

Privacy information sheet 5

Security and personal information

Keeping personal information secure

Organisations that are subject to the *Privacy Act 1988 (Commonwealth)* have specific obligations to keep personal information secure. Under National Privacy Principle (NPP) 4, organisations must take reasonable steps to:

1. protect the personal information they hold from misuse and loss, and also from unauthorised access, modification or disclosure
2. destroy or permanently de-identify personal information that is no longer needed. Note that careful consideration should be given in determining whether the client may need the information in the future. Refer to Information Sheet 3 for details about granting access.

Data security is an important way of ensuring that personal information is only used for permissible purposes. The key to effective compliance with NPP 4 is developing an organisational culture that respects privacy. Organisations should ensure that both management and staff have a good understanding of their responsibilities to protect personal information from unauthorised misuse, loss, corruption or disclosure. These privacy information sheets can help with this. However, it is recommended that organisations also read the NPPs to understand their specific legal obligations. The NPPs are available at <http://www.privacy.gov.au/publications/npps01.html>.

Risk profile

Organisations must determine their risk profile when deciding on the *reasonable steps* that will be followed to ensure data security.

What is reasonable will depend on the specific circumstances under which the organisation holds personal information. The sensitivity of the stored personal information is an important factor and higher levels of security could be expected for sensitive information. In the case of an organisation holding non-sensitive information, where there is a low risk of unauthorised access and a small likelihood of serious consequences to the individual, then basic security measures may be adequate.

Security

There is a range of security measures for organisations to consider.

1. Physical security measures prevent unauthorised access to information and are relevant to all forms of storage. Physical measures may include barriers (e.g. locks), security keys and containers (e.g. filing cabinets and safes), and alarm systems to detect unauthorised access. In addition, these physical measures may be complemented by procedural measures that include:
 - recording file movements, especially if files are sent to different office locations
 - encouraging a *clean-desk policy*
 - storing files after use.
2. Computer and network security measures reduce the risk of unauthorised disclosure of personal information by protecting the integrity of information systems and networks.

Privacy information sheet 5

Security and personal information

Computer and network security measures may include access control for authorised users (eg. user passwords), and computer virus checking.

3. Telecommunications security measures reduce the risk of unauthorised or accidental disclosure of personal information through telecommunication networks. Communications security measures:
 - check facsimile numbers before sending personal information, and confirm their receipt
 - check the identity of individuals before disclosing personal information over the phone.
4. Personnel security measures reduce the risk of unauthorised staff accessing personal information, by limiting access to personal information to authorised staff only. Those people who need such personal information to carry out their duties should only access personal information.
5. Organisations should also ensure that those who do have access to personal information respect the organisation's culture of privacy. Personnel security measures:
 - train staff and management in security awareness, practices, and procedures
 - develop policies on who can access and use particular categories of information.

Securely disposing of personal information

An organisation that no longer needs to hold personal information for any purpose must take reasonable steps to securely dispose of the information. Reasonable steps may be determined by the organisation's risk profile (see page 1).

Disposal of personal information must occur by secure means to protect the privacy rights of individuals. Garbage disposal of intact documents leaves personal information vulnerable to unauthorised access and misuse; avoid this method of disposal.

Shred, pulp, or disintegrate paper-based records to ensure secure disposal.

When disposing of electronic records, remove all personal information from the computer system to ensure secure disposal.

Additional information

More information is available from:

1. the Office of the Federal Privacy Commissioner www.privacy.gov.au
2. the Privacy Hotline 1300 363 992 (local call charge)
3. the department's Privacy Contact Officer (07 3224 5850)

Disclaimer

This information sheet is intended as a reference to privacy legislation. It offers general discussion and explanation on a range of privacy issues. However, it does not cover all circumstances faced by the diverse range of organisations in the non-government sector. This information sheet is advisory only and does *not* represent legal advice. If advice of a legal nature is required, independent legal advice must be sought and the content of this information sheet cannot be relied upon.

Privacy information sheet 5

Security and personal information
