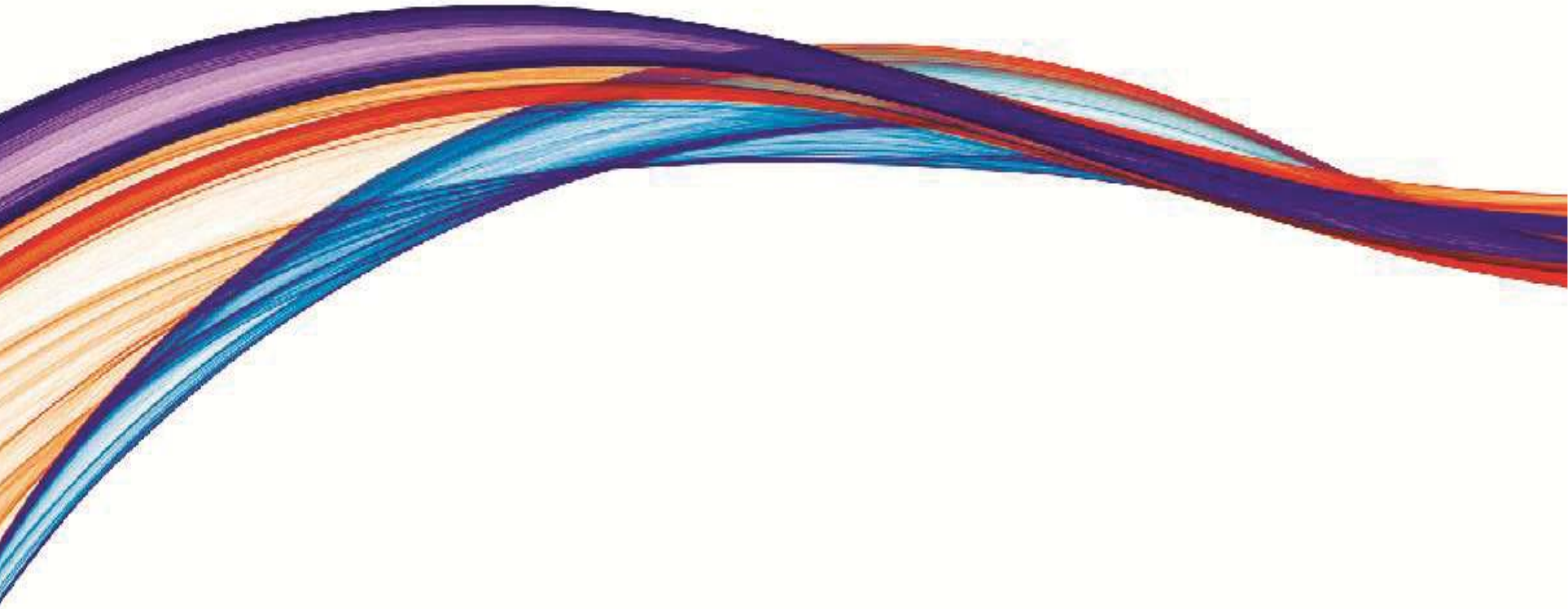
Australian Government

Office of the Australian Information Commissioner

Guide to information security

‘Reasonable steps’ to protect personal information

Consultation draft – December 2012



Contents

Key messages

- This guide provides guidance on information security, specifically the reasonable steps entities are required to take under the *Privacy Act 1988* (Cth) to protect the personal information they hold.
- This guide discusses some of the circumstances that the Office of the Australian Information Commissioner takes into account when assessing the reasonableness of the steps taken by entities to ensure information is kept secure. It also presents a range of steps and strategies that may be reasonable for an entity to take in order to secure personal information.
- What is reasonable may vary between entities and may also change over time. Therefore it is important that entities regularly review the relevance of security measures which protect personal information.
- In some circumstances the use of electronic and online records can increase the possibility of personal information being misused, lost or inappropriately accessed, modified or disclosed. It is critical that entities consider the steps and strategies required to protect and secure personal information they hold in order to meet the Privacy Act's requirements.
- Entities should build privacy into their processes, systems, products and initiatives at the design stage. This, and other preventative steps, assists entities to ensure that they have appropriate measures in place to minimise the security risks to personal information they hold.

Key terms

Agency has the meaning set out in s 6 of the Privacy Act and includes, amongst other things, a Minister, an Australian Government Department, an ACT Government Department, and a Norfolk Island agency.

Cth means Commonwealth

Data breach means, for the purpose of this guide, when personal information held by an entity is lost or subjected to unauthorised access, use, modification, disclosure, or other misuse.

Entity means an agency, organisation or other person covered by the Privacy Act, including the IPPs, NPPs, Part IIIA and the *Tax File Number Guidelines 2011*.

IPPs means the Information Privacy Principles set out in s 14 of the Privacy Act, which apply to agencies unless a listed exemption applies (see s 7 of the Privacy Act).

NPPs means the National Privacy Principles set out in Schedule 3 of the Privacy Act, which apply to organisations unless a listed exemption applies.

OAIC means the Office of the Australian Information Commissioner.

Organisation has the meaning set out in s 6C of the Privacy Act and, in general, includes all businesses and non-government organisations with an annual turnover of more than $3 million, all health service providers and a limited range of small businesses (see ss 6D and 6E of the Privacy Act).

