Australian Government
Office of the Australian Information Commissioner

Guide to information security

Privacy and your business

The Privacy Act requires you to take **reasonable steps** to protect personal information (which includes sensitive information). But it's not just about compliance... you also risk:

- loss of reputation and customer trust
- harm to your customers
- reduced business functions and activities

Privacy by design

Build privacy into your processes, systems, products and initiatives at the design stage.

Conduct a Privacy Impact Assessment (PIA). See the OAIC's Privacy Impact Assessment Guide: www.oaic.gov.au.
Also consider conducting an information security risk assessment in conjunction with a PIA.

What are reasonable steps?

Reasonable steps will always depend on the circumstances, including the following:

- Nature of entity holding the personal information
- Nature and quantity of personal information held
- Risk to individuals if personal information is not secured
- Data handling practices of entity holding the information
- Ease of implementation of security measure

Steps and strategies that may be reasonable to take include:

Governance
- Robust information asset management
- Dedicated individual or body responsible for managing personal information
- Governance arrangements to:
  - implement and maintain information security plans and measures
  - promote awareness and compliance

ICT security
- Whitelist and/or black list entities, content or applications
- Up to date software security
- User authentication
- Policies to prevent inappropriate or unauthorised access
- Point of access logs and audit trails
- Encryption
- Network security measures
- Testing ICT systems and processes
- Back ups
- Communications security measures

Data breach
- Develop data breach response plan
- Train staff about how to respond to data breaches
- If you are facing a data breach use the OAIC's Data breach notification guide www.oaic.gov.au

Physical security
- Security and alarm systems
- Access logs
- Workplace design
- Secure work and storage spaces
- Clean desk policy
- Storage and movement of files audited and monitored

Personnel security and training
- Appropriate security clearances
- Staff training (including contractors and service providers)
- Employee exit procedures

Workplace policies
- Policies documenting security matters, such as physical and ICT security
- Conflict of interest policy addressing handling of personal information of person known to staff member
- Policies addressing use of portable/mobile devices, and staff's own devices
- PSD, BYOD and offsite work policies

Information life cycle
- PIAs and information security risk assessments conducted for new or changed acts or practices
- Collection practices periodically reviewed
- Personal information protected:
  - during system upgrades
  - when passed to/handled by a third party
- Policies for data retention and destruction
- Outsourcing contracts address handling of personal information

Standards
- Relevant international, Australian and industry/sector standards on information security
- Compliance with standards tested internally or by third party

Monitoring and review
- Operation and effectiveness of information security measures monitored and reviewed regularly
- Changes implemented as a result of monitoring and review

The full text of the *Guide to information security—'Reasonable steps' to protect personal information* is available on the OAIC website: **www.oaic.gov.au.**