Practicality of implementation

The practicality of implementing a security measure, including the time and cost involved, will influence the reasonableness of taking that step.

However, you are not excused from taking specific steps to protect information just because it would be inconvenient, time-consuming or costly to do so. Whether these factors make it unreasonable to take particular steps depends on whether the burden is excessive in the specific circumstances.

In deciding whether these factors make a step unreasonable, you should have regard to other circumstances such as the sensitivity of the personal information and the risk to an individual if that information is misused, interfered with, lost, or inappropriately accessed, modified, or disclosed.

Example 5:

An investigation into a medical centre found that there were boxes of unsecured medical records being stored in a garden shed at a site no longer occupied by the medical centre.

The medical centre advised the Commissioner that patient health records were transferred from the locked room inside the former premises to a garden shed at the back of the site (so that renovations for sale of the site could occur). The garden shed door was locked with padlocks.

The Commissioner found that the medical centre did not take reasonable steps to protect the personal information, some of which was also sensitive information. Further, the Commissioner did not consider there to be any circumstances in which it would be reasonable to store health records, or any sensitive information, in a temporary structure such as a garden shed.

Read the full investigation report for Example 5

Privacy invasiveness

It may not be reasonable to implement a security measure if it is itself privacy invasive. For example, requiring users to supply extensive personal information to identify themselves prior to giving access to their records under APP 12 may result in collecting personal information that is unnecessary (contrary to APP 3).[28]

In that instance, you will need to balance what you need to do to prevent disclosure of personal information to the wrong person with the need to ensure that access is given on request.

[28] APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.

Part B — Steps and strategies which may be reasonable to take

Appropriate security measures for protecting personal information need to be considered in regards to all of your entity's acts and practices. This section outlines examples of key steps and strategies you should consider under the nine broad topics listed below. It includes a number of questions to ask yourself when considering or implementing these steps and strategies.

- Governance, culture and training.
- Internal practices, procedures and systems.
- ICT security.
- Access security.
- Third party providers (including cloud computing).
- Data breaches.
- Physical security.
- Destruction and de-identification.
- Standards.

These steps and strategies are not intended to be prescriptive or exhaustive and it may not be necessary to take all the steps and strategies outlined below. You should also consult relevant standards and guidance on information security including any which are particular to your sector or industry (see 'Standards' and 'Information security resources' below).

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, and may change over time, for example, as a result of technological change or if you become aware that security measures that previously protected personal information are no longer adequate.

You should be fully aware of all the personal information you handle, where it is kept and the risks associated with that information before deciding what steps to take. You could undertake robust information asset management by developing and maintaining a list or register which provides a high level description of the types of and location of personal information you handle. This will help ensure that your personal information security measures are comprehensive.

Many of the steps and strategies in this guide may also assist you in protecting other types of information, such as commercially confidential information.

Governance, culture and training

Fostering a privacy and security aware culture

Your privacy and security governance arrangements should include appropriate training, resourcing and management focus to foster a privacy and security aware culture among your staff. Personal information security should be an integrated component of your entire business and not left to the compliance or ICT area alone. The creation of this culture will require the active support of, and promotion by, senior management.

Insufficient interest in personal information security from staff, in particular senior management including the board (or equivalent decision making body), can lead to threats to the security of personal information being ignored and not properly attended to. Appropriate training can assist in mitigating these issues and making staff aware of common personal information security threats (see 'Personnel security and training' section below).

If your entity has experienced a significant breach of personal information security, the focus of your senior management should be to look at whether significant cultural changes are needed to improve security in the long term rather than relying on superficial solutions or treating such issues as 'someone else's problem'.

Oversight, accountability and decision-making

You should establish clear procedures for oversight, accountability and lines of authority for decisions regarding personal information security. You could have a body or designated individual/s that are aware of what personal information you hold, where and how it is held and responsible for ensuring that it is held securely. This role could include defining information security measures and implementing and maintaining those measures. This role should be overseen by, and accountable to, your senior management.

- Are privacy and personal information security steps and strategies driven by your senior executives?
- Do the governance arrangements foster a privacy and security aware culture among your staff?
    - Do the governance arrangements promote awareness and compliance with personal information security obligations?
    - What governance arrangements do you have in place?
- Are there clear procedures for oversight, accountability and lines of authority for decisions related to personal information security?
    - Is it clear who is responsible for the overall operational oversight and strategic direction of your information handling projects?
    - Are there distinct areas or persons who have responsibility for security and privacy issues?
        - Are these areas or persons aware of what personal information you hold and where and how it is held?

  - If there are several areas or teams responsible for information security and privacy, are there governance arrangements in place to ensure that they work together, creating a focal point for privacy advice and solutions and preventing silos?
  - Are regular meetings held at the senior management and operational level to discuss security and privacy issues and incidents?
- Do your change management processes include consideration of the effect of changes on personal information security?
- Do governance arrangements include risk management and business continuity plans?
- Do you have procedures in place to respond to data breaches?
  - Is there is a focal point for coordinating your data breach response?
  - Are there clear roles and responsibilities for staff when in responding to a suspected data breach, including an eligible data breach?
  - Are these roles and responsibilities set out in a written data breach response plan?[29]
  - Who will ensure that you meet your NDB scheme obligations?
- Are there ICT governance protocols in place? For example are there persons responsible for the accreditation and approval of personal information security controls to ensure that each control is effective and appropriate?