Personal information has the meaning as set out in s 6 of the Privacy Act:

> ... personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Privacy Act means the *Privacy Act 1988* (Cth)

Sensitive information has the meaning as set out in s 6 of the Privacy Act:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

Background

The purpose of this guide

This guide provides guidance on the reasonable steps entities are required to take under the *Privacy Act 1988* (Cth) to protect the personal information they hold from misuse, loss and from unauthorised access, use, modification or disclosure.

This guide is aimed at helping entities meet their Privacy Act obligations by:

- outlining the circumstances that can affect the assessment of what steps are reasonable to take, and
- providing examples of steps and strategies which may be reasonable for an entity to take.

This guide highlights the importance of preventative measures as part of an entity's approach to information security. Such measures can assist in minimising the security risks to personal information.

Although this guide is not binding, the OAIC will refer to this guide when assessing an entities compliance with its information security obligations in the Privacy Act.

Who is this guide for?

This guide is intended for entities, including Australian, ACT and Norfolk Island Government agencies, and private sector organisations that are covered by the Privacy Act. It is also relevant to credit reporting agencies (CRAs), credit providers and tax file number (TFN) recipients.

What is this guide about?

The Privacy Act requires entities to take 'reasonable steps' to protect the personal information that they hold from misuse, loss and from unauthorised access, use, modification or disclosure. These obligations are set out in Information Privacy Principle (IPP) 4 for agencies[i] and National Privacy Principle (NPP) 4 for organisations (see Appendix A for IPP 4 and NPP 4).[ii] Additionally, s 18G(b) of the Privacy Act imposes equivalent requirements on CRAs and credit providers in relation to credit information files and credit reports. Also, Guideline 6.1(a) of the *Tax File Number Guidelines 2011* (TFN Guidelines), issued under s 17 of the Privacy Act, requires TFN recipients to take reasonable steps to safeguard TFN information.

When the Office of the Australian Information Commissioner (OAIC) investigates a possible breach of IPP/NPP 4, s 18G(b), or Guideline 6.1(a) of the TFN Guidelines, or conducts an own-motion investigation into an act or practice, including when information security has been breached, it considers two factors:

- the steps that the entity took to protect the information, and
- whether those steps were reasonable in the circumstances.

This guide discusses some of the circumstances that the OAIC takes into account when assessing the reasonableness of steps. It will then present a range of steps and strategies that may be reasonable for an entity to take. However, it is important that agencies and organisations regularly review the relevance of security measures which protect personal information.

Guide to handling personal information security breaches

The OAIC has also published a Data breach notification guide, which outlines steps that entities should consider in preparing for and responding to information security breaches, including notifying affected individuals.

Depending on the circumstances, reasonable steps to protect personal information may include the preparation and implementation of a data breach policy and response plan (that includes consideration of whether to notify affected individuals and the OAIC).

Further information

Additional resources on information security are widely available.

Australian Government agencies should also be aware of the *Australian Government Information Security Manual*, which governs the security of government ICT systems, and the *Australian Government Protective Security Policy Framework*, which aims to provide a common approach to the implementation of protective security across government.

The *National e-Authentication Framework*, developed by the Australian Government Information Management Office, assists Australian Government agencies and state jurisdictions in authenticating the identity of another party to a desired level of assurance or confidence.

Further information for private-sector organisations is available from Australia’s official national computer emergency response team CERT Australia.

Information security

Protecting personal information

Security is an important element of information privacy. Entities have security obligations under the Privacy Act, including in IPP 4 and NPP 4.

There are a variety of ways in which personal information may be misused, lost or inappropriately accessed, modified or disclosed. Common situations that an entity's information security measures should seek to guard against include:

- unauthorised access or misuse of records by a staff member
- failure to store records containing personal information appropriately or dispose of them securely
- loss or theft of hard copy documents, computer equipment or portable storage devices containing personal information
- mistaken release of records to someone other than the intended recipient
- hacking or other illegal access of databases by someone outside the entity.

The possibility of these types of incidents occurring may be increased due to greater collection of personal information in the online environment and the reliance on electronic and online records. This will mean that taking steps to protect against external attacks will become critical to meeting the Privacy Act's requirements. At the same time, entities will also need to guard against internal risks such as unauthorised access or misuse of personal information.

Privacy and your business

Good privacy practice is important for more than just ensuring compliance with the requirements of the Privacy Act. If an entity mishandles the personal information of its clients or customers, it can cause a loss of trust and considerable harm to the entity's reputation. Additionally, if personal information that is essential to an entity's activities is lost or altered, it can have a serious impact on the entity's capacity to perform its functions or activities.

It is important for entities to integrate privacy compliance into their risk management strategies. Robust information-handling policies, including a privacy policy and data-breach response plan, can assist an entity to embed good information handling practices and to respond effectively in the event that personal information is misused, lost or accessed, used, modified or disclosed without authorisation.

Many of the steps and strategies in this guide will also assist entities to ensure good handling of confidential information, such as commercially sensitive information, that is not protected by the Privacy Act but is nevertheless important to an entity's functions and activities.

