Inspector-General Practice Guideline 2

Guidelines relating to the security of record storage for practitioners

1. Introduction

This guideline has been issued as at 28 September 2020.

1.1 The purpose of this guideline is to provide general information for a practitioner to consider as part of their decision making about the storage of administration records. The requirements and expectations about the period of retention of administration records can be found in *IGPD 5 Trustees' guidelines relating to handling funds* and *IGPD 15 Debt agreement administrator guide to proper accounts.*

1.2 This guideline is relevant to trustees, controlling trustees and debt agreement administrators ('practitioners').

1.3 Increasingly, more practitioners are maintaining digital records of their administrations, whether they be on in-house computer servers, cloud-based systems or a combination of these. The nature of information stored digitally is private and sensitive, so it is essential practitioners ensure storage systems have adequate cybersecurity in place.

2. Storage of Records – Method of Storage & Security

2.1 The *Bankruptcy Act 1966* does not prescribe how records are to be maintained for either trustees or administrators– whether manually, digitally or a combination of these.

2.2 The benefits of digital record keeping compared to manual records include the following:

- Avoid having to pay high amounts for storage space (especially important given the approximate decade over which records must be kept in bankruptcy)
- Avoid having to shred records after mandatory retention period has expired
- Lower handling costs – allowing electronic workflow
- Greater accessibility and transportability
- Allow mobile workforce
- Assuming a copy of the records is backed up – less prone to loss, physical threats – fire, flood
- May facilitate keyword search location of documents

2.3 Disadvantages of digital record keeping include the following:

- Discipline required in digital record nomenclature to facilitate fast retrieval of particular documents
- Possibility of hardware or software crash leading to loss of information if backup not performed
- Potential for hackers particularly if software and virus protections are not updated
- Performing file reviews of digital records may not be as intuitive and easy as a well ordered manual file

3. Security of Physical (Manual) Records

3.1 Practitioners are expected to:

1. Lock Everything Down – Records should be secured in lockable cupboards
2. Install Fire and Security Alarms.
3. Limit Access to the records to those who require access
4. Label All Records, Files and Cupboards Appropriately.
5. Conduct Regular Audits
6. Destroy the Records Securely—and document when you do
7. Consider digitising records if practicable
8. If multiple staff need access to records – maintain a file register for signing out files
9. Ensure that the books of the regulated debtor are returned at the end of the retention period or earlier, with creditor approval (trustees only – administrators are not required to retain such records)
10. Maintain a schedule for destruction of records in accordance with legislation

3.2 Trustees have duties to administer the estate as efficiently as possible by avoiding unnecessary expense; and exercising powers and performing functions in a commercially sound way.[1]

3.3 If trustees are relying on paper-based systems and by doing so are administering the estate inefficiently, they may be in breach of their duties which may lead to regulatory scrutiny of, and reduction of their remuneration.

4. Digital Method of Storage

4.1 Digital methods of storage have included either local computer servers and or off-site remote servers (Cloud)

In-House Servers

4.2 Advantages of in-house servers including the following:

- Having physical control over your back up
- Being able to keep critical data and information in house with no 3rd party access available
- No requirement for an internet connection to access the data
- Can be more cost effective for some small and medium businesses

4.3 Disadvantages of in-house servers including the following:

- Sizeable capital investment required for infrastructure and hardware
- Dedicated IT support required with a dedicated space needed for the in house server
- Being more susceptible to data loss during disaster situations. This will be dependent on how often data is stored securely offsite.
- No recovery time or uptime guarantees
- Having your servers in-house may give you a sense of security, but it's unlikely your staff will possess the knowledge to keep threats at bay.

Security of in-house servers

4.4 *Physical security*

Physical security is always the number one priority for a server. No matter what methods, technologies or software you use, if you allow uncontrolled physical access to a server, you risk compromising the device. For a data centre, whether your own or a cloud service, physical security is usually built in to the operation. Only authorized people are allowed in the facility, and specific data halls or equipment cages may have additional levels of physical security, further limiting access to these critical servers.

