Australian Government

National Indigenous Australians Agency

NIAA

Privacy Management Plan

2025-26

What is a Privacy Management Plan?

The National Indigenous Australians Agency (NIAA) is required to have a Privacy Management Plan (PMP) under the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (the Code).

The PMP is a strategic planning document that the NIAA uses to:

- identify its privacy risk profile
- assess its privacy maturity level
- set privacy goals and targets, and
- set out how it will meet its compliance obligations under the Australian Privacy Principles (APPs) and the *Privacy Act 1988* (Privacy Act).

The NIAA has developed this PMP with reference to the Interactive PMP Explained resource published by the Office of the Australian Information Commissioner (OAIC). The PMP is reviewed annually.

Privacy Risk Profile

The NIAA must self-assess its privacy risk profile (low, medium or high) to help set appropriate targets and actions in its PMP.

Low risk	**Medium risk**	**High risk**
• Agencies which provide no public services, are largely policy focused, and handle little to no personal information	• Agencies which provide some public services but handle less personal information, or which influence the privacy practices of other agencies	• Agencies which provide complex public services to individuals and handle a significant amount of personal information

The NIAA has assessed its privacy risk as MEDIUM.

Risk assessment rationale

The NIAA (we, us, our) works in genuine partnership to enable the self-determination and aspirations of First Nations communities. We lead and influence change across government to ensure Aboriginal and Torres Strait Islander peoples have a say in the decisions that affect them.

We handle sensitive information about racial or ethnic origin, and other personal information, for our engagement, policy development, design and implementation functions and activities, and in limited direct service delivery and program implementation.

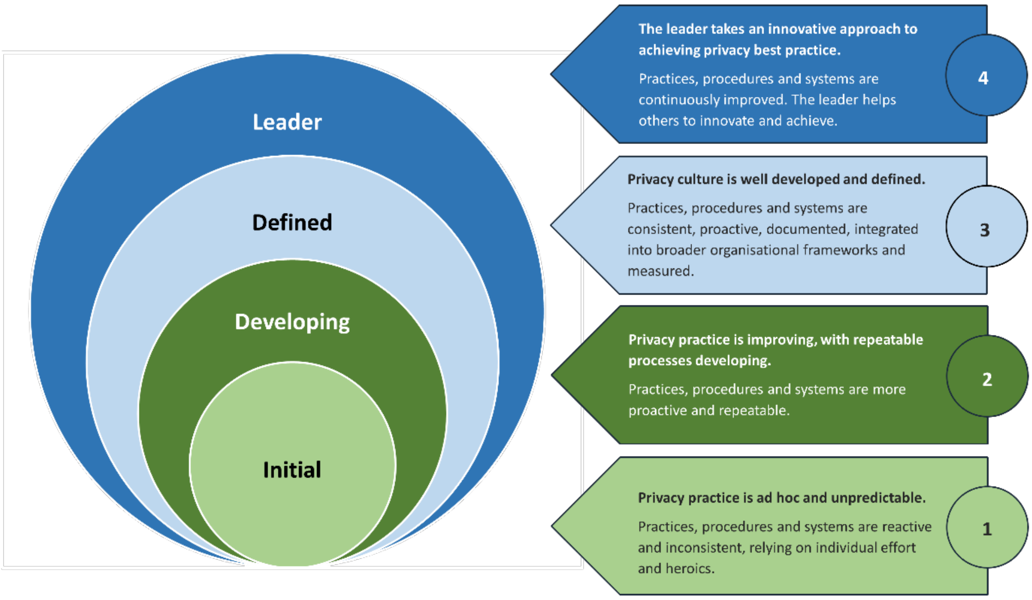
Our PMP supports our purpose by recognising the role of collecting, using and sharing personal information to empower Aboriginal and Torres Strait Islander peoples and communities, influence change across government, and build and maintain genuine partnerships.