Personnel security and training

Personal information security includes ensuring your entire staff are aware of their privacy and security obligations (including senior management). Human error can be a contributing cause to data breaches and undermine otherwise robust security practices where the systems have not been designed to deal with it.[30]

It is therefore important that all staff understand the importance of good information handling and security practices. The commencement of the NDB scheme also highlights the importance for all staff to have the capability to recognise eligible data breaches and understand the appropriate steps to be taken. Privacy training may help staff understand

[29] For more information about why you should have a data beach response plan, and how to develop one, see the OAIC's *Data breach preparation and response — A guide to managing data breaches in accordance with the* Privacy Act 1988 *(Cth)*.

[30] See the Own motion investigation report AICmrCN 5. The case illustrates how the failure to put in place adequate policies, procedures and systems to mitigate the risk of human error can result in a data breach.

their responsibilities and avoid practices that would breach your privacy obligations. Training should take into account new starters, contractors and temporary staff.

- Where appropriate, do staff have appropriate security clearances or undergo security vetting?
- Are staff provided with training on physical and ICT security and the handling of personal information?
    - When is training provided to new starters?
    - Is training also provided to short term staff and contractors?
    - Is refresher training provided to your staff and does this occur on a regular basis?
    - Are your staff informed of your internal practices, procedures and systems which relate to the handling of personal information? (see 'Internal practices, procedures and systems' section below)
    - How are your staff informed of changes to these practices, procedures and systems?
- Is personal information security training of staff considered at the project design stage?
- Is there an appropriate amount of training, resourcing and active management support to promote a privacy and security aware culture?
    - 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 identity authentication procedures?
    - Does training emphasise to staff the importance of authentication processes not infringing customer/client privacy?
    - Does training cover recognising and avoiding inadvertent disclosures?
        - When verifying an individual's identity?
        - When publishing files online — are staff trained to identify and remove embedded personal information not intended for public release?
    - Does training cover staff obligations under the NDB scheme?
- Does training address the need to avoid weak passphrases and passphrase reuse?
- Are staff reminded on a regular basis of their obligations to handle personal information appropriately?
    - Are there signs in the workplace or alerts on computer systems?
    - Do computer logon screens outline staff privacy and security responsibilities?

- When a staff member moves to a different position, or leaves your organisation or agency, is their access to personal information reviewed or revoked?
- Are staff trained to report privacy issues and suspected or actual data breaches to the area or persons who have responsibility for security and privacy?
- Does training cover recognising and avoiding 'phishing' and 'spear phishing' attacks and 'social engineering'?
- Are staff advised on how to mitigate against unauthorised access if they discuss customers' or clients' personal information over the telephone?
- Are there procedures governing the printing of documents containing personal 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?
    - 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 ICT systems, what measures are in place to secure this access?
    - Who has overall responsibility for the security of personal information at those workspaces?
- Are there clear polices governing the use of end-user mobile devices, including 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 end-user mobile devices (such as password protection, encryption)?
    - Are return address labels placed on end-user mobile devices in case of loss?
    - Are staff members educated about the risks of accessing or handling the entity's data on unauthorised/insecure devices, including the risks associated with BYOD practices?
    - If it is necessary for staff to take personal information off the premises, what steps do you take to ensure the security of personal information that is removed?
    - Is confidential business information segregated from personal user information?

Internal practices, procedures and systems

Under APP 1.2, entities are required to take reasonable steps to establish and maintain practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code.[31]

For the purposes of APP 11, you should document the internal practices, procedures and systems that you use to protect personal information. Your documentation should

[31] For further information see the APP guidelines, Chapter 1.

outline the personal information security measures that are established and maintained against the risks and threats to personal information. These documents should be regularly reviewed and updated to ensure they reflect your current acts and practices.

You could also consider documenting the security choices you have made about your security profile, including the reasons why you have or have not adopted specific personal information security measures.

Internal practices, procedures and systems which relate to personal information security may be addressed in a single policy or in a number of separate policies.[32] Additionally, you should make sure that staff are aware of, and have access to, these policies and are trained regarding their responsibilities (see 'Governance, culture and training' section above).

- Do you have policies which address personal information security matters, such as the physical, ICT and access security and other appropriate personal information handling practices?
    - Did a PIA and an information security risk assessment inform the development of these policies?
    - Are your documented policies easy to understand?
    - If there are multiple policy documents involved, is it clear how they relate to each other, for example their hierarchy or order of importance?
    - Do the policies use language and concepts that are consistent with the Privacy Act?
    - Do your policies refer to your obligations under the Privacy Act, including the NDB scheme, and other laws to protect personal information? Do they clearly explain how these obligations underpin these policies?
    - Are all staff, including short-term staff and contractors, aware of and able to access these policies easily?
    - Do these policies reflect your current acts or practices? Are mechanisms in place for ensuring that policies are updated and regularly reviewed?
    - Are mechanisms in place to enable staff members to seek clarification or suggest updates?
    - How do you ensure compliance with internal policies, for example, are there designated privacy officers and regular reporting to the entity's governance body to ensure this occurs?
    - What steps do you take if it becomes evident that staff members are not observing elements of your policies?
    - 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

[32] Use of the term 'policy' in this section refers to your entity's internal documentation regarding its personal information security profile, not its APP privacy policy which is discussed in APP 1.3-1.6.

them?

ICT security

Effective ICT security requires protecting both your hardware and software from misuse, interference, loss, unauthorised access, modification and disclosure. However, ICT security measures should also ensure that the hardware, software and personal information stored on it remain accessible and useful to authorised users.

It is expected that entities regularly monitor the operation and effectiveness of their ICT security measures to ensure that they remain responsive to changing threats and vulnerabilities and other issues that may impact the security of personal information.