Not every business can afford this level of security. But leaving a server sitting in an open office area risks unauthorized access. Simply keeping a departmental server locked in a closet can make a big difference. Running it headless, with no monitor or keyboard, provides an additional layer of security.

4.5 *Explicit levels of administrative access control*

Users with a requirement for administrative access, whether IT staff or business workers, should be assigned only those privileges necessary for them to accomplish their required tasks. Operating systems have granular levels of control so that administrative tasks can be assigned to specific users, without the need to grant overall administrative access rights. Web consoles for cloud services will also often offer graduated levels of administrative access, depending on the service. Remember that in almost all cases, less is more.

4.6 *Keep server and application software updated*

Unpatched servers are one of the biggest sources of malware infections on the Internet, so unless you are planning to keep a server disconnected from the outside world, you need to make sure that, at the very least, security patches are applied as they appear and are tested. For cloud-based servers and applications, you may need to regularly update client software running on your end to make certain that the latest security fixes have been applied.

Keeping up to date on these changes can also create staffing issues, especially at smaller practices where the IT department may consist of just a handful of people. One solution to this problem is to outsource these sorts of tasks to an outside vendor or partner, to allow your in-house staff to focus on mission-critical tasks.

4.7 *Maintain application security*

Many applications, especially those with web-based or collaborative components, have their own security models. Because the applications themselves may have elevated security privileges based on the needs of the application, allowing unsecured access to the applications and their resources can compromise the security of the hosting servers.

Specific applications, such as web servers, will have their own security processes that need to be followed. Proper installation and management of the applications will prevent the sort of user-introduced errors that can compromise server security.

4.8 *Turn off every function the server doesn't need*

Servers don't need web browsers, yet you often find them present. Disable them or, depending on the operating system, remove them completely. If you're running a Windows Server for file and print services, it needs very few other features installed. Do your homework, and disable any other feature unnecessary to the desired operation. Every extra feature that has remote access or availability provides another venue for attack.

Cloud Based Services

5.1 Cloud computing is the practice of using servers hosted on the internet to store, manage and process data, rather than a local server or a personal computer. The main insolvency accounting software providers Insol 6 and Core offer cloud services.

5.2 Advantages of Cloud based services include the following:

- No requirement for capital expenses or onsite hardware. This usually suits organisations that outgrow data storage quickly.
- Storage can be easily added when needed with most cloud solution providers charging you only what you need.
- Easy and efficient to backup and restore from anywhere, using any device including computers, tablets, or smartphones.
- Data losses can be minimised by having data backed up to the cloud as regularly as 15-minute intervals.
- Security - cloud service providers should have the expertise to ensure you're data is safe.

5.3 Disadvantages of cloud based services include the following:

- If your business isn't dependent on uptime and instant data recovery, the costs could outweigh the benefits.
- There is a limit to how much data can be stored in the cloud, which depends on cost and storage availability.
- You will have no access to any data or information if the Internet goes down at your business or at the cloud provider's side.
- If full data recovery is required, it can be time-consuming and impact heavily on your business.

Security of Cloud based services

5.4 The Australian Cyber Security Centre (ACSC) leads the Australian Government's efforts to improve cyber security.

5.5 ACSC recommends against outsourcing information technology services and functions outside of Australia, unless organisations are dealing with data that is all publicly available. The ACSC strongly encourages organisations to choose either a locally owned vendor or a foreign owned vendor that is located in Australia and stores, processes and manages sensitive data only within Australian borders. Note that foreign owned vendors operating in Australia may be subject to foreign laws such as a foreign government's lawful access to data held by the vendor.

5.6 The ACSC has published guidance about security considerations with cloud services:

https://www.cyber.gov.au/publications/cloud-computing-security-considerations

5.7 The guidance recommends some basic protections:

- The ACSC strongly encourages organisations to choose either a locally owned vendor or a foreign owned vendor that is located in Australia and stores, processes and manages sensitive data only within Australian borders.
- When entering into a contractual arrangement for outsourced information technology or cloud services, contractual ownership over an organisation's data is explicitly retained.
- Consider options for encrypting the data as well as a form of Multi-Factor Authentication when accessing the data source/repository.