The privacy maturity framework

The NIAA measures its privacy maturity using the Privacy Program Maturity Framework (Maturity Framework) developed by the OAIC. The Maturity Framework has 21 attributes, which are sorted into 5 elements:

1. Governance and Culture
2. Privacy Strategy
3. Privacy Processes
4. Risk and Assurance
5. Data Breach Response

Each attribute is assessed against four maturity levels:



The leader takes an innovative approach to achieving privacy best practice.

Practices, procedures and systems are continuously improved. The leader helps others to innovate and achieve.

Privacy culture is well developed and defined.

Practices, procedures and systems are consistent, proactive, documented, integrated into broader organisational frameworks and measured.

Privacy practice is improving, with repeatable processes developing.

Practices, procedures and systems are more proactive and repeatable.

Privacy practice is ad hoc and unpredictable.

Practices, procedures and systems are reactive and inconsistent, relying on individual effort and heroics.

Privacy Maturity Assessment - Current and Target

Using the OAIC Maturity Framework, the NIAA has assessed its current privacy maturity level as ‘DEFINED’.

A DEFINED maturity level recognises the NIAA’s key privacy compliance and governance systems are established, documented and measured. This privacy maturity level acknowledges there are opportunities to continuously improve privacy and information handling practices across the agency, to support strategic outcomes and promote a culture that values privacy.

The NIAA’s privacy maturity target is ‘LEADER’.

A target maturity of LEADER reflects the NIAA’s vision as a reliable and trusted digital leader that shares and uses personal information with confidence and is a trusted custodian of others’ data. This PMP identifies goals and targets to support continuous improvement of the NIAA’s privacy capability, to drive and inform evidence-based policy and program outcomes that make a tangible different to the lives of First Nations peoples.’

Privacy Maturity Assessment – Detail by Element

Overall privacy maturity level

Average of element scores	**3.4 / 4**
Overall privacy maturity level	**3 / 4 (DEFINED)**

Governance and Culture

Governance & Culture			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Privacy Champion*	**Defined**	**Leader**	The NIAA's Deputy Chief Executive Officer is the NIAA's Privacy Champion. The Privacy Champion promotes a culture of privacy that values and protects personal information. This includes regular emails to engage with all staff about privacy compliance focus areas, messaging during Privacy Awareness Week and annual reporting to the Executive Board. The NIAA's Legal Services Branch supports the Privacy Champion by providing updates on privacy developments, such as PIAs conducted, emerging privacy risks, significant data breaches and regulatory change. The performance of the Privacy Champion is not measured as a KPI.
Privacy Values	**Defined**	**Defined**	The NIAA promotes a culture of respecting and protecting personal information to build trust. The NIAA's vision is documented in this PMP and Data and Digital Strategy (2024 - 2028), to be a trusted digital leader that shares and uses data and personal information with confidence, and as a trusted custodian of others' data and personal information. The NIAA PIA threshold assessment template encourages staff to assess how a new project or initiative aligns to the Agency's values.

Governance & Culture			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Privacy Officer*	**Defined**	**Leader**	The NIAA has 3 designated Privacy Officers within the Legal Services Branch (LSB). LSB has established practices, templates and procedures to support staff to meet privacy obligations, which are integrated into broader organisational frameworks. There is agency-wide awareness of the Privacy Officers, including through intranet presence and messaging during Privacy Awareness Week. The Privacy Officers make proactive privacy improvements, including providing plain-language templates, privacy advice and delivering privacy training to staff. A Privacy Officer will attend and participate in the AGD Officials Working Group on privacy reform.
Management & Accountability	**Leader**	**Leader**	The NIAA's Legal Services Branch (LSB), led by the Chief Lawyer, oversees privacy compliance and trends. The Privacy Champion provides strategic leadership and promotes the value of personal information. LSB has created and maintained documents promoting privacy compliance and accountability. Documents are published on the intranet and reinforced through staff messaging, including through Privacy Awareness Week. Other documents (such as the Access and Corrections Policy and complaints standard operating procedure) are available for LSB use only. Privacy Officers measure and document the Agency's privacy performance and undertake continuous improvement initiatives (review and uplift of privacy governance, processes and templates). The Privacy Team and / or Privacy Officers regularly report to senior management, the NIAA Executive Board and the Privacy Champion on significant privacy issues. The Chief Lawyer is a member of the NIAA's Risk and Operations Committee and raises significant or strategic privacy risks in this forum.