You should be aware of the personal information you hold on your ICT system and where it is located. Your ICT security measures should ensure that all of your systems are secure and that they provide a safe environment for your:

- staff to carry out your business
- customers to interact with your agency or business, for example when they make payments or provide their banking details and/or other personal information.

You need to consider the security of all systems that use or interact with your ICT system. This includes securing your website(s), social media platforms, mobile device applications (apps),[33] along with Internet connected end-user mobile devices (such as smartphones, tablets and laptops), portable storage devices, desktop terminals, kiosks, as well as Wi-Fi networks, remote access and other aspects of your systems.

ICT security measures help mitigate the risks of internal and external attackers and the damage caused by malicious software such as malware, computer viruses and other harmful programs. These programs can be used to gain unauthorised access to your computer systems in order to disrupt or disable their operation and steal any personal information stored on those systems. ICT security measures can also help mitigate the risks of internal threats.

As well as ICT security against external and internal threats, it is important to consider the possibility of:

[33] The OAIC has developed a guide to help mobile device application (app) developers embed better privacy practices in their products and services. See the OAIC's *Mobile privacy: a better practice guide for mobile app developers*.

- human error (for example, misplacing devices such as laptops and data storage devices, noting that encryption and password protection can mitigate this risk)
- hardware or software malfunctions
- power failure
- system failure caused by natural disasters such as earthquakes, floods, and extreme weather conditions.

Software security

You should consider whether the software you use is sufficiently secure. Errors made during software development can potentially result in privacy breaches.

- Do you regularly review your software security to confirm its continued effectiveness? Is software tested to ensure that there no flaws which can result in privacy breaches?
- Has security software been deployed across all network components (for example on servers and network gateways), not only workstations?
- Are the latest versions of software and applications in use?

Patches can result in a number of extra functions and features that should be assessed for their privacy impacts before they are installed.[34]

- What processes are in place to ensure that patches and security updates to applications and operating systems are installed as they become available?

Removing or disabling unneeded software, operating system components and functionality from a system reduces its vulnerability to attack, and can make it harder for malware to run or an attacker to gain access.

- Are operating system functions that are not required disabled (for example AutoPlay or remote desktop access)?

There is a risk that content delivered through 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 browsers, including 'add-ons' or 'plug-ins' are up to date.[35] Disabling unused applications may also assist in preventing unauthorised access to a computer system.

- Are applications and web browsers configured for maximum security (eg. plug-ins up to date, unused applications disabled)?
- Are add-ons and plug-ins regularly reviewed and updated?

If you are downloading or using web applications (such as web-based email, wikis, directly updating personal details on databases) or importing data to a system, you should ensure that appropriate security and scanning measures are in place.

[34] Patches are software that is used to correct a problem with a software program or a computer system.
[35] Add-ons and plug-ins are software that add specific functions to a browser

- Are all email attachments received from an external source scanned before they are opened?
- Are computer files scanned and checked for abnormalities at workstation level?
- Do you have security measures in relation to web applications?

Encryption

Encryption is important in many circumstances to ensure that information is stored in a form that cannot be easily understood by unauthorised individuals or entities. Encryption methods should be reviewed regularly to ensure they continue to be relevant and effective and are used where necessary. This includes ensuring that the scope of encryption is wide enough so that attackers cannot access another unencrypted copy of your encrypted information.

- What encryption methods do you use? Are they reviewed regularly to ensure they are effective?
- Have you considered whether you should employ encryption of:
  - Databases used to store personal information?
  - Servers?
  - Backups?
  - Information stored in third party cloud servers?
  - Internal network communications, such as email or file shares?
  - End-user mobile devices, such as smartphones, tablets and laptops, including BYOD?
  - Portable storage devices?
  - Data in transit, for example data transferred over the Internet?
- How are decryption keys managed?[36]
- Do you enable encrypted communications on your website (for example, for making payments)?
- Is there another unencrypted copy of your encrypted data?

Network security

You need to have appropriate security controls in place to protect your network. The security controls that are appropriate will depend on the circumstances.

Intrusion prevention and detection systems can be an effective way of identifying and responding to known attack profiles. This may include using firewalls, which control the incoming and outgoing network traffic, and software applications, such as filtering, that monitor network or system activities for malicious activities, anomalous behaviour, or

[36] Decryption is the process of converting encrypted data back into its original form, so it can be understood. In order to easily recover the contents of encrypted information, the correct decryption key is required.

policy violations.

- Do you employ and maintain an intrusion prevention and detection system and regularly analyse event logs?
- What sorts of firewalls are employed and are they appropriately configured?
- Is both incoming and outgoing web traffic filtered?
- How do you monitor and detect unauthorised downloading, transferring or theft of bulk data, for example through the use of personal storage devices?

Spammers may use spoofed email to try to bypass filters and make it appear as though email comes from a legitimate source.[37] Such emails may ask the recipient to provide their own or other individuals' personal information.

- Do you have systems in place to protect your email systems from malware, spam and spoofing, including blocking spoofed email?
- Do you employ email validation and authentication systems, for example the Sender Policy Framework[38] and Domain Keys?[39]

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?
- Does the information with the highest risk have the highest level of protection applied?
- What steps have been taken to ensure that this information is not inadvertently taken outside of the secured environment?
- Are downloaded files quarantined from the network until it is established that they are safe (opened in a segregated testing environment such as a sandbox)?

[37] Spoofed email is email in which parts of the email header are altered so that it appears to have come from a different source.

