Ombudsman
New South Wales

Security of information

Why information security is important

Increasingly, information is becoming a valuable commodity that can be misused and abused. Government agencies gather, keep and use vast quantities of information. While the majority of this information relates to relatively mundane day-to-day operational matters, some concerns the personal affairs of individuals and business affairs of companies, or is sensitive for other reasons. This is exactly the kind of information that is most vulnerable to misuse.

Good public administration requires that a proper balance be drawn between the need on the one hand for government to be transparent and accessible to the public, and the need on the other hand to protect the integrity of official information and to prevent the unauthorised disclosure of personal or otherwise sensitive information. Information security ensures the availability, integrity and confidentiality of information systems and information.

While the Ombudsman has long supported a positive approach by agencies to the disclosure of information (often referred to as '*open government*'), we have also recognised that there are circumstances where effective public administration or the privacy rights of individuals requires confidentiality.

The circumstances where it may or will be important to ensure that official information is kept confidential include those where the release of information would:

- be an unreasonable disclosure of personal information or business affairs (eg. disclosure of information that could damage a person's reputation or be an invasion of their privacy without any important public interest being served)
- prejudice law enforcement or the security of premises and individuals
- prejudice the effectiveness of methods of an investigation, audit or review
- be premature, for example in some circumstances in relation to working documents prior to a final decision being made
- give unfair commercial advantage to individuals
- cause unreasonable damage to the government's commercial interests.

Legal requirements

The legal foundations for confidentiality/secrecy in relation to official information can be found in various legislation including the *Privacy and Personal Information Protection Act 1998* (PPIP Act), *Health Records Information Privacy Act 2002* (HRIP Act), *Freedom of Information Act 1989* (FOI Act), *State Records Act 1998*, and in the common law obligation of fidelity on employees.

It is also important to consider government policy as set out in various Premier's Department Circulars and Memoranda (for example Premier's Department Circular No 2001-46 *Security of Electronic Information* and 2002-69 *Labelling Sensitive Information*).

Security levels for sensitive material

The Premier's Department Circular 2002-69 sets out required standards for the labelling and handling of sensitive information, which meet Commonwealth security classifications. The guidelines are designed to ensure confidentiality and consistent safeguards for sensitive information distributed amongst NSW government agencies or wholly within an agency.

There are three levels of classification of sensitive information:

- **Highly protected** – used in exceptional circumstances and reserved for sensitive material and resources requiring the highest degree of protection.
- **Protected** – rarely used and reserved for sensitive material and resources requiring a substantial degree of protection.
- **In-confidence** – used for sensitive material and resources requiring a limited degree of protection.

These apply to sensitive material or resources which, if disclosed, lost, issued or damaged, could be expected to cause harm to individuals, the agency or government. It is assumed that only very small amounts of Highly Protected and Protected information will be held by most NSW agencies.

Obligations on agencies

All government agencies should adopt and regularly review policies, procedures and practices for the safe custody, preservation, distribution and disclosure of personal or otherwise sensitive information. Agencies should also ensure that all their staff understand their obligations in relation to the security of information held by the agency.

Since 2001 it has been government policy that agencies take adequate steps to safeguard their electronic information, including developing and implementing plans for information security management and seeking certification to the national standard for information security management – AS/NZS 7799.

Obligations on public officials

Public officials are obliged to protect the integrity and maintain the security of official information for which they are responsible. In this regard they must only use official information in the legitimate exercise of their official functions and not for personal purposes.

The use of official information for personal advantage, the release of official information at the whim of particular public officials, or the selective leaking of official information for an improper purpose, undermines the integrity of government and can cause unnecessary harm to individuals. Such conduct is conduct which could be investigated pursuant to the Ombudsman Act and may constitute corrupt conduct or criminality (eg. a breach of ss.62-63, PPIP Act).

Official information should only be released by public officials with proper authority and in accordance with established agency policies and procedures in the following circumstances:

- where it is necessary for the purpose of properly discharging the agency's functions
- in accordance with statutory rights of individuals to be given access to information (for example under the FOI Act, PPIP Act or HRIP Act)
- in accordance with government policy (for example Premier's Memorandum No. 2000-11 setting out guidelines for the disclosure of information in government contracts with the private sector)
- in accordance with the rules or enforceable orders of a court of tribunal
- in accordance with a requirement made by a body with the statutory power to require production of documents or statements of information (for example under the Ombudsman Act or Independent Commission Against Corruption Act).

Resources

- Premiers Department, specifically, circulars 2001-46 *Security of Electronic Information* and 2002-69 *Labelling Sensitive Information*. www.premiers.nsw.gov.au.
- Department of Commerce, government chief information office. www.oict.nsw.gov.au.
- SAI Global certification services. AS/NZS 7799 Part 2: 2003 (formerly AS/NZS 4444 Part 2: 2000) or BS 7799.2: 2002 are the information management standards against which organisations can be certified. www.sai-global.com.

Contact us for more information

Our business hours are: Monday to Friday, 9am–5pm (*Inquiries section closes at 4pm*)

If you wish to visit us, we prefer you make an appointment. Please call us first to ensure your complaint is within our jurisdiction and our staff are available to see you.

Level 24, 580 George Street
Sydney NSW 2000

Email nswombo@ombo.nsw.gov.au
Web www.ombo.nsw.gov.au

General inquiries 02 9286 1000
Facsimile 02 9283 2911

Toll free (outside Sydney metro) 1800 451 524
Tel. typewriter (TTY) 02 9264 8050

Telephone Interpreter Service (TIS): 131 450
We can arrange an interpreter through TIS or you can contact TIS yourself before speaking to us.

ISBN: 978-1-921132-95-7 03/2012