Governance & Culture			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Awareness	**Defined**	**Defined**	The Privacy Officers, supported by the Legal Services Branch (LSB), work with clients to ensure their work complies with the Privacy Act. This includes ensuring privacy is built into the lifecycle of grants and procurements. There is an increased engagement on privacy issues. Data from LSB’s matter management system shows that privacy is the second most frequent type of request for advice. The Privacy Officers are continuing efforts to encourage staff to view privacy as a positive and valuable part of business as usual. This includes updating the staff intranet so that information and resources on privacy are easy to find and understand, and activities and communications through Privacy Awareness Week.
Element score (average of attribute scores)			**3.2 / 4 (Defined)**

Privacy Strategy

Privacy Strategy			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Privacy Management Plan*	**Defined**	**Defined**	The Privacy Management Plan is a strategic planning document used by the Privacy Officers, Champion and Senior Executive to measure the NIAA's privacy maturity and identify opportunities to improve, innovate and uplift privacy practices across the Agency. The PMP is considered and endorsed by the NIAA's Risk and Operations Committee. The PMP includes measures for addressing any known privacy compliance gaps and details the handling of personal information throughout the information lifecycle with specific focus on areas that the Agency assesses as having greater risk. It also includes actions to improve privacy maturity outcomes. The NIAA advises staff and senior management of the NIAA's PMP including publishing the PMP on the intranet.
Inventory of Personal Information*	**Leader**	**Leader**	The NIAA has a comprehensive Personal Information (PI) Holdings Register that documents data flows in and out of the agency. The PI Holdings Register is being updated as part of a regular review to ensure changes are documented. Material updates to the NIAA's information holdings have informed the review of the NIAA's privacy policy.
Data Quality Processes*	**Defined**	**Leader**	The NIAA has a range of data management policies to support staff to maintain data quality. These resources include the Information Management Policy and Records Management Policy. These resources are routinely reviewed to improve the quality of information holdings (including those with personal information). The NIAA also has project and team-level procedures to support good data governance practices for teams dealing with high amounts of data, including personal information. The NIAA Data and Digital Strategy 2024-28 reinforces the strategic importance of accurate, timely, reliable and reusable data and information. The Strategy supports a continuous improvement approach to developing processes and systems that ensure the quality of personal information and data. The Digital Transformation Agency's Policy for the Responsible Use of AI in Government states that agencies should consider integrating AI and related issues and risks into privacy frameworks. The PM&C has an Artificial Intelligence Policy that addresses privacy issues. The NIAA does not yet have its own AI policy that addresses privacy risks (including data quality issues) around using AI to handle personal information.

Privacy Strategy			
Attribute	Current Level	Target Level	Rationale/Commentary
			Privacy Officers, with Legal Services Branch support, encourage staff to keep personal information complete, accurate and up to date.
Information Security Processes	Defined	Leader	Under a Shared Services arrangement, the NIAA leverages PM&C's information security policies, systems and processes, aligned with the Australian Government's Protective Security Policy Framework (PSPF). The NIAA predominantly holds electronic records, stored in its Electronic Document and Records Management System (EDRMS), SharePoint and Share+. The records in EDRMS are accessible to staff with the appropriate security clearances within the Records Management Team only. Share+ and SharePoint files are accessed in accordance with business needs. For Share+, access is controlled through Aurion, and access is granted based on that profile (e.g. a staff member is part of a particular team and there is a business need to access particular records). The Privacy Officers work collaboratively with key operational stakeholders (including the ICT Security Adviser, Chief Information Officer, and Records Management Team) on managing mutual and shared risks and issues, such as data breaches. The Privacy Officers influence the development and setting of technology controls, to help mitigate privacy risk. The Privacy Officers will continue to raise awareness on complementary privacy and security policies and processes relating to mutual risks and issues (such as data breaches, access controls, appropriate use of technology, workplace surveillance, retention etc.)
Element score (average of attribute scores)		3.3 / 4 (Defined)	