[38] Sender Policy Framework is an email validation system designed to detect email spoofing by allowing receiving mail exchangers to check that incoming mail from a domain is being sent from a host authorised by that domain's administrators.

[39] DomainKeys is an email authentication system designed to verify the domain of an email sender and that the email message was not modified in transit.

Whitelisting and blacklisting

Whitelisting and blacklisting are ways of controlling the content, applications or entities that are allowed to run on or access a device or network.[40]

Both can prevent potentially harmful material from accessing your system. Whitelisting may offer greater protection than blacklisting 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 whitelisted. Reputation-based lists used for blacklisting need to be maintained and updated to be effective due to the rapid pace with which malicious sites come and go.

- Is whitelisting of applications, email attachments and web domains and IP addresses employed?
- If not, has blacklisting of applications, email attachments and web domains and IP addresses been used instead?
    - If so, what steps are in place to ensure the blacklist remains relevant, up to date and complete? For example, is the blacklist automatically updated from time to time?

Testing

Testing of ICT systems should occur during their development, transition to operations and regularly once they are operational. Depending on the situation, you may wish to consider penetration (or vulnerability) testing to discover security weaknesses, or configuration reviews, to test whether networks are operating towards a certain standard.

You need to consider how to scope your testing — remember that testing only discrete elements of your ICT system may miss systemic issues.

- How often is testing conducted?
- Does it cover all aspects of the system?
- Who is responsible for conducting testing (eg. internal, independent)?
- How is test data handled?
- Is actual personal information or dummy data used for testing? If actual personal information is used:
    - has a PIA and information security risk assessment been undertaken to assess the personal information flows caused by the testing?[41]

[40] Whitelisting is permissive — it is a list of the content, applications or entities that are allowed. Blacklisting is prohibitive — it is a list of the content, applications or entities that are not allowed.

[41] An example of a 'use' that an individual may be taken to reasonably expect is use for the secondary purpose of a normal internal business practice, such as auditing, business planning, billing or de-identifying personal information. The OAIC generally considers that the use of personal information to test ICT security systems may be a normal internal business practice in limited circumstances, such as where it is

  - do your internal practices, procedures and systems reflect the use of personal information for testing?
- If testing identifies weaknesses, how is this reported and addressed?

Backing up

To prevent personal information you hold from being lost, you should make copies of important files and store them on a physical device or online using a cloud-based storage solution.

- Are backups set up to run frequently?
- Is all essential information included in backups?
- How far back is data recoverable?
- Do you have a data retention policy which reflects APP 11.2?
- Do you review your backups to check that personal information that is no longer needed is:
  - destroyed or de-identified?
  - if contained in a Commonwealth record, handled in accordance with the Archives Act?
  - if required by law or a court/tribunal, is retained? (see 'Destruction or de-identification of personal information' section below)?
- Are backups regularly tested to see if the data is recoverable?
- Are physical devices used to store your backup files kept in a secure location?
- Are backups stored remotely to protect from natural disasters?

Email security

Email is not a secure form of communication and you should develop procedures to manage the transmission of personal information via email.

- Do you avoid sending certain types of personal information via unsecured email (for example sensitive information)?
- Do you use secure methods for communicating information, such as a secure website or to a secure online mailbox?
- Do you use secure messaging where appropriate and available?
- Do you obtain a recipient's consent to send their own personal information to them via email?
- Do you validate the email address with the recipient before sending the unencrypted email to reduce the chance of unauthorised disclosure to a party who

unreasonable or impracticable to use de-identified or dummy data (subject to the exception in APP 6.2(a)). For further information see APP guidelines, Chapter 6, paragraph 6.22.

is not the intended recipient?

- Do you ensure that accurate records are kept regarding when external emails are sent and received?
- Do you only send sensitive information or large amounts of non-sensitive personal information by email as an encrypted or password protected attachment?

Access security

Access security and monitoring controls help you protect against internal and external risks by ensuring that personal information is only accessed by authorised persons.

'Unauthorised access' is a separate concept from 'disclosure', as an entity is not taken to have disclosed personal information under APP 6 (Use and disclosure) where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information. However, the entity may breach its security obligations under APP 11 if it did not take reasonable steps to protect the personal information from unauthorised access.[42]

In addition, unauthorised access of personal information by a third party could trigger notification obligations under the NDB scheme if it is determined that, as a result of this unauthorised access, individuals are likely to be at risk of serious harm.

Trusted insider risk

You need to guard against internal threats such as unauthorised access or misuse of personal information by your staff, including contractors (the trusted insider risk). Trusted insider breaches can occur when staff mishandle personal information while carrying out their normal duties. These actions are often motivated by personal advantage, for example insiders accessing personal information for financial gain.

To minimise this risk you should, when possible, limit internal access to personal information to those who require access to do their job (ie provide access on a 'need to know' basis). Limiting such access is an important personal information security mechanism.

If someone is transacting with you using a pseudonym, you could also consider further restricting access to personal information that is linked to that person to protect the pseudonym.[43]

- Do you limit access to personal information to those staff necessary to enable your entity to carry out its functions and activities?
- Is the number of users with administrative privileges limited to staff requiring those privileges?
- Is access revoked promptly when no longer required?

[42] The terms 'unauthorised access' and 'unauthorised disclosure' are not defined in the Privacy Act. See Chapter 11 of the APP guidelines for further guidance on the meaning of these terms.

[43] APP 2 covers issues related to anonymity and pseudonymity.