Privacy by design and privacy impact assessments

Entities that handle personal information should build privacy into their processes, systems, products and initiatives at the design stage. Building privacy into data handling practices from the start, rather than 'bolting it on' at a later stage is known as 'privacy by design'. If agencies and organisations have appropriate security measures in place before they begin to handle personal information (either for the first time or in a new way), they will be better placed to meet their Privacy Act obligations. For example, entities should consider the security of personal information before they purchase, build or update information technology (IT) and electronic records management (ERM) systems.

One way in which privacy by design can be achieved is if entities undertake Privacy Impact Assessments (PIAs). A PIA is an assessment tool that examines the privacy impacts of a project and assists in identifying ways to minimise those impacts. A PIA will assist in identifying where there are privacy gaps, and where additional privacy protections may be required. Generally, a PIA should

- describe the personal information flows in a project
- analyse the possible privacy impacts of those flows
- assess the impact the project as a whole may have on the privacy of individuals
- explain how those impacts will be eliminated or minimised.

The OAIC expects entities to undertake a PIA for any new acts, practices or projects that involve the handling of personal information. A PIA, especially one conducted at the early stage of a project's development, can assist entities in identifying any information security risks and inform the reasonable steps that an entity needs to take to protect the personal information they hold.

A detailed guide to conducting PIAs is available from the OAIC website.

Circumstances that affect assessment of reasonable steps

What are reasonable steps to ensure information security under IPP 4 and NPP 4 will depend on the circumstances, including the following:

- the nature of the entity holding the personal information
- the nature of the personal information held
- the risk of harm to the individuals concerned if the information is not secured
- the data handling practices of the entity holding the information
- the ease with which a security measure can be implemented.

These circumstances (along with relevant examples from recent OAIC investigations) are discussed further below.

Nature of the entity

In determining the steps that it is reasonable for an entity to take to protect its holdings of personal information, the nature of the entity itself is relevant. Factors include the size of the entity and the business model on which the entity operates. For instance, if an entity operates through franchises or dealerships, or gives database and network access to contractors, the steps that it is reasonable for it to take may differ from the steps that it is reasonable for a centralised entity to take.

On 10 January 2011, the Privacy Commissioner opened an investigation into Vodafone Hutchison Australia following allegations that customer information had been compromised. Vodafone's business model uses licenced dealerships to sell its products and services. These dealerships were given remote access to Vodafone's databases of customer information via a store login ID. Customer identification information held on the database, such as the number and expiry date of passports, was visible to all Vodafone staff and dealership employees through the login shared across the store.

Appropriate authentication of users is an important network security measure and the use of store logins reduces the effectiveness of audit trails to assist in investigations and access control monitoring. The use of shared logins means that anomalies may not be detected and if they are, they may not be able to be effectively investigated as the actions are not linked to an individual authorised user. Limiting access to personal information is another important means of protecting it from inappropriate access, use or disclosure.

While Vodafone had a range of security safeguards in place to protect the personal information on its system at the time of the incident, the use of store logins and the wide availability of full identity information caused an inherent data security risk. For this reason, in the Privacy Commissioner's view, Vodafone had not taken reasonable steps to protect the personal information it held at the time of the incident and therefore it did not meet its obligations under NPP 4.1.

The full investigation report is available on the OAIC's website.

Nature of Personal Information held

The Privacy Act defines personal information as

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or an opinion.

The nature and quantity of personal information held by an entity will affect the steps that it is reasonable for that entity to take.

The Privacy Act defines sensitive information as

> (a) information or an opinion about an individual's:
>
> (i) racial or ethnic origin; or
>
> (ii) political opinions; or
>
> (iii) membership of a political association; or
>
> (iv) religious beliefs or affiliations; or
>
> (v) philosophical beliefs; or
>
> (vi) membership of a professional or trade association; or
>
> (vii) membership of a trade union; or
>
> (viii) sexual preferences or practices; or
>
> (ix) criminal record;
>
> that is also personal information; or
>
> (b) health information about an individual; or
>
> (c) genetic information about an individual that is not otherwise health information.

The community generally expects that their sensitive information will be given a higher level of protection than non-sensitive information. This expectation is reflected in the additional restrictions in the Privacy Act concerning the handling of sensitive information by organisations.

Although it is not classed as sensitive information in the Privacy Act, people also often expect that their financial information will be given a high level of protection. Generally, as the quantity, extent and sensitivity of personal information held increases, so too will the steps that it is reasonable for that entity to take to protect that information.

On 5 July 2010 the Privacy Commissioner opened an investigation of the Professional Services Review Agency (PSR), which holds Medicare Benefits Program (MBP) and Pharmaceutical Benefits Program (PBP) claims information. It was alleged that PSR was holding medical records in an unsecured manner. During the investigation PSR provided information about the different measures it has in place to keep information secure. In particular, the Commissioner noted that PSR:

- retains records in accordance with the National Archives of Australia guidelines, Normal Administrative Practice and existing Records Authorities
- destroys records in accordance with the timeframes set by the National Archives of Australia and mechanisms set by the PSM and ISM guidelines
- commissioned a review of its information and communication technologies in 2009 to ensure it was achieving best practice standards, and a Records Management Program was undertaken as a result of this review
- undertook a Protective Security Assessment of its practices and undertakes an annual Strategic Risk Assessment as part of its wider audit and compliance regime.