5.8 **Additional Guidance – Cloud Computing - Privacy Considerations**

The Office of the Australian Information Commissioner publishes guidance with respect to securing personal information which includes the following information about security with cloud computing.

Cloud computing

Cloud computing can range from data storage to the use of software programs, with data being stored and processed by the cloud service provider. For instance, an entity can store data on remote servers operated by the cloud service provider rather than storing it on their own servers.

If you continue to 'hold' personal information when storing or using it in the cloud, reasonable steps may include robust management of the third party storing or handling your clients' personal information, including effective contractual clauses, verifying security claims of cloud service providers through inspections, and regular reporting and monitoring.

*If you choose to adopt cloud computing you need to assess the security controls of the provider to ensure that you continue to comply with APP 11.**[59]** However, other APPs may also apply in these circumstances, including APP 8 (where personal information is disclosed to an overseas recipient),**[60]** and APPs 12 and 13 (access and correction). These are discussed in more detail in the APP guidelines.*
*You should also be aware of your obligations under the Notifiable Data Breach scheme, and have measures in place to manage your relationship with the cloud provider to ensure all eligible or suspected data breaches are assessed and notified in accordance with those obligations.**[61]***

You should also consider whether your cloud service provider should be required to have similar controls to those you might apply to your own systems, such as governance arrangements and controls relating to software security, access security and network security set out in the sections above.

- *Does the contract require the cloud service provider to put in place reasonable security steps that enable you to comply with your obligations under the APPs?*
- *From a security controls perspective, do you understand what controls you are responsible for and what your cloud service provider is responsible for?*
- *Are you able to verify the security controls of the cloud service provider to a sufficient level of detail, such as through independent testing and validation?*
- *Will those contractual obligations be reasonably easy to enforce from a costs and practicality perspective?*

- *Are the cloud service provider's information handling practices certified against information security standards (such as the ISO 27000 group)?**[62]***
- *How will you manage the relationship to ensure that all suspected or eligible data breaches are communicated between entities and handled in accordance with the NDB scheme? For example, what contractual provisions and verification measures are in place? Does the cloud service provider have reasonable data breach response processes to facilitate the required response? In particular, are sufficient controls in place to properly investigate and respond to any suspected or actual breach to determine when and how it occurred, and what was taken?**[63]***
- *Does the cloud service provider enable secure transactions and encrypted storage?*
- *Have you considered encrypting the data yourself before transmission (rather than relying on the cloud service provider's encryption)?*
- *Have you considered who is able to decrypt data stored in the cloud?*
- *Does the cloud service provider intend to use your data for its own commercial purposes (separately or combined with other customers' data)? If so have you considered the security implications, including:*
    - *can you control the use of your data?*
    - *is the personal information de-identified before the provider uses it?*
    - *can you verify that the de-identified personal information cannot be re-identified?*
- *Does your cloud service provider subcontract to or use the resources of other parties to perform its services, and if so, how do they protect your data?*
- *Will your data be stored separately from the data of other customers of the cloud service provider; for example, on separate servers?*
- *Does the cloud service provider possess appropriate data recovery plans to deal with a natural disaster or system failure and prevent disclosure of your information?*
- *Is your data stored in a format you will be able to access or use if you need to retrieve it or amend it?*
- *Can the cloud service provider confirm whether it copies or otherwise replicates your information for its internal operational purposes (for example, if it moves your information between its IT assets), and what controls it has in place?*
- *Can the provider confirm that your information and any copies (including backups) have been destroyed at the conclusion of the contract? Can you retrieve the information?*
- *How easily can you contact a representative of the cloud service provider about privacy concerns or to liaise with in the event of a suspected or eligible data breach?*

Endnotes

[1] Section 19 of the Act