Privacy Processes

Privacy Processes			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
External Privacy Policy & Notices*	**Leader**	**Leader**	The NIAA Privacy Policy is comprehensive and clear and is published to the NIAA website. The NIAA Privacy Policy and external notices were comprehensively reviewed and simplified as part of the 2024-25 PMP. There is a clear link between privacy notices and the privacy policy, which are easy to locate on the NIAA website. Privacy messaging is consistent and clear, and notices are usually provided at the point of contact. Privacy messaging is viewed positively and as an important part of the NIAA's privacy practice. Teams are proactive in developing privacy notices for projects and consultations, using available templates. They regularly seek advice from the Privacy Team on drafting privacy notices. The Privacy Team provides both a standard and plain English template privacy notice to clients, where appropriate.
Internal Policies & Procedures	**Defined**	**Leader**	Internal privacy policies and procedures are clear, relevant, comprehensive, and easy to locate on the NIAA intranet. This includes a privacy resources page, with templates and links to information, and a dedicated data breach response page. All privacy governance documents are proactively reviewed and kept up to date (as required) in response to emerging privacy risks. The Privacy Officers, supported by the Corporate and Commercial Law team, take innovative approaches to improve these resources, including engaging with Communications team experts to ensure privacy resources are accessible, clear and can influence staff to build a privacy-aware culture and behaviour.

Privacy Processes			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Privacy Training*	**Defined**	**Defined**	Privacy training is mandatory for all new staff, and annually for all staff. This training is delivered through the NIAA eLearning platform. The Privacy Officers, supported by the Legal Services Branch (LSB), develop and deliver bespoke privacy training that is operationalised to a business unit. LSB works with the NIAA's Workforce Capability Team to develop a clear and integrated privacy training program that supports and is relevant to staff depending on their role and business unit. Staff training completion rates and monitored and reported regularly at senior executive levels.
Privacy Impact Assessments*	**Leader**	**Leader**	The NIAA has tailored and clear PIA threshold assessment (PTA) templates to encourage and empower business areas to assess privacy risk and incorporate privacy by design into new projects and initiatives. The Privacy Officers, supported by the Corporate and Commercial Law team, support business areas to undertake comprehensive PTAs and PIAs for high privacy risk projects. The Privacy Officers leverage PIAs to continue to raise awareness to ensure privacy by design principles are understood and applied consistently across the agency.
Dealing with Suppliers	**Developing**	**Defined**	Privacy Officers provide advice on privacy due diligence and risk management in arrangements with third parties to produce better privacy outcomes. Business areas engage with privacy risks when engaging third parties in a variety of manners, including grants and procurements. The Legal Services Branch (LSB) works with the Procurement Team to update the procurement risk assessment template. It now includes consideration of whether the goods or services may introduce privacy data breach risks to Agency. LSB continues to work with the Procurement Team to develop procurement case studies. The NIAA is working to mature its capability when engaging with grantees on privacy risks and opportunities. The Privacy Officers, supported by LSB, continue to raise awareness of privacy risks through established forums with key business areas.