PSR has policy documents that set out how it manages data security including its Privacy Policy, Breach of Code of Conduct Policy and Clear Desk Policy. Some of the practical data security measures flowing from these policies include PSR's secure office environment, its ICT audit logs and tracking program. Based on the information that PSR provided, the Commissioner was satisfied that PSR's practices are consistent with its obligations under IPP 4.

The full investigation report is available on the OAIC’s website.

Risk of harm

When entities are assessing the steps that they take to protect personal information in their possession, they should consider the risk of harm to the individuals concerned if the information is not secured. For instance, individuals may suffer reputational harm if information becomes public, or material harm if the information exposed enables identity theft or fraud. The likelihood of this harm eventuating will influence whether it is reasonable to take a particular step.

On 20 July 2011, the Privacy Commissioner opened an investigation into Medvet Laboratories, following reports that customer information held by Medvet had been compromised. Medvet offers services such as parentage and illicit drug testing and has an online store, which entails handling customers' sensitive health information as well as credit card details.

Medvet was notified that certain client information from orders placed via Medvet's online Webstore could be accessed via a Google search. Medvet initially advised that up to 692 online orders had been made accessible and captured via a Google cache. The orders were primarily for parentage or illicit drug testing services or products. However, a subsequent independent investigation into the incident stated that 848 online orders were stored in Medvet's online Webstore. The investigation also showed that 29 of these orders had been accessed over a two month period. Medvet advised that no customer names, client bank account details or details of any test results were disclosed.

The independent investigation revealed that the online ordering software used by Medvet did not include appropriate security and the development and quality management practices associated with the Webstore application were deficient. The Commissioner considered whether Medvet had taken reasonable steps to protect the personal information that it held. In considering whether reasonable steps had been taken, the Commissioner considered Medvet's particular circumstances, including that the type of information it held included sensitive health information. The Commissioner concluded that Medvet did not have reasonable steps in place to protect the personal information it held at the time of the incident and therefore did not meet its obligations under NPP 4.1.

The full investigation report is available on the OAIC's website.

Data handling practices

When determining the appropriate steps to protect personal information, entities should consider the ways in which they handle data. This may include considering how personal information is collected, processed and stored. An entity should also consider whether it outsources any of its data handling. If an entity outsources data handling to a third party, it will need to consider how the third party handles and secures the information. Relevant factors include whether those suppliers are subject to the Privacy Act.

Appropriate steps should be taken to ensure third parties meet the entity's Privacy Act obligations. Appropriate steps may include having specific obligations about the handling of personal information in contracts or conducting inspections of the third party's facilities. Similarly, it may be reasonable for entities that store personal information remotely, such as with cloud computing services that may be located overseas, to take different steps from or additional steps to, an entity that stores information in its own facilities.

Section 95B of the Privacy Act requires agencies to take contractual measures to ensure that a contractor does not do an act, or engage in a practice, that would breach an IPP. In particular, the agency must ensure that the contract does not authorise a contractor to do or engage in such an act or practice. An agency must also ensure the contract contains provisions to ensure that such an act or practice is not authorised by a subcontract.

In July 2011, the Privacy Commissioner published a report on his investigation of Telstra after a mailing list error had resulted in approximately 60,300 letters with incorrect addresses being mailed out. The letters had been sent on Telstra's behalf by a mailing house to contact customers about Telstra's fixed-line phone service. In response to the questions raised by the OAIC, Telstra advised that it had a range of security measures in place to protect customer personal information involved in mail campaigns. These include:

- having an agreement with the mail house which includes privacy and confidentiality obligations
- conducting privacy impact assessments at the outset of mail out initiatives which use personal information
- a series of approvals before a mail out process can begin
- procedures to ensure staff handle personal information appropriately during the mail campaign process, including quality control procedures for creating mailing lists.

In this case, despite these measures being in place, an employee inadvertently used the wrong data table, which resulted in inaccurate address information being recorded on a campaign mailing list.

The Privacy Commissioner concluded that Telstra was not in breach of NPP 4 as he was satisfied that this incident occurred due to human error rather than any systemic failure of Telstra's processes or procedures.

The full investigation report is available on the OAIC's website.

Ease of implementation and proportionality

The ease with which a security measure can be implemented will influence the reasonableness of taking that step. It may not be reasonable to implement a measure if doing so will be impracticable or unduly expensive when balanced against the risks.

Additionally, it may not be reasonable to implement a measure if doing so might result in privacy infringements. For example, requiring users to supply extensive personal information to identify themselves prior to accessing their records may result in the entity collecting personal information which it would not otherwise require.

In deciding whether these costs make a step unreasonable, an entity should have regard to other circumstances such as the sensitivity of the personal information and risk of harm if that information is lost, altered, or inappropriately accessed, used, or disclosed. Similarly, entities must balance the taking of steps to prevent disclosure of personal information to someone other than the individual concerned with the right of individuals to access their own personal information.

In 2009, the Privacy Commissioner investigated a private medical centre following reports that a number of medical documents, including patients' prescriptions and pathology results, were found scattered in a public park adjacent to the centre. The name of the centre was visible on some of the documents as were patients' names, addresses and phone numbers. The medical centre informed the Commissioner that a lock on a medical waste bin, kept outside at the rear of the centre, had been tampered with and the contents of the bin thrown around an adjacent public park.

