (e) Understand how the provider handles requests for stored data from national and international governments, regulatory bodies, agencies, and courts. Understand:
 - (i) How they validate the legality of requests and release processes, and if they notify you before sharing your data;
 - (ii) If there is a contractual obligation to obtain necessary consent from your client before sharing their data with third parties; and
 - (iii) The provider's jurisdiction, as it can impact client confidentiality and legal privilege.
- (f) Ensure the SLA explicitly prohibits the sale of your data to third parties.
- (g) Exit clauses are critical. Ensure that if you terminate the contract, you can retrieve your data in the format and timeframe you stored it. Confirm if the provider keeps any of your data after termination or securely deletes it, and how you can verify its deletion. If you decide to switch providers, understand the process of transferring your data.

(4) Cessation of Practice

Upon the dissolution of their firm, advocates and solicitors shall, forthwith, cause all access to any cloud services to be terminated and securely remove all data from such cloud services.

(5) Recommended Practices⁵

Usage of cloud computing services comes with inherent technological related risks thus its use should be coupled with cyber security measures. The following appendices provide recommended practices advocates and solicitors may adopt:

Appendix A: Technology by firm size

Appendix B: Organisational processes by firm size

Appendix C: Security controls by firm size

Appendix D: Awareness and training programme

Appendix E: Cybersecurity training

⁵ Cybersecurity Guidelines, International Bar Association's Presidential Task Force on Cyber Security, October 2018

APPENDIX A: Technology by firm size⁶

E – Expected; R – Recommended; O – Optional

#	Control Description / Firm Size (Number of lawyers)	Sole Proprietor (1)	Small (2-5)	Medium- sized (6-30)	Large (>30)
1	Keep system software updated	E	E	E	E
2	Implement endpoint protection	E	E	E	E
3	Use secure internet connections	R	R	E	E
4	Secure web browsing and email	E	E	E	E
5	Implement data retention, loss recovery capability	R	R	E	E
6	Encrypt data and devices	O	O	R	R
7	Enable remote erasure	O	O	E	E
8	Make sure cloud service provider is secure	O	O	E	E
9	Strictly manage access control	O	R	E	E
10	Create robust network segmentation	O	O	R	R
11	Implement audit logs	O	O	R	R
12	Consider application whitelisting / blacklisting	O	R	R	R
13	Secure mobile devices	E	E	E	E
14	Secure devices that retain data	O	R	E	E

⁶ Reference to firm size is as follows: (a) Sole proprietor: 1 lawyer (b) Small: 2 to 5 lawyers (c) Medium-sized: 6 to 30 lawyers (d) Large: more than 30 lawyers. Retrieved from the Malaysian Bar website on 27 February 2023.

APPENDIX B: Organisational processes by firm size

E – Expected; R – Recommended; O – Optional

#	Process Recommendation / Firm Size (Number of lawyers)	Sole Proprietor (1)	Small (2-5)	Medium-sized (6-30)	Large (>30)
1	Use strong usernames and passwords, and enable multi-factor authentication	O / R	R / E	E	E
2	Allocate roles and responsibilities clearly	O	R	R	E
3	Identify sensitive data and apply protection protocols	E	E	E	E
4	Regularly assess cybersecurity risks and test systems	O	O	R	E
5	Create a cybersecurity policy that matches the identified risks and sets minimum standards	O	R	R	E
6	Develop business continuity plans	R	R	R	R
7	Establish and test a comprehensive Incident Response Procedure (“IRP”)	R	R	R	E
8	Review legal and regulatory obligations	E	E	E	E
9	Manage risks associated with vendors and third-party service providers	R	R	R	R
10	Provide training and conduct testing for cybersecurity	O	O	E	E
11	Consider cyber liability or cybersecurity insurance	R	R	R	R
12	Participate in cybersecurity information sharing	R	R	R	R