- Have you considered restricting access to personal information when a customer/client is using a pseudonym?
- Have you considered physically disabling USB or other external port access to devices or disabling internal CD/DVD writers in devices?
- Have you considered employing remote wiping software to allow for the deletion of personal information stored on end-user devices which have been lost or stolen?

Identity management and authentication

You should have processes in place to identify individuals accessing your systems and control their access by associating user rights and restrictions with their identity. This will ensure that only authorised persons can access your systems.

Authentication is a key part of this process and is often managed by providing one of three factors— something one knows (such as a password or code), something one has (a physical token, such as a bank card, security pass, or a mobile phone to receive SMS confirmation), or something one is (biometric information such as a fingerprint). 'Multi-factor authentication' requires at least two factors.

Appropriate authentication can be used to limit a person's access both to the system or network and also to the information contained within it. It can also assist in mitigating security risks such as 'social engineering'[44] (including 'phishing' and 'spear phishing'[45]).

- What factors do you use for authentication?
- Is multi-factor authentication employed in circumstances that may pose a higher security risk (such as remotely accessing a system or where they are accessing sensitive/restricted personal information)?
- Have technical solutions which block or mitigate the effects of phishing, spear-phishing and social-engineering attacks been applied (where appropriate)?

Access to non-public content on web servers

If you host content that is not intended for public release (non-public content) on your web servers, you should consider storing this content elsewhere or restrict access to this information to authorised and authenticated users only. This ensures that non-public content will not be accessed by unauthorised third parties, including search robots[46] such as GoogleBot.[47] In conjunction with authentication, you should also disable directory

[44] 'Social engineering' is a term used to describe manipulating individuals into revealing confidential information or performing actions such as granting access to systems.

[45] 'Phishing' typically involves sending an email that appears to come from a legitimate organisation and attempts to trick the recipient into supplying personal information. 'Spear phishing' is a personalised attack utilising personally relevant information to attempt to appear legitimate to a particular user.

[46] Search robots or bots are software programs which run automated repetitive tasks over the Internet. They are most commonly used by web search engines and other sites for 'Web crawling' or 'Web spidering'. This involves a search engine using bots to discover new and updated pages which are then added to the search engine's index of Web content.

[47] GoogleBot is Google's web crawling bot.

browsing when configuring web servers.[48]

- Are there clear policies and procedures in place governing the identification and removal of embedded personal information from files before they are published online where the information is not intended for public release?

If you store non-public content on your web servers:

- Do you have access controls in place?
- Can the information be stored on a separate system which is not publicly accessible?
- Have you disabled directory browsing on your web servers?
- Are web servers configured to request search robots such as GoogleBot (via the robots.txt.file)[49] not to index, archive or cache files containing personal information?
- Do you regularly review and monitor your web servers to ensure that:
    - files containing non-public content are not vulnerable to being accessed by unauthorised persons?
    - you are aware of unusual or anomalous traffic on the website? (see 'Audit logs, audit trails and monitoring access' section below).

Passwords and passphrases

Your entity should use passwords and passphrases to identify that users requesting access to your systems are authorised users. Passwords and passphrases should be complex enough so that others are not able to guess it, for example using a combination letters, numbers and symbols rather than actual words or common numbers.

- Is password or passphrase complexity enforced? For example, including uppercase characters, lowercase characters, punctuation, symbols, and/or numbers.
    - Are there mechanisms for changing them regularly?
    - Is reuse of passwords or passphrases blocked?
    - Is there a minimum length requirement? Is sharing of passwords or passphrases forbidden?

[48] Directory browsing gives permission to users to view a listing of the files in a web server. If directory browsing is disabled, an 'Access Forbidden' error message is displayed if the user attempts to access either a file or folder on the web server.

[49] One way to prevent GoogleBot from crawling content on a website is to use robots.txt to block access to files and directories on a server. 'Robots.txt' is a protocol used to request cooperating search robots not to access all or part of a website which is otherwise publicly accessible. Search engines comply with 'robots.txt' voluntarily and the OAIC has noted that most search engines comply with 'robots.txt', including Google, Bing and Yahoo.

  - Are passwords or passphrases stored securely, such as in a 'hashed', 'salted'[50] or 'encrypted' format?
- Do accounts lock the user out after a specified number of failed logins?
  - Is a system administrator required to unlock accounts?
  - Do you suspend accounts that are unused or inactive for a period of time?
  - How quickly are accounts removed or suspended once someone leaves the entity?
- Are screen lock 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?
- Are staff (including contractors) trained in the importance of strong passwords or passphrases and how to choose them?

Sometimes passwords are created using patterns that are known only to an entity and its staff (or part of its staff). Whilst each password is unique, there is a risk that a password may be inferred by someone who is aware of the pattern but is not authorised to access the file.

Longer password patterns with many variations that are selected randomly rather than following a recognisable or known pattern are less likely to be guessed by unauthorised persons.

- Are passwords generated by patterns which are randomly selected and complex in terms of their length, character and order?

Collaboration

If you collaborate and share personal information with other entities while working on projects, you may continue to 'hold' personal information that is being used by the other collaborator. In these circumstances you must take reasonable steps to protect the information from unauthorised access while in their physical possession, including having

[50] 'Salting' is basically where an additional string of data, such as random numbers or text, is added to the password to make it less predictable and harder to attack, and 'hashing' is where passwords are processed through cryptographic algorithms that convert them into seemingly random characters. While passwords may be guessed through computational 'brute-force' attacks, this becomes very difficult when strong hash algorithms and passwords are used. Hashed passwords are therefore more secure to store than their clear-text passwords. The Australian Signals Directorate's *Australian Government Information Security Manual, Controls Manual* [PDF] (Control 1252, page 177) requires agencies to ensure usernames and passwords are hashed with a strong hashing algorithm which is uniquely salted.

effective controls in place to ensure that it is only accessed by authorised persons.