Having regard to the sensitivity of the information held by the medical centre, the Commissioner and the centre devised a number of steps that the centre could take to ensure that information was kept securely:

- The medical centre sought council approval to have secure fencing installed around the premises to reduce the risk of break-ins and vandalism
- It moved the secure medical waste bin inside the secured premises so that it could not be tampered with
- The bin was fitted with a new secure lock to which the medical centre manager held the key.

The medical centre developed policies and procedures for the secure destruction of personal information and trained medical and administrative staff in the proper destruction of both medical waste and medical documents.

The medical centre instructed its staff that medical documentation was not to be left with general medical waste for collection.

The centre obtained a shredder so that medical documents that were no longer needed could be securely destroyed on-site.

The Commissioner determined that, following the implementation of these measures, the medical centre met its obligations under NPP 4 and closed her investigation.

The full investigation report is available on the OAIC website.

Steps and strategies which may be reasonable to take

Appropriate security safeguards and measures for personal information need to be considered by entities across a range of areas. This could include taking steps and implementing strategies to manage the following issues:

- IT security
- data breaches
- physical security
- personnel security
- the information life cycle
- workplace policies
- communications security
- standards

This section outlines examples of key steps and strategies an entity could take in order to protect personal information and satisfy the security obligations in the Privacy Act.

The steps and strategies vary in ease of implementation and the impact that they will have on users. What is reasonable in the circumstances may vary between entities. What is reasonable may also change over time, for example, after a privacy breach occurs, if an entity becomes aware that security measures which previously protected data are no longer adequate or the entity handles data in a new way.

Although it is not necessary for all entities to take all the steps and strategies outlined below, the OAIC will refer to this guide when assessing an entities compliance with its security obligations in the Privacy Act.

IT security

Effective IT security requires protecting both computer hardware (the physical devices that make up a computer system) and the data that the computer hardware holds from unauthorised use, access, theft or damage. However, IT security measures should also ensure that the hardware and the data stored on it remain accessible and useful to legitimate users.

Entities are expected to consider IT security measures and the protection of personal information as part of their decision to use, purchase, build or upgrade IT systems rather than attempting to address privacy later, for example after a privacy breach has occurred.

There is an expectation that entities which provide online customer services or engage in electronic commerce, such as online retail businesses, will utilise IT security measures to ensure that their website is secure and that it provides a safe environment for individuals to make payments or provide their banking and personal information.

IT security measures help entities to protect themselves against attacks by malicious hackers and the damage caused by malicious software (or malware), computer viruses and other harmful programs. These programs can be used to gain unauthorised access to computer systems in order to disrupt or disable their operation and steal any personal information stored on those systems.

IT security measures can also guard against unauthorised use or disclosure of personal information stored on a computer system, while the system is being legitimately used. Such unauthorised use or disclosure can occur as a result of:

- human error (for example, the misplacing of hardware components and peripherals such as laptops and data storage devices)
- hardware or software malfunctions
- power failure
- natural disasters such as earthquakes, floods, and extreme weather conditions.

Whitelisting

Whitelisting describes listing entities, content or applications that are allowed to run on a computer or network. This allows only designated applications to run on a device. This can prevent malware from running. Whitelisting may offer greater protection than blacklisting (blocking material that is known to be harmful) as it is not dependent on identifying the material to be blocked. However a drawback is that it can also block harmless content that is not on the list.

- Is whitelisting of applications employed?
- Is whitelisted filtering of email content employed?
- Is whitelisting of web domains and IP addresses employed?

Software security

- Are the latest versions of software and applications in use?
    - What processes are in place to ensure that patches (software that is used to correct a problem with a software program or a computer system) and security updates to applications and operating systems are installed as they become available?
- Is the anti-virus software up to date?
- Has the operating system been fully patched?

Removing or disabling unneeded software, operating system components and functionality from a system reduces its vulnerability to attack. Disabling functions such as AutoPlay or remote desktop, if they are not required, can make it harder for malware to run or an attacker to gain access.

- Are operating system functions that are not required disabled?

There is a risk that content delivered though websites can be used to arbitrarily access system users' files or deliver malicious code. This risk can be reduced by ensuring that software applications and web browser 'add-ons' or 'plug-ins' (software that adds specific functions to browsers) are up to date. Disabling unused applications may also assist in preventing unauthorised access to a computer system.

- Are applications configured for maximum security at workstation level?

Entities importing data to a system should ensure that the data is scanned for malicious content.

- Are computer files checked for abnormalities at workstation level?

Access

There are three forms of authentication – something one knows (eg passphrases), something one has (eg a security token) and something one is (eg biometric information). Multi-factor authentication requires at least two forms of authentication.

- Is multi-factor authentication employed, especially when users are about to perform privileged actions or access sensitive/restricted personal information?
- Is the number of users with administrative privileges limited to the number necessary to enable the entity to carry out its functions and activities?
    - Is access revoked promptly when no longer required?
- Are strong passphrases enforced?
    - Are there mechanisms for changing them regularly?
    - Is reuse of passphrases blocked?
    - Are staff trained in the importance of strong passphrases and how to choose them? Is password complexity enforced? For example uppercase, lowercase, special character, numeric.
    - Is sharing of passphrases permitted?