APPENDIX C: Security controls by firm size

E – Expected; R – Recommended; O – Optional

#	Control Description / Firm Size (Number of lawyers)	Sole Proprietor (1)	Small (2-5)	Medium-sized (6-30)	Large (>30)
1	Keep track of authorised and unauthorised devices	O	R	R	E
2	Keep track of authorised and unauthorised software	O	R	R	E
3	Ensure secure settings for hardware and software on various devices	R	R	E	E
4	Regularly assess vulnerabilities and fix them	R	R	E	E
5	Limit and monitor the use of administrative privileges	R	R	E	E
6	Maintain and analyse audit logs	O	O	R	R
7	Implement protections for email and web browsing	E	E	E	E
8	Use defences against malware	E	E	E	E
9	Control network ports, protocols, and services	O	R	R	R
10	Have the ability to recover data	R	R	E	E
11	Configure network devices securely	R	E	E	E
12	Establish boundary defence measures	O	O	D	E
13	Protect data from unauthorised access	E	E	E	E
14	Grant access based on the need to know	A	R	E	E
15	Control remote and wireless access	R	E	E	E
16	Monitor and control user accounts	O	R	E	E
17	Assess security skills and provide appropriate training	R	R	R	R
18	Secure application software	O	O	O	R / O
19	Establish plans for incident response and management	O	O	A	E
20	Perform penetration tests and simulated attacks	O	O	E	E

APPENDIX D: Awareness and Training Protocols

E – Expected; R – Recommended; O – Optional

#	Description / Firm Size (Number of lawyers)	Sole Proprietor (1)	Small (2-5)	Medium-sized (6-30)	Large (>30)
1	Password management awareness	E	E	E	E
2	Multi-factor authentication on all business and personal accounts	E	E	E	E
3	Awareness of the dangers (both cyber and ethically) in the use of social media	E	E	E	E
4	Physical access control: only authorised personnel to have physical access and to limit server equipment access to IT staff only	E	E	E	E
5	Logical access control: Computer systems should operate to a standard of least privilege	R	R	R	R
6	Encrypt all portable devices such as hard drives, USB flash drives, memory cards, and optical media whenever possible. If encryption is not possible, use password-protected ZIP/RAR files as an alternative	E	E	E	E
7	Encourage employees to report suspicious computer activity, such as unexpected windows or applications opening, unusual mouse movement, and unsolicited emails	E	E	E	E
8	Employees should not click on links or open attachments in unsolicited emails. Instead of deleting the email, the organisation should provide a designated mailbox where suspicious emails can be forwarded without being opened to gather email intelligence and analyse why certain emails were not detected by security software	R	R	R	R
9	Employee awareness of when they will be legitimately prompted (after clicking a link) to enter their login credentials	R	R	R	R
11	Tips and reminders about confidential information and policies, such as information security; clean desk policy; Bring Your Own device (“BYOD”) device policy; remote working and removable media policy; document retention policy; Mobile Device Management (“MDM”) policy; privacy policy and social media policy	R	R	R	R
12	Policies should include protocols on the use of web-based email and storage systems (e.g., Dropbox, OneDrive, Gmail and Yahoo! Mail)	R	R	R	R

13	Mobile phones: employees who use their personal mobile devices for business purposes should ensure that: 1. the minimum password length is six (6) digits; 2. remote wiping capabilities should be turned on; 3. Apple iOS devices should be configured to wipe after ten (10) unsuccessful login attempts; 4. backups to computers should be encrypted; 5. memory cards (if applicable) should be encrypted; and 6. application and operating system updates should be applied as practicable	E	E	E	E
14	Contractors and third-party suppliers due diligence	E	E	E	E
15	Awareness raising of current threats and warning signs	R	R	R	R

APPENDIX E: Cybersecurity training

Cybersecurity: The protection of electronic systems to maintain the confidentiality, integrity and availability of data. While an external attacker is perceived as the greatest threat, you must consider that internal employees, contractors and third-party suppliers can intentionally, accidentally or negligently cause data loss and damage to systems.

Recommendation: All employees receive training in the following areas as well as any organisation-specific training that may be required.

Password management	Good password management should be reinforced as applicable to both business accounts and personal accounts (to reduce social engineering attacks). The general rules are: (a) Passwords should not be recorded on paper and attached to computer equipment; (b) Passwords should not be shared between users; (c) Strong and complex passwords should be used, comprising numbers, upper and lower-case letters, and special characters. Employees should be encouraged to use alphanumeric-and-symbols passwords such as "50%like2sleepunder@*"; (d) Personally identifiable information such as dates of birth, postcodes, children's or pets' names, should be avoided; (e) Password reuse across multiple systems or devices should be avoided. A password manager should only be used to remember the master password and the application generates and inputs the rest; (f) When a password is required to enrol in a system or make a one-time or rare purchase, consider using a random one-time series of characters and then using the password reset feature if subsequent access is required; and (g) Strongly encourage users to have separate passwords for business and private accounts.
Multi-factor authentication	Activate multi-factor authentication on all business and personal accounts. Inform employees that attackers target personal accounts to gather information and launch social engineering attacks by sending phishing emails to colleagues. Provide employees with step-by-step guides to enable multi-factor authentication on popular applications such as LinkedIn, Gmail, Yahoo!, Facebook, Instagram, and Apple iCloud.
Social media	Social media is a valuable information source for potential attackers. Employees should be aware of the associated social media risks in terms of cybersecurity and ethics. They should receive training on the potential dangers of sharing material, such as photographs, on social media accounts that could reveal the physical layout of a law firm.

