Australian Government
Department of Home Affairs

Tips on storing client information

Carefully manage portable storage devices

Risk: Easy to lose and prone to theft – a client's confidential information falls into the wrong hands

- Avoid use of portable devices where possible.
- Use password protection.
- Encrypt data on discs, USB flash drives, SD cards and the like.
- Lock portable devices away securely.

Make sure laptops are protected and secure

Risk: Easily damaged and prone to theft – a client's confidential information falls into the wrong hands

- Use a reliable antivirus program and a personal firewall and keep these regularly updated.
- Backup the information on your laptop as often as possible to a secure device or site.
- Don't store unnecessary confidential information on a laptop's hard drive.
- Never leave access numbers, passwords or security devices in your laptop case.
- Where possible, carry your laptop with you and always keep a close eye on it – pay careful attention when going through airport security and avoid leaving your laptop in a parked car.

Ensure hard copies of client information is kept secure

Risk: Easily copied, lost or stolen – a client's confidential information falls into the wrong hands

- Employ a 'clear desk' policy – hard copies containing a client's personal or sensitive details should be filed and locked away securely at the end of each day.
- Keep paper files in locked filing cabinets unless actively working on them.
- Make sure filing cabinets are locked at night or during the day if the office is unattended for an extended time.
- Use the secure print function when printing in an open office environment.
- File printed material promptly and lock client files away when not in use.
- Use a shredder rather than disposing of unwanted information in normal waste.
- Keep a register of significant documents held (such as passports and original client documents).

Data hosted by a third party

Risk: Easily compromised as control lost – a client's confidential information falls into the wrong hands

- Check the third party's ownership and whether owned or controlled by a foreign company.
- Find out where geographically the data will be stored.
- Find out who will have access and how access will be controlled.
- Find out what happens when data is compromised and whether you will be notified in a timely manner.
- Consider whether it is really cost-effective to have data stored offsite having regard to all the risks.