Privacy self assessment guide

Appendix two – assessment questions

1.0 Purpose

An effective self-assessment will involve measuring the practices and procedures of a business unit against set criteria. For a privacy self-assessment, these criteria can be drawn from the privacy principles.

The following checklists may be useful in conducting a privacy self-assessment, but note that they contain very general questions, based on high level principles drawn from both the Information Privacy Principles and the National Privacy Principles. Agencies should consider developing additional agency or business unit specific questions to assist in conducting the assessment.

2.0 Accountability

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Are privacy policies complete and easy to understand?					
Is there someone in the agency who is responsible for agency compliance with or overseeing/managing the IP Act?					
Do privacy policies apply to the information of officers as well as members of the public?					
Have agency officers been given training about their obligations under the IP Act?					
Has the agency met its obligations when entering into contracts involving personal information?					
Have personal information policies been clearly communicated to agency officers?					
Does the agency have procedures in place to ensure new staff are given appropriate training in personal information handling?					
Has the agency developed documentation to explain their personal information policies and procedures to the public?					

3.0 Collection

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Does the agency identify why it is collecting personal information before it is collected?					
Does the agency provide a collection notice to individuals from whom personal information is being collected?					
Has the agency determined how much and what kind of personal information it needs to collect?					
Is the amount of personal information collected no more than is necessary for the purpose for which it is required?					
Is the agency collecting personal information lawfully and fairly?					
Has the agency taken the necessary steps to ensure the personal information being collected is accurate?					
Does the agency collect only personal information which is relevant to the purpose for which it is being collected?					

Appendix two – assessment questions

4.0 Security

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Is the personal information held by the agency protected against unauthorised access, use, modification or disclosure?					
Is the personal information held by the agency protected against loss or misuse?					
Has the agency adopted physical, technical and administrative safeguards to protect personal information?					
Are security safeguards appropriate considering the sensitivity of the personal information?					
Have agency staff been made aware of the importance of protecting personal information?					
Are there processes in place to record access to electronic records?					
Are there processes in place to ensure personal information is disposed of in a way that does not allow unauthorised access?					

5.0 Accuracy

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Are there reasonable measures in place to ensure that personal information is accurate, complete and up to date before it is used?					
Are their procedures in place for people to amend their personal information if it is incorrect?					
Are there processes in place to record when and where key personal information was collected, including when it was updated?					

6.0 Openness

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Does the agency make information available about its personal information policies and procedures?					
Does the agency tell people why it collects, how it uses and when it discloses their personal information when It collects it?					
Is there a person members of the public can contact about privacy questions?					
Does the agency tell people how they can access and amend their personal information?					
Does the agency provide details to the public of the categories of personal information it holds?					

Appendix two – assessment questions

7.0 Use and disclosure

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Does the agency use information only for the purpose it was collected, unless one of the exceptions in IPP 10 or NPP 2 applies?					
Does the agency disclose information only where the person was advised when it was collected or one of the exceptions in IPP 11 or NPP 2 apply?					
Does the agency have procedures in place to ensure that use or disclosure of personal information under NPP 2 or IPP 10 and 11 is noted on the personal information?					

8.0 Complaint and Breach Review

Criteria question	Assessment			Evidence	Actions
	Met	Not met	Partially met		
Is there a documented process for managing privacy complaints and privacy breaches?					
Is this process documented and available to agency officers?					
Is the process, or a version of it, available to the public?					
Is the privacy complaint handling process timely and are complainants generally satisfied with the response given?					
Is there a clear process for complaint handlers to inform relevant agency officers when practices that need changing are identified?					
Is there a clear process to action needed changes where complaint handlers have identified issues?					
Have identified reforms to agency processes been successfully implemented?					
Has there been a reoccurrence of any privacy breaches?					

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

Last updated 1 December 2009 – Changes to the legislation after this date are not included.