Physical access control	Employees should receive training on the significance of allowing only authorised personnel into the law firm. Access to server equipment should be restricted to essential IT staff. Employees should be encouraged to question unfamiliar individuals. Employees must ensure the safekeeping of their access / security cards to prevent unauthorised access to the law firm. They should not share or exchange their security cards with other employees. Employees should surrender old devices with law firm data to the IT department for thorough wiping or physical destruction.
Logical access control	Employees should adhere to the principle of “least privilege” when it comes to computer systems i.e., they should only request access to systems and data that are necessary for their work. Encrypt all portable devices such as hard drives, USB flash drives, memory cards, and optical media. If encryption is not possible, using password protected ZIP / RAR files can serve as an alternative.
Suspicious activity	Employees must promptly report any suspicious activity on their computers, such as unexpected windows or applications appearing, mouse movements not controlled by them, and unsolicited emails. Employees should be informed about legitimate instances when they will be prompted to enter their login credentials after clicking on a link. Conducting regular active phishing campaigns is an educational exercise for employees.
Policy awareness	Employees awareness of the following policies (if applicable), the reason for their implementation, and the implications of not following them, are critical: (a) Appropriate use of IT systems; (b) BYOD policy; (c) Document retention policy; (d) Working from home policy; (e) MDM policy; (f) Privacy policy; and (g) Social media policy These policies should include protocols on the use of web-based email and storage systems (e.g., Dropbox, OneDrive, Gmail and Yahoo! Mail).
Mobile phones	Mobile phones: employees who use their personal mobile devices for business purposes should ensure that: (a) The minimum password length is six (6) digits; (b) Remote wiping capabilities should be turned on; (c) Apple iOS devices should be configured to wipe after ten (10) unsuccessful login attempts; (d) Backups to computers should be encrypted; (e) Memory cards (if applicable) should be encrypted; and (f) Application and operating system updates should be applied as practicable.

Contractors and third-party suppliers	Employees should be aware of the risk that poorly validated contractors and third-party suppliers may have access to the organisation. Employees who engage contractors and third parties should be encouraged to thoroughly review the security credentials of all external parties before allowing them access to IT systems and before sending organisational data to them. All contractors and third parties should be monitored if they are provided with access to the data holdings of the organisation. Unless absolutely essential, contractors and third-party suppliers should never be given administrative-level access to the network.
Continued training	Security awareness training should be delivered on a regular basis. Continued training and the development of a “cyber aware” culture is paramount to mitigating the ongoing cyberthreats.



WHAT ARE CLOUD SERVICES?

Cloud services are application and infrastructure resources that exist on the internet. Subscribers contract with third party providers for these services, allowing subscribers to leverage powerful computing resources without having to purchase or maintain hardware and software. These services enable remote data storage, management, and access.

HOW DO THEY WORK?

Users upload data

(files, documents, photos, videos, music, and more) to servers in global data centres, replacing local storage on individual computers.

ADVANTAGES OF CLOUD STORAGE

Access

The data can be accessed anywhere, anytime with an internet connection, on any device.

Scalability

Users can increase / decrease their storage capacity as needed.

Built-in security features

Data encryption and user authentication protect user data from unauthorised access.

WHO PROVIDES SUCH SERVICES?

There are a variety of global and local

cloud storage services available. These have free and paid storage plans with varying levels of storage capacity and additional features.

HOW DOES THIS ENHANCE THE PROVISION OF LEGAL SERVICES?

Documents are digitally accessible

anywhere with internet access.

Potential cost savings

Reduce need to physically exchange documents internally / externally.

Multiple back-ups, disaster recovery procedures and better security

IS IT SAFE TO USE SUCH SERVICES?

Providers use advanced security measures

to protect data. They have dedicated teams to respond to security threats and vulnerabilities. There are potential security risks, which will be discussed in the next publication issue.

