Privacy Maturity Matrix

Version 1.0

Information and Privacy Commission NSW

	Meeting Compliance		Pursuing Best Practice	
	Maturity Level			
Area of Practice	**Level 1 – Developing Foundations**	**Level 2 – Established Compliance**	**Level 3 – Embedded Operations**	**Level 4 – Optimised Excellence**
Culture and Leadership	The Executive and Senior Leadership are building awareness of their role in promoting a privacy-positive culture. Privacy practices and procedures do not exist, are not fully developed, are not fit for purpose or are performed in an ad-hoc manner.	The Executive and Senior Leadership support the promotion of a privacy-positive culture to all levels of the organisation. Privacy practices and procedures are available and routinely performed.	The Executive and Senior Leadership pro-actively monitors the promotion of a privacy-positive culture to all levels of the organisation. Privacy practices and procedures are embedded into business-as-usual processes.	The Executive and Senior Leadership promote a privacy-positive culture and advocate it as a priority to all levels of the organisation. Privacy practices and procedures are subject to continuous improvement activities.
Privacy Reporting	A statement that demonstrates privacy compliance is not available in the organisational annual report or it does not include statistical details of any internal reviews conducted.	A statement that demonstrates privacy compliance is available in the organisational annual report, including statistical details of any internal reviews conducted.	Reporting privacy compliance in the annual report statement forms an explicit and documented part of wider privacy responsibilities and processes and reflects identifiable and documented privacy activities performed in the reporting period.	Review and continuous improvement processes are in place to maximise the amount of information provided in the annual report statement demonstrating privacy compliance including the range of privacy responses and improvements performed in the reporting period, as well as privacy priorities of the organisation and how privacy risks and issues are addressed and mitigated.
Data Breach Reporting	The organisation is unaware of the data breach notification scheme and does not consider reporting in the event of data breaches.	The organisation is aware of the data breach notification scheme and follows the IPC NSW advice in the reporting of data breaches.	The organisation has in place a data breach response plan which includes defined reporting thresholds that are specific to the risks associated with the personal information held by the organisation and the format it is held in. Documented processes to follow in the event of notification of a data breach are documented and understood by all relevant staff.	A data breach response team is in place to ensure that the organisational data breach plan is followed in the event of a data breach, including notifying the IPC NSW of a data breach. Processes to respond to a data breach and the threshold for notification are regularly reviewed and improved, including after each data breach.
Information Holdings	There is not a clear understanding of the full scope of personal information held by the organisation, or there are gaps in knowledge about where it is stored, what it is used for and who has access to it. Who has responsibility for personal information held by the organisation is not clearly defined.	The organisation has a clear understanding of the personal information held, where it is stored, what it is used for and who has access to it. It is clearly defined who is responsible for the personal information held by the organisation.	Identification and management of personal information is integrated into wider organisational information classification and management functions. The organisation has a schematic view of the personal information it holds, where it is stored, and who has access to it. The purposes for each holding of personal information is clearly documented. Responsibility of individuals over personal information is an explicit component of data governance arrangements.	The scope of personal information holdings is regularly reviewed as part of risk and audit management processes, which identify privacy risks and privacy-positive improvements that can be made to the extent of personal information held, how it is governed, how it is stored and accessed, and the purposes for which it is held.

	Meeting Compliance		Pursuing Best Practice	
	Maturity Level			
Area of Practice	**Level 1 – Developing Foundations**	**Level 2 – Established Compliance**	**Level 3 – Embedded Operations**	**Level 4 – Optimised Excellence**
Privacy Impact Assessments	Privacy impact assessments are not undertaken for new projects or where there is a significant change planned, or else they are completed at a point where their outcomes can no longer influence project design and implementation.	Privacy impact assessments are undertaken for new projects or where there is a significant change planned. The assessments are completed at a point where outcomes of the assessment can influence project design and implementation.	There is documented guidance provided to project teams that communicates the purpose and process for carrying out a privacy impact assessment for new projects or where there is a significant change planned. Incorporation of assessment outcomes into project design and implementation is explicitly included in project planning and management. Privacy impact assessments performed by the organisation are available to inform wider and future project teams.	The performance of privacy impact assessments form part of a wider privacy-by-design approach, whereby privacy positive activities are built into projects from initiation and planning through to implementation and operation. Project teams are provided with specific training and guidance to follow a privacy-by-design approach. Privacy impact assessment outcomes are communicated through audit and risk committees and result in actions across the organisation that drive privacy improvements.
Privacy Functions	Delegations and authorisation of functions as required in legislation are not in place.	The organisation has in place the delegations and authorisation of functions as required in legislation and publicised as required.	Delegations and authorisation of functions are in place and there are processes to regularly review these. There is an accessible record of the delegations and authorisations that exist and when they were last reviewed.	Privacy delegations and authorisation of functions are considered as part of any structural changes to the organisation. Reviews of delegations and authorisations result in improvements that seek to address identified deficiencies, risks and issues in the management of personal information.
Privacy Management Plan	A Privacy Management Plan has not been developed or else does not address all required inclusions or a Privacy Management Plan has been developed but a copy of the plan has not been provided to the IPC NSW.	A Privacy Management Plan has been developed and addresses all required inclusions and a copy of the plan has been provided to the IPC NSW.	There are processes in place to ensure that the Privacy Management Plan is complete, reflects the current state of the organisation, and has periodic reviews. Processes include providing the IPC NSW with a copy of the plan whenever updates or other changes are made, as well as making the current plan available through the organisation's website and by request.	The Privacy Management Plan is used as a key reference in areas such as data management, training and onboarding, and strategic planning. The organisation has in place processes to ensure that any activities, actions or reviews that affect privacy trigger a review and update to the plan. Processes include providing the IPC NSW with a copy of the plan whenever updates or other changes are made, as well as making the current plan available through the organisation's website and by request.
Internal Reviews	There is no process in place to perform an internal review in a timely manner when an application is received. Individuals conducting the review are external to the organisation, are not suitably qualified to deal with the subject of complaint or are involved some way in the original matter. Timings for completion of the review and notification to applicants are not in line with legislative requirements.	A process is in place to perform an internal review in a timely manner when an application is received. Reviews are undertaken by an individual within the agency who is directed by the agency to deal with the application, is suitably qualified to deal with the subject of the complaint and was not involved in any way in the original matter. Timings for completion and notifications of reviews are in line with legislative requirements.	A structured process to respond to and manage requests for internal reviews is in place. The roles and responsibilities for undertaking a review – including the identification and nomination of qualified individuals – are clearly defined and communicated in regular staff training sessions. The reviews process includes identifying clear remedial actions that should be implemented and monitoring to ensure that these occur. There is oversight in place to ensure completion of the review and notification to the applicant occur as soon as possible and well within legislative requirements.	