Privacy Processes			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Access & Correction*	**Leader**	**Leader**	The NIAA approaches access and correction requests as an opportunity to demonstrate openness and transparency. The Agency has an Access and Correction Policy to ensure requests are managed consistently and in line with the Agency's privacy obligations. The Freedom of Information (FOI) Team in Legal Service Branch (LSB) consults with Privacy Officers on FOI requests made by applicants for access to their own personal information. A joint decision is made on whether the request should be handled as a FOI request or an APP 12 access request. The Privacy Officers, supported by the LSB, continue to raise awareness across the Agency to ensure access and correction requests are handled in a consistent manner.
Complaints & Enquiries	**Defined**	**Leader**	The NIAA maintains open communication channels for privacy-related complaints and enquiries (by internal or external stakeholders) through the dedicated privacy telephone line and inbox. The Privacy Team has developed a Privacy Complaints Standard Operating Procedure (Privacy Complaints SOP) to assist Corporate and Commercial Law staff in responding to privacy complaints. The Privacy Officers continue to engage with the Complaints Team on client-focused approaches to support consistent complaints-handling practice at an Agency level.
Element score (average of attribute scores)			**3.3 / 4 (Defined)**

Risk and Assurance

¡Risk & Assurance			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Risk Identification & Assessment	**Defined**	**Defined**	The NIAA has integrated information security into its wider risk management framework. Information security controls are embedded into the Agency's processes and systems (including the ways staff can send, store and access emails and documents). A range of related information security policies and guidelines are accessible to all staff (such as PM&C's Security Policy Framework and Information Management Policy). Privacy risks are proactive identified and responded to using the PIA threshold assessment (PTA) process, and through annual review of privacy information and governance (data breaches, enquiries, complaints and requests for advice). The NIAA's Audit and Assurance team are conducting an audit of the Agency's management of privacy risks and their impacts on the NIAA's relationships and influence, people and capability and information and records management.
Reporting & Escalation	**Leader**	**Leader**	Reporting lines are defined and documented. Privacy risks, issues and incidents are escalated to Executive. Mechanisms for reporting and escalating privacy issues is generally understood across the agency. Legal Services Branch (LSB) briefs the Privacy Champion annually on privacy. This is to ensure the Privacy Champion is supported to brief the CEO on Privacy annually (including in relation to the Privacy annual report, privacy case load trends and PIAs conducted). Privacy Officers and LSB provide regular updates to the Chief Lawyer on privacy related casework and privacy management priorities. The documented Privacy Complaints process provides guidance on reporting expectations for privacy complaints. Privacy Officers raise awareness with NIAA staff to ensure that they understand the thresholds for escalation of privacy risks, issues, incidents and complaints (including data breaches).

iRisk & Assurance			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Assurance Model	**Defined**	**Leader**	Privacy assurance activities occur in the development and review of this privacy management plan and creating governance processes for the Legal Services Branch to ensure privacy activities and processes are understood and implemented. Privacy risks and identified and managed through delivering privacy advice and when responding to data breach incidents, including through maintaining a data breach register and PTA/PIA register. Recommendations are documented by the LSB and communicated to business areas with responsibility to implement controls. The Privacy Officers collaborate with information security, ICT, data governance and risk functions to ensure privacy risks are considered. The Privacy Team are currently assisting the NIAA's audit and assurance function in relation to a privacy audit. The audit will provide further assurance of privacy governance and risk management.
Element score (average of attribute scores)			**3.3 / 4 (Defined)**

Data Breach Response

Data Breach Response			
Attribute	**Current Level**	**Target Level**	**Rationale/Commentary**
Data Breach Response Plan	**Leader**	**Leader**	The NIAA has a well-defined data breach response plan that empowers staff to identify and respond to data breaches. It clearly defines response personnel, processes and escalation pathways to contain, assess, notify (if required) and review a data breach. A quick reference guide and data breach assessment templates support staff to recognise and respond to data breaches when they occur, and to identify the factors that may indicate a notifiable data breach. The Privacy Team has a data breach response advice template which promotes consistency in advice and streamlines assessments. It enhances compliance with statutory timeframes. The Privacy Officers have proactively reviewed the data breach response plan to incorporate lessons learned and changes in business functions, including in response to data breaches that occurred in the previous PMP year. It is currently being updated to streamline reporting and remove duplication in the Data Breach Response Report. The Privacy Officers will continue work to strengthen data breach response across the agency, by promoting awareness and considering opportunities to test the data breach response plan with business areas and key stakeholders.
Data Breach Notification*	**Leader**	**Leader**	The NIAA has a data breach response plan that includes a notification process that aligns with OAIC notifiable data breach guidance, and to ensure incidents are assessed against relevant tests for an eligible data breach. The data breach response plan acknowledges the obligations and benefits of notification. It outlines notification options such as individual notifications or establishing communication channels for affected individuals to contact the Agency. It includes a drafting and review procedure that supports notifications that are appropriate to the circumstances, transparent and timely.
Element score (average of attribute scores)			**4 / 4 (Leader)**