- How is the sharing of personal information managed to ensure access only by authorised persons?
  - How is access monitored?
  - Is the personal information shared using a secure method?
  - Is a platform that is managed, controlled or owned by another entity (such as a contract service provider), used to share the information? If so, what controls are in place to limit access?
  - Is the information encrypted and password protected? How are passwords managed and distributed to the user group?
  - Is there an access control policy in place which applies to everyone handling the personal information?
  - Are there policies and controls in place to prevent the unauthorised downloading, transferring or theft of bulk data shared with other entities, for example through the use of personal storage devices?

Audit logs, audit trails and monitoring access

Unauthorised access of personal information can be detected by reviewing a record of system activities, such as an audit log. Maintaining a chronological record of system activities (by both internal and external users) is often the best way for reviewing activity on a computer system to detect and investigate privacy incidents. Audit logs should also be named using a clear naming convention.

Audit trails are used to reconstruct and examine a sequence of activities on a system that lead to a specific event, such as a privacy incident.[51]

Access monitoring software that provides real time (or close to real time) dynamic review of access activity can also be useful for detecting unauthorised access to personal information. Use of proactive monitoring to identify possible unauthorised access or disclosure, including any breach that might amount to an eligible data breach for the purposes of the NDB scheme, may be a reasonable step for you to take particularly if you use many systems or databases which hold large amounts of personal information.

- What methods do you use to identify inappropriate access of files or databases containing personal information?
  - Do you use audit logs and audit trails?
  - Is access by both internal and external persons monitored? Is there a method for identifying anomalous behaviour?
  - Are these measures mainly reactive (review of logs, responding to incidents) or do they also involve real time or close to real time monitoring of access activity,

[51] 'Audit log' and 'audit trail' are defined in the Australian Signals Directorate's *Australian Government Information Security Manual, Control Manual* [PDF], Glossary of Terms, p. 307.

noting that the greater the number of systems and databases you use and amount of personal information you handle, the more important it is to proactively monitor access? (also see 'Network security' section above)

- When anomalous behaviour is detected, what processes are used to determine whether such behaviour amounts to unauthorised access, including any processes in place to assess whether the access might give rise to an eligible data breach for the purposes of the NDB scheme?[52]

- What points of access (such as access to devices, files, networks, databases, and websites) do you audit?
- Are audit logs reviewed on an on-going basis?
  - do you check/audit the activity of administrators?
- Does the audit log or audit trail indicate when an individual has:
  - accessed or viewed material
  - changed or destroyed material, or
  - unsuccessfully tried to access personal information?
- Does the audit log or audit trail enable actions to be linked to individuals, including both regular users and administrators?
- What procedures exist to address any issues, such as anomalous patterns of access, identified during a review of an audit log?
- How long are the audit logs kept for?
  - Are they part of a backup process?
- How are audit logs protected from tampering?
- Do logs or reports contain personal information and if so is it adequately protected?

Individuals accessing and correcting their own personal information

Under the Privacy Act, entities must, on request, give individuals access to the personal information held about them unless an exception applies.[53] Individuals are also able to request correction of the personal information held about them.[54]

- What processes do you have in place to assess requests from individuals to access

[52] Note that an entity must take all reasonable steps to assess whether a suspected data breach is an eligible data breach within 30 calendar days after the day the entity became aware of the grounds that caused it to suspect an eligible data breach. For more information about evaluating suspected data breaches, see the OAIC's Assessing a suspected data breach.

[53] See APP 12. Along with the right to request access under the Privacy Act, individuals have a right under the *Freedom of Information Act 1982* (Cth) (the FOI Act) to request access to information held by Australian Government agencies.

[54] See APP 13 — where an individual requests an APP entity to correct their personal information, APP 13.1 provides that the entity must take reasonable steps to correct the personal information it holds, to ensure it is accurate, up-to-date, complete, relevant, and not misleading, having regard to the purpose for which it is held. Individuals also have rights under the FOI Act to have their personal information amended if it is out of date, misleading, incorrect or inaccurate.

or correct their personal information?

- How do your staff identify customers/clients prior to disclosing their personal information online, by phone or in person?
- What measures do you take to ensure that these authentication processes do not result in collecting personal information that it is not reasonably necessary to collect?

Third party providers (including cloud computing)

Entities that outsource part or all of their personal information handling will need to consider whether they still 'hold' that personal information. If so, APP 11 will apply and you will need to take reasonable steps to comply with APP 11. If APP 11 applies to you, you will also be subject to the requirements of the NDB scheme, even if it is the third party who suffers the eligible data breach.[55] In this instance, while both you and the third party are subject to the requirements of the NDB scheme, only one of you is required to notify individuals of an eligible data breach.[56]

General issues

Relevant factors in deciding the steps that are reasonable in the circumstances include whether the third party is subject to the Privacy Act in its own right. Even if the third party is subject to the Privacy Act, if you hold the personal information, you still need to consider what steps are reasonable to protect the personal information. Steps may include influencing the third party's conduct.