Controlling bulk data transfers or downloads may help to prevent the theft of large amounts of data and identify inappropriate access of personal information.

- Are there controls on downloading or transferring data, especially bulk data? Are there policies in place to prevent the theft of bulk data through the use of personal storage devices?
- What means exist to identify inappropriate access of files or databases?
- Is there an audit trail of access to databases?
    - Does this audit trail indicate when an individual has accessed or viewed material, as well as when an individual has changed material?
    - Does the audit trail enable actions to be linked to individuals?
    - How often are checks/audits undertaken?

  - What procedures exist to address any issues, such as anomalous patterns of access, identified during audit?

- Are screensaver programs activated when computers are not in use? Do the screensavers properly blank out computer screens or fill them with moving images or patterns so that no personal information can be displayed when computers are not in use?
- Do computers automatically lock if left inactive or unattended for periods of time?
- Are users advised to lock their computers when they leave their desks, even for short periods?

Encryption

- Does the entity employ encryption of:
  - Portable devices?
  - Email communications?
  - Communication between internal information systems?
  - Hard drives?
  - Information stored over a network, such as the Internet or an entity's internal network, which has servers at a remote location (ie cloud computing)?
- Does the entity use a securely encrypted webpage for individuals who carry out transactions with the entity's website, such as making payments or providing their personal information?

Encryption methods should be reviewed regularly to ensure they continue to be relevant.

Network security

Filtering of web traffic provides an opportunity to prevent harmful content from reaching user systems.

- Is both incoming and outgoing web traffic filtered?
- Are downloaded files quarantined from the network until it is established that they are safe (e.g. opened in a segregated testing environment such as a sandbox)?

Intrusion detection strategies, which for example may involve using software applications that monitor network or system activities for malicious activities, anomalous behaviour, or policy violations, can be an effective way of identifying and responding to known attack profiles. Entities will need to ensure that such strategies are configured correctly, kept current and supported by appropriate security policies and processes.

- Does the entity maintain an intrusion detection strategy that includes intrusion detection mechanisms and analysis of event logs?

Spoofed email is email in which parts of the email header are altered so that it appears to have come from a different source. Spammers may use this technique to try to bypass filters and make it appear as though email comes from a legitimate source. Such emails may ask the recipient to provide their own or other individuals' personal information.

- Is spoofed email blocked?
- Does the entity employ email validation and authentication systems such as the Sender Policy Framework (SPF) and DomainKeys?

Firewalls are intended to prevent unauthorised network access. There are different types of firewalls and ways of setting them up which will affect the level of protection offered.

- What sorts of firewalls are employed and how are they configured?

Separating an entity's network into multiple functional segments makes it difficult for an intruder to propagate inside the network. Proper network segmentation assists in the creation and maintenance of network access control lists. Segmentation can also allow for different security measures to be applied to different types of information depending on its sensitivity and the risks associated with it.

- Is the network segmented and segregated into security zones?
- Are different security measures applied to different security zones, depending on the type of information in that zone and the risks associated with it?

Testing

Testing of IT security systems and processes may take a number of forms. Penetration testing uses approaches such as scanning networks to discover security weaknesses. Intrusion detection is used to identify unauthorised activity on a network and violation analysis involves examining logs to discover unusual or inappropriate activity. Testing may be conducted internally or contracted out.

- Is testing of security systems and processes undertaken?
    - How often is testing conducted?
    - Who is responsible for conducting testing?
    - If testing identifies weaknesses, how is this reported and addressed?

Data breaches

In the event of a data breach, having a response plan that includes procedures and clear lines of authority can assist entities to contain the breach and manage their responses. Ensuring that staff are aware of the plan and understand the importance of reporting breaches is essential for the plan to be effective. The OAIC has published a guide to handling personal information security breaches, the data breach notification guide, which is available from its website.

- Is there a data breach response plan?
- Does the plan include a strategy to assess and contain breaches?

- Does the plan clearly identify those actions that are legislative or contractual requirements?
- Are staff educated about the plan and how to respond to data breaches?
- Does the plan enable staff to identify data breaches and require that breaches be reported?
- Does the plan establish clear lines of command and indicate responsible officers?
- Does the plan outline clearly when affected individuals should be notified of breaches?
- Does the plan include a strategy to identify and address any weaknesses in data handling/data security that contributed to the breach?

Physical security

Physical security is an important part of ensuring that personal information is not inappropriately accessed. Entities are to consider what steps, if any, are necessary to ensure that physical copies of personal information are secure. Similarly, they should consider whether the workspace itself is designed to facilitate good privacy practices.

- What measures are used to control access to the workplace?
    - Are security and alarm systems used to control entry to the workplace?
    - Is it possible to identify staff movements from access logs?
- Has privacy and security been considered when designing the workspace?
    - Are workstations positioned so that computer screens cannot be easily read by third parties?
- Do visitors have access to general workspaces or are there designated areas for them?
- Are employees working on sensitive matters able to do so in a private/secure space?
- Is there a clean desk policy?
    - Is it enforced?
    - How often is it monitored?
- Do employees have access to secure storage spaces near their workstations to secure documents temporarily?
- What provisions are made for securing physical files containing personal information?
    - How is the movement of physical files recorded?
    - Is storage and movement of files containing personal information audited or monitored?
    - On what basis is access to physical files granted?

