Commissioner for Privacy and Data Protection

Media release

# Reasonable security under Information Privacy Principle 4.1

## 25 January 2017

The Commissioner for Privacy and Data Protection has today published new guidance to provide the Victorian public sector direction on what 'reasonable security' means under Information Privacy Principle (IPP) 4.1. IPP 4.1 requires an organisation to "take reasonable steps to protect the information it holds from misuse and loss and unauthorised access, modification or disclosure".

The *Guidelines to protecting the security of personal information: 'Reasonable steps' under Information Privacy Principle 4.1* will assist organisations bound by the privacy provisions of the *Privacy and Data Protection Act 2014* to implement security measures that are appropriate to their organisation.

The guidelines promote a risk-based approach to information security, echoing the sentiment of the Victorian Protective Data Security Standards (VPDSS). Both IPP 4.1 and the VPDSS recognise that the security measures an organisation puts in place should be based on the organisation's individual circumstances and the risks they may face. The Commissioner regards that adherence to the VPDSS constitutes 'reasonable steps' under IPP 4.1. Accordingly, the reasonable security measures offered in the guidelines are drawn from the VPDSS.

Some of the steps that may be considered 'reasonable' to protect the security of personal information include:

- putting in place a security management framework to define roles, responsibilities, and approaches to security risk management
- embedding security and privacy training and awareness programs into corporate inductions
- establishing processes for responding to security incidents
- effective monitoring and oversight of contracted service providers in relation to information security practices
- appropriately valuing information so that commensurate security measures can be applied
- personnel security management, including pre-employment screening and assessing the ongoing suitability and eligibility of employees
- securing ICT systems throughout the system lifecycle
- securing physical environments, to prevent unauthorised access to personal information that could be exposed as a result of poor physical security.

The steps that will be appropriate to take will be dependent on an organisation's individual circumstances. The guidelines also provide an overview of the factors that will influence which steps may be considered 'reasonable', including the size of the organisation, its resourcing, the type and value of the information it holds, and the potential impact that a privacy or security breach may have on the organisation and the individuals involved.

The guidelines are available in full at https://www.cpdp.vic.gov.au/menu-resources/resources-privacy/resources-privacy-guidelines.