Goals for improvement

The privacy goals and targets in this section are based on the agency's privacy maturity assessment outcomes. This section includes mandatory actions which the agency must take to meet its compliance obligations under APP 1.2 (Code, s 9(2)(b)).

Element	Attribute	Action	Due
Governance & Culture	Privacy Champion	Privacy Champion Annual Report is delivered to the Privacy Champion. Develop a Privacy Champion bi-annual message to all staff and staff engagement KPI. Support the Privacy Champion to influence privacy culture, including engaging with stakeholders.	01/08/2025 31/12/2025 Ongoing
	Privacy Officer	Regularly review privacy practices to stay aligned with governance, security, and business priorities. Work with teams through forums and collaborate with other agencies to meet privacy goals and prepare for upcoming law changes	Ongoing
	Awareness	Make privacy resources easy to access and understand and find creative ways to engage staff with policies and processes. Promote awareness through activities like Privacy Awareness Week, tailored training, and feedback opportunities.	Ongoing PAW (16 – 22/6/25)
Privacy Strategy	Privacy Management Plan	Privacy Management Plan review is finalised in Q2 (1 April 2025 - 30 June 2025).	30/06/2025
	Inventory of Personal Information	Complete the personal information holdings stocktake and update the personal information register, using findings to review privacy governance and policies. Establish an annual review process to monitor changes and update the register as needed.	30/09/2025 Ongoing
	Data Quality Processes	Use existing data quality practices to create guidance for staff. Promote data quality as a key goal through awareness activities, training, and privacy communications.	Ongoing During PAW (16 – 22/6/25)

Element	Attribute	Action	Due
	Information Security Processes	Engage with operational areas and Shared Services to manage shared risks and strengthen collaboration on privacy and security. Work with PM&C, IT, and relevant teams to implement recommendations from the Information Commissioner's Messaging Apps Report.	Ongoing
Privacy Processes	External Privacy Policy & Notices	Explore innovate ways to deliver privacy messages, including through using infographics and images to improve user experience. Proactively engage with the expertise in the Communications branch to develop these resources.	31/09/2025 Ongoing for new privacy notices
	Internal Policies & Procedures	Work with the Communications team to create clear privacy resources and tools. Involve staff and managers in shaping procedures to ensure they are practical and support a strong privacy culture.	31/12/2025
	Dealing with Suppliers	Work with procurement and grants teams to embed privacy considerations in third-party assessments. Review related procedures and templates to ensure consistent processes for managing privacy risks.	Ongoing
	Complaints & Enquiries	Review the Privacy Complaints SOP and update as needed.	Ongoing
	Privacy Impact Assessments	PTA and PIA register is kept up to date. PIA register is published to the NIAA website.	Quarterly update
	Privacy Training	Engagement with Workforce Capability Team on updating privacy training eLearning.	N/A
	Access & Correction	Review intranet content to promote staff awareness of access and correction policy and process.	31/12/2025
Risk & Assurance	Assurance Model	Continue improving assurance activities by updating registers, using advisory data for best practice, and measuring staff privacy awareness. Work with internal audit to strengthen independent assurance through audits.	Ongoing
Data Breach Response	Data Breach Response Plan	Promote awareness of data breach response plan, including by testing the data breach response plan with business areas and key stakeholders (e.g. PM&C Shared Services).	31/12/2025