  - If files are placed in lockable cabinets or similar, are these storage units kept locked? How is access to keys controlled?

Personnel Security

Human error can cause data breaches and undermine otherwise robust security practices. It is therefore important that all staff members understand the importance of good information handling and security practices. Additionally, privacy training may help staff to avoid practices that would breach the entity's privacy obligations by ensuring that they understand their responsibilities.

- Are staff required to maintain a security clearance?
- What training is provided to staff regarding physical, IT and communications security?
  - When is training provided to new starters?
  - Is training also provided to short term staff and contractors?
  - Is refresher training provided to staff? Does this occur on a regular basis?
  - How are staff informed of changes to policy and procedures or other workplace security requirements?
- Does staff training cover information security and appropriate handling of personal information?
  - Does training emphasise to staff the importance of not accessing personal information or databases unnecessarily?
  - Does training make it clear to staff what would constitute misuse of personal information?
  - Does training cover recognising and avoiding 'phishing' and 'spear phishing' attacks and social engineering?

'Social engineering' is a term used to describe manipulating individuals into revealing confidential information or performing actions such as granting access to systems. 'Phishing' typically involves sending an email that appears to come from a legitimate organisation and attempts to trick the recipient into supplying confidential information. 'Spear phishing' is a personalised attack utilising personal identifiers to attempt to appear legitimate to a particular user.

- Does training address the need to avoid weak passphrases and passphrase reuse?

Passphrases are sequences of words or other text used to control access. They are similar to passwords but are often longer and more complex, which is intended to increase their effectiveness as a security measure.

- Does training address matters covered in workplace privacy and security policies (see below) and familiarise staff with those policies?
- Are staff reminded on a regular basis of their obligations to handle personal information appropriately? For example, are there signs in the workplace or alerts

on computer systems? Do computer logon screens outline staff privacy and security responsibilities?

- How do employee exit procedures ensure that physical and network access is cancelled and personal information in the employee's possession (eg in files) is returned?
    - At what time is physical and IT access revoked?

Workplace policies

Privacy protections have the best chance of being effective if they are integrated into workplace policies. Policies should be regularly monitored and reviewed to ensure that they are effective.

Information security, including appropriate handling of personal information, may be addressed in a single policy document or in a number of separate documents. Policies could cover a number of issues including physical security, IT security, and communication security. Additionally, entities should ensure that staff are trained regarding their responsibilities under these policies.

- Are there documented policies that address security matters, such as physical, IT and communications security and other appropriate information handling practices?
    - Are all staff, including short term staff and contractors, able to access the policy easily?
    - Are mechanisms in place for ensuring that the policy updated and reviewed? For example, are regular reviews scheduled? Do designated staff members have responsibility for maintaining the policy?
    - Are mechanisms in place to enable staff members to seek clarification of the policy or suggest updates?
    - Are staff reminded to refer to the policy and informed of updates as they occur?
    - How does the entity ensure that the policy is being observed? For example, does the policy require that regular security reviews or audits are conducted?
    - What steps does the entity take if it becomes evident that staff members are not observing elements of the policy?
- Is there a conflict of interest policy in place that instructs staff members on how to proceed if they handle personal information relating to a person known to them?
- Are there clear polices governing the use of portable/mobile devices, use of staff's own devices (known as bring your own device (BYOD)), and procedures for taking work home?
    - Are there minimum standards for security of portable devices (eg password protection, encryption)?

    - Are staff members educated about the risks of accessing or handling the entity's data on unauthorised/insecure devices?
    - If it is necessary to take personal information off the entity's premises, what steps does the entity take to ensure the security of personal information that is removed?
    - Is confidential business information segregated from personal user information?
- Is there a policy that covers information security when staff members work offsite, such as from home, a secondary site office or a temporary office?
    - Is there an offsite work agreement that addresses data security, including the storage and security of personal information?
    - What standards of physical security are applied to those workspaces, for example, the appropriate storage of physical files?
    - If employees are given remote access to work IT systems, what measures are in place to secure this access?
    - Who has overall responsibility for the security of personal information at those workspaces?

Managing the information life-cycle

Entities that handle personal information as part of their functions and activities need to take reasonable steps to ensure that that information is not inappropriately used or disclosed during its lifecycle. This includes ensuring that personal information is not mistakenly disclosed to the incorrect individual, that information is not lost and that it is disposed of appropriately when it is no longer required.

Additionally, entities that pass personal information to a third party for storage, processing, or destruction should consider what steps are required to ensure that the third party will protect that information.

- Are privacy impact assessments (PIAs) (see 'Privacy by design' above) conducted for new acts or practices, or changes in existing acts or practices that involve the handling of personal information?
    - Are new acts or practices assessed at an early stage to identify whether they raise any privacy issues?
    - Are mitigation strategies recommended by any PIA implemented?
    - Are those strategies reviewed after a period following implementation to assess whether they are effective?
- Does the entity review its collection practices at appropriate intervals to ensure that unnecessary personal information is not collected or retained?
- What processes does the entity have in place to assess requests from individuals to access or correct their personal information?

    - How does the entity verify the identity of an individual prior to giving access to their personal information?
    - How does the entity ensure that the personal information of other individuals is not improperly disclosed when providing this access?
    - Has the entity considered whether the steps required prior to granting access to an individual's personal information are proportionate to the amount and sensitivity of the information concerned to ensure that these steps do not unduly impede the individual's right to access their personal information?