Have you:

- conducted appropriate due diligence on the services to be provided (particularly data storage services)?
- considered the scope of the personal information handling services to be provided (for example, will the provider also backup your personal information holdings and if so what data will be captured)?
- considered what security controls and personal information handling measures you expect the third party supplier to use?
- included terms in the contract to deal with specific obligations about the handling of personal information and mechanisms to ensure the obligations are being fulfilled, such as regular reporting requirements?
- considered your obligations under the NDB scheme and how you will manage your relationship with the third party, such as including contractual terms, to ensure all eligible data breaches are identified, assessed and notified as required?
- for agencies, complied with s 95B of the Privacy Act which requires agencies to take contractual measures to ensure that a contracted service provider (as defined in the Privacy Act) does not do an act, or engage in a practice, that would breach an

[55] See the OAIC's Entities covered by the NDB scheme resource.
[56] For more information about data breaches involving more than one organisation, see the OAIC's Notifying individuals about an eligible data breach resource.

APP?[57]

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.[58] 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 NDB 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

[57] 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.

[58] Cloud computing services have been defined as a way of sourcing and delivering ICT which enables convenient, on-demand network access to a shared pool of configurable computing resources (eg. networks, servers, storage, applications and services). The Australian Government has adopted the US Government's National Institute of Standards and Technology definition for cloud computing. For further information see the Australian Government's Secure Cloud Strategy and supporting material which apply to the use of cloud services by Commonwealth entities, available on the Digital Transformation Agency's website.

[59] The Australian Signals Directorate publishes resources with guidance on addressing information security risks of cloud computing.

[60] You may also need to consider the data protection or privacy legislation in place where the data is stored by the cloud provider, as well as any other jurisdictions the cloud service provider may be subject to.

[61] For more information, see the OAIC's guidance on the NDB scheme.

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

[62] In 2014, the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) also published ISO/IEC 27018:2014 which relates to the implementation of measures to protect personal information while it is being processed in the public cloud. The standard uses a definition of 'Personally Identifiable Information' adopted from ISO/IEC 29100:2011. If adopting this standard, entities must ensure that they apply the definitions of personal information and sensitive information in the Privacy Act. More information can be found in the 'Standards' section below.

[63] For more information about assessing a suspected data breach, see the OAIC's Assessing a suspected data breach resource.

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?

Data breaches

In the event of a data breach, having a response plan that includes procedures and clear lines of authority can assist you to contain the breach and manage your response. Ensuring that staff (including contractors) are aware of the plan and understand the importance of reporting breaches is essential for the plan to be effective. The OAIC has published its *Data breach preparation and response — A guide to managing data breach in accordance with the* Privacy Act 1988 *(Cth)*.

- Is there a data breach response plan and does it flow logically from any broader information security plan?
  - Is the plan regularly tested?
  - Does the plan include a strategy to assess and contain breaches?
  - Does the plan clearly identify those actions that are legislative or contractual requirements, such as any steps required by the NDB scheme?
  - Are your staff educated about the plan and how to identify and respond to data breaches?
  - Does the plan enable staff to identify data breaches and require that breaches be reported?
  - Does the plan include guidance on how to assess a data breach to determine whether it is likely to result in serious harm for the purposes of the NDB scheme?[64]
  - Does the plan establish clear lines of command and indicate responsible officers?
  - Does the plan outline clearly when and how affected individuals and the OAIC should or must 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?

Following the commencement of the NDB scheme, data breaches that are likely to result

[64] For more information about assessing suspected or eligible data breaches, see the OAIC's Assessing a suspected data breach resource.

in serious harm to an individual are also subject to notification requirements. Entities covered by the *My Health Records Act 2012* and current and former contracted service providers covered by the *National Cancer Screening Register Act 2016* have additional notification obligations to the Commissioner.[65]

Physical security

Physical security is an important part of ensuring that personal information is not inappropriately accessed. You need to consider what steps, if any, are necessary to ensure that physical copies of personal information are secure. Similarly, you 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?
- Are work areas with particular access to personal information (for example, human resources sections, complaints handling sections) physically segregated from other areas of business?
- Is there a record management system that identifies files and the location of responsible staff that contain personal information?
- Have privacy and security been considered when designing the workspace?
  - Are workstations positioned so that computer screens cannot be easily read by unauthorised 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, particularly in open plan workplaces?
  - Do employees have access to secure storage spaces near their workstations to secure documents temporarily?
- Is there a clean desk policy where personal information is being handled? Is it enforced?
- What provisions are made for securing physical files containing personal information?
  - How is the movement of physical files recorded?
  - Are storage and movement of files containing personal information audited or monitored?
  - On what basis is access to physical files granted?

[65] For more information about the mandatory My Health Record data breach notification requirements, see the OAIC's *Guide to mandatory data breach notification in the My Health Record system*. Information about the interaction between these requirements and the broader NDB scheme can be found in that Guide under the heading 'The broader Notifiable Data Breaches (NDB) scheme'.

  - If files are placed in lockable cabinets or similar, are these storage units kept locked? How is access to keys controlled?
- Are there procedures governing the transmission or transport of personal information to offsite work locations?

Destruction or de-identification of personal information

Where an entity holds personal information it no longer needs for a purpose that is permitted under the APPs, it must ensure that it takes reasonable steps to destroy or de-identify the personal information (APP 11.2) — in some cases, one or the other may be more appropriate. This obligation applies even where the entity does not physically possess the personal information, but has the right or power to deal with it.[66]

However, depending on the type of entity and the type of personal information involved, you may have specific obligations under law or a court/tribunal order to retain and/or destroy or de-identify personal information. Agencies also have specific retention obligations for personal information that forms part of a Commonwealth record.

- Do you have policies, procedures and resources in place to determine whether personal information you hold needs to be: retained under law or a court/tribunal order, destroyed or de-identified?
- Are your staff informed of document destruction procedures?