Along with the right to apply for access under the Privacy Act, individuals have enforceable rights under the *Freedom of Information Act 1982* (Cth) (the FOI Act) to request access to their personal information held by Australian Government agencies. Individuals also have rights under the FOI Act to have their personal information amended if it is out of date, misleading, incorrect or inaccurate.

- What processes does the entity use to identify customers/clients prior to disclosing personal information by phone or in person?
    - What measures does the entity take to ensure that these verification processes do not infringe customer/ client privacy?
- What processes does the entity use to ensure mail containing personal information is sent to the intended recipient?
- What measures does an entity have in place to protect personal information during a system upgrade?
- What measures does the entity take to prevent data loss?
    - Does the entity have a data contingency plan that incorporates system back-ups? How is the system backed up, and how often?
    - Does the entity have a data contingency plan that incorporates disaster recovery?
- Is processing, storage or other handling of personal information out-sourced to a third party? If so, what measures has the entity taken to protect personal information when it is passed to a third party?
- What steps does the entity take to ensure that contractors and third parties that handle personal information on its behalf do not breach information security requirements?
    - Do contracts place explicit obligations on contractors in relation to their handling of personal information? Are security requirements, such as storing and processing personal information explicitly addressed?
    - Is compliance with contractual provisions regarding the handling of personal information reviewed or audited?
    - What procedures are in place for ensuring that all personal information is either returned to the entity or destroyed at the end of the contract?

    - Do invitations to tender require applicants to outline how they will address information security?

- Is there a policy outlining when and how to dispose of personal information when it is no longer required?
    - What steps does the entity take to securely dispose of personal information when it is no longer required?
    - Are staff informed of document destruction procedures?
    - Is destruction of personal information done in-house or outsourced? If outsourced, what steps has the entity taken to ensure appropriate handling of the personal information (see above)?
    - How is compliance with data destruction procedures monitored and enforced?
    - How does the entity ensure that data has been permanently deleted from electronic devices prior to disposal?

Communications security

Personal information can be vulnerable to being improperly accessed or disclosed when it is transmitted. For example, personal information may be disclosed if it is left on a fax machine or printer or discussed over the telephone in an open office.

- Are staff made aware of the risks of disclosure if they discuss customers' or clients' personal information over the telephone?
- Are there procedures governing the transmission of personal information via fax or email?
- Are there procedures governing the transmission of personal information to offsite work locations?
- Does the entity employ encryption when communicating sensitive personal information?

Standards

Standards Australia states that standards are documents that set out specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform the way they are intended to. Standards may be general or specific to particular industries or practices, such as electronic funds transfers. Compliance with standards can be tested internally or certified by a third party. Adopting a standard is one way that entities can gain some confidence regarding their security practices. However, a standard does not absolve the entity of taking further steps to protect its holdings of personal information.

- What standards, if any, does the entity comply with?
- How does the entity determine which standards to adopt?

    - If the entity determines not to adopt a standard, are the reasons for this decision clearly documented?
- How does the entity ensure that the standards employed are the most current and appropriate?
- Is internal auditing undertaken to ensure compliance with the standard?
- Is external auditing/certification undertaken to ensure compliance with the standard?
- If auditing reveals areas of weakness or non-compliance, how is this reported and addressed?

Appendix A – Information security obligations in the Privacy Act

Privacy Principles

Information Privacy Principle 4 – Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

a. that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

b. that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonable within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

National Privacy Principle 4 – Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

Part IIIA – Credit Reporting

Section 18G – Accuracy and security of credit information files and credit reports

A credit reporting agency in possession or control of a credit information file, or a credit provider or credit reporting agency in possession or control of a credit report, must:

(a) take reasonable steps to ensure that personal information contained in the file or report is accurate, up-to-date, complete and not misleading; and

(b) ensure that the file or report is protected, by such security safeguards as are reasonable in the circumstances, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(c) if it is necessary for the file or report to be given to a person in connection with the provision of a service to the credit reporting agency or credit provider, ensure that everything reasonably within the power of the credit reporting agency or credit provider is done to prevent unauthorised use or disclosure of personal information contained in the file or report.

Tax File Number Guidelines 2011

Guideline 6 – Storage, security and destruction of TFN information

6.1 ***TFN recipients*** must take reasonable steps to:

(a) protect ***TFN information*** from misuse and loss, and from unauthorised access, use, modification or disclosure, and

(b) ensure that access to records containing ***TFN information*** is restricted to individuals who need to handle that information for ***taxation law***, ***personal assistance law*** or ***superannuation law*** purposes.

6.2 A ***TFN recipient*** must take reasonable steps to securely destroy or permanently de-identify ***TFN information*** where it is no longer:

(a) required by law to be retained, or

(b) necessary for a purpose under ***taxation law***, ***personal assistance law*** or ***superannuation law*** (including the administration of such law).

[i] The IPPs are set out in section 14 of the Privacy Act and apply to Australian, ACT and Norfolk Island government agencies.

[ii] The NPPs are set out in Schedule 3 of the Privacy Act and apply to large businesses (with an annual turnover greater than $3 million), all health service providers and some small businesses and non-government organisations.