Destroying personal information — irretrievable destruction

Personal information is destroyed when it can no longer be retrieved. The steps that are reasonable for an entity to take to destroy personal information will depend on whether the personal information is held in hard copy or electronic form.

- Are your staff informed of document destruction procedures?
- Is destruction of personal information done in-house or outsourced?
  - If outsourced, what steps have you taken to ensure appropriate handling of the personal information?
- Has personal information contained in hard copy records that are disposed of through garbage or recycling collection been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding?
- Is hardware containing personal information in electronic form properly 'sanitised' to completely remove the stored personal information?
- Have steps been taken to verify the irretrievable destruction of personal stored by a third party on a third party's hardware, such as cloud storage? Where the third party has been instructed by the organisation to irretrievably destroy the personal information, have steps been taken to verify that this has occurred?

[66] See Chapter 11 of the APP guidelines for further guidance on the destruction or de-identification of personal information and the *De-identification Decision-Making Framework* published by the OAIC and CSIRO's Data61

- Are back-ups of personal information also destroyed? Are backups arranged in such a way that destruction of backups is possible? If not:
  - have steps been taken to rectify this issue in the future
  - has the backed-up personal information been put beyond use?
- How is compliance with data destruction procedures monitored and enforced?

Destroying personal information held in electronic form — putting beyond use

Where it is not possible for an entity to irretrievably destroy personal information held in electronic format, reasonable steps to destroy it would include putting the personal information 'beyond use'. For example, this could include where technical reasons may make it impossible to irretrievably destroy the personal information without also irretrievably destroying other information held with that personal information.

Personal information is 'beyond use' if you:

- are not able, and will not attempt, to use or disclose the personal information
- cannot give any other entity access to the personal information
- surround the personal information with appropriate technical, physical and organisational security. This should include, at a minimum, access controls including logs and audit trails, and
- commit to take reasonable steps to irretrievably destroy the personal information if, or when, this becomes possible.

It is expected that only in very limited circumstances would it not be possible for an organisation to destroy personal information held in electronic format.

- Where it is not possible to irretrievably destroy personal information held in electronic format has the organisation taken steps to put the information 'beyond use'?

De-identifying personal information

De-identification of personal information may be more appropriate than destruction where the de-identified information could provide further value or utility to the entity or a third party, but you should consider whether de-identification is appropriate in the circumstances.

Personal information is de-identified under s 6 of the Privacy Act, 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'.

- Do you have policies, practices and procedures in place to determine when it is appropriate to de-identify personal information?
  - How do you manage and mitigate the risk of re-identification?
  - Have steps been taken to verify the de-identification of personal stored by a third party (such as cloud storage)?

Standards

'Standards' are documents that set out requirements, specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform in the way they are intended.[67] Standards can include guidelines, handbooks, manuals or policies and may be general or specific to particular industries or sectors, or practices.

Entities should consider using relevant international and Australian standards, policies, frameworks and guidance on information security. This includes any which are particular to their sector or industry (for example the *National eHealth Security and Access Framework*, which is relevant to the Australian healthcare sector).

Australian Government agencies must apply the Attorney-General's Department's *Protective Security Policy Framework* and the Australian Signals Directorate's *Australian Government Information Security Manual*. These documents articulate the Australian Government's requirements for protective security and standardise information security practices across government. They may also be used by other government agencies (including state and territory agencies) and the private sector as a model for better security practice.

You may also want to consult the ISO/IEC 27000 series of information security management standards and the ISO/IEC 31000 series of risk management standards published by both the International Organization for Standardization and the International Electrotechnical Commission, parts of which have been adopted by Standards Australia.[68] The 27000 series of standards provide recommendations on information security management, risks and controls. The 31000 series relates to standards for the design, implementation and maintenance of risk management processes. Compliance with standards can be tested internally or certified by a third party.

Adopting a standard is one way that you can gain some confidence regarding your security practices, but complying with a standard does not of itself mean that you have taken reasonable steps to protect personal information. It may be a reasonable step, but you may also need to take further action to meet your obligations under APP 11.

You may also seek to use certification of compliance with a standard as an assurance that you are protecting personal information. However, you will need to be aware of the scope of any certification, for example, whether it includes an assessment of the implementation of the relevant standard/s in practice; or the suitability of the risk profile underpinning the adoption of the standard/s. You will also need to be aware of the extent to which you may rely on any certification of your processes or the processes of a party you are dealing with. Relying on the certification of your processes or the processes of a party you are dealing with may not of itself be considered 'reasonable steps' for the

[67] The term 'standards' is defined on the Standards Australia webpage What is a Standard?.

[68] Further information regarding Australian and international standards is available from the Standards Australia website at www.standards.org.au and the International Organization for Standardization website at www.iso.org.

purposes of APP 11. You may need to take further action to meet your security obligations under APP 11.

In adopting any standard, you must make sure that you apply the definition of personal information and sensitive information from the Privacy Act, and not any other similar definitions that might by imported by or used in the standard.

- Have you considered standards particular to your industry or sector?
- If you have decided not to adopt a widely used standard, are the reasons for this decision clearly documented?
- Do you ensure that the standards you employ are the most current and appropriate?
- Is internal or external auditing undertaken to ensure compliance with relevant standards?
- If you have sought a certification of compliance with a relevant standard, did the scope of the certification include implementation; and the suitability of the risk profile underpinning the adoption of the standard?
- If auditing reveals areas of weakness or non-compliance with a standard, are these reported and addressed in a timely and complete manner?