Privacy Commissioner
Te Mana Mātāpono Matatapu

Privacy Management Plan

Overview

The purpose of a Privacy Management Plan is to identify specific, measurable goals to improve your organisation's privacy capability and outline how these goals will be achieved. The goals should be based on an assessment of organisational weaknesses and risks when it comes to compliance with the Privacy Act.

Your plan should address each of the guidance pou and identify the steps and timeframe for meeting these. Your plan can cross-reference, rather than duplicate, existing material such as your privacy strategy, policies, and procedures.

The template below will help you develop your own plan. The key objectives and actions you commit to for each pou will depend on your specific circumstances, such as the size of your organisation, your risk profile, your business model, and resources.

When completing the template, delete the key objectives and actions that you won't be focusing on or aren't applicable to your organisation. You might use this template as your annual privacy management plan – selecting the key priority objectives and actions that your organisation will focus on for the year.

Privacy Commissioner
Te Mana Mātāpono Matatapu

Governance			
Key objectives			
• The governance function can demonstrate that it takes action to ensure that privacy risks, gaps or issues are appropriately identified, documented and addressed. • The governance function actively supports embedding privacy in operational practice. • Ownership and accountability for oversight of privacy within the organisation is clearly documented (for example, in an organisational chart, role descriptions, or other administrative documents). • Resourcing of the privacy function is appropriate for the organisation's risk profile and is regularly reviewed.			
Action examples	**Position responsible**	**Due**	**Status**
Define key roles and responsibilities for privacy management			
Assign staff responsibility for managing privacy			
Assess organisational privacy risk and assign a risk profile			
Create reporting processes that ensure senior leadership and governance groups are routinely informed about privacy issues			

Privacy Commissioner
Te Mana Mātāpono Matatapu

Know Your Personal Information			
Key objectives			
• The organisation has a data inventory or equivalent and has used this to assess its risk profile. • Staff understand what personal information is and how they can use it in their role. • There is a central log or record of the organisation's current data/information sharing agreements. • Policies for data classification, including handling and retention, are documented and compliance with these policies is assessed.			
Action examples	**Position responsible**	**Due**	**Status**
Categorise the types of personal information you collect and hold			
Complete a data inventory of the personal information you collect and hold			
Assign data owners to your various datasets and categories of personal information			
Create and maintain a log of any information sharing agreements (MoU, AISA, information matching programmes)			

Privacy Commissioner
Te Mana Mātāpono Matatapu

Security and Internal Access Controls			
Key objectives			
• Security controls are specific to the type and sensitivity of information held across the organisation, rather than a 'one size fits all' approach. • Regular auditing of systems is undertaken to ensure appropriate access. • Organisation follows industry guidelines and security standards relevant to its business context. • There is a remediation plan for managing and/or replacing legacy systems (where necessary). • Identified risks are proactively managed. For example, by incorporating them into the organisation's risk and assurance reporting processes to ensure visibility. • Organisational controls (i.e. policies, procedures, and decisions) are regularly reviewed and fit for purpose.			
Action examples	**Position responsible**	**Due**	**Status**
Ensure staff understand their privacy obligations and access controls relevant to their role			
Develop processes and procedures for managing staff access to facilities and systems			
Establish and maintain a log of user access to systems holding personal information			
Develop and maintain system operating procedures that document the security arrangements and controls in place to protect the data held within systems and applications			
Monitor and address new security risks and threats			

Privacy Commissioner
Te Mana Mātāpono Matatapu

Transparency			
Key objectives			
• The organisation can provide evidence about its privacy practices e.g. policies, processes, risk assessments, and statements. • Privacy notices and policies are reviewed regularly and kept up to date. • Privacy notices and statements are accessible and can be understood by their intended audience			
Action examples	**Position responsible**	**Due**	**Status**
Regularly monitor and review privacy processes, policies, and notices			
Ensure privacy policies are clear and easy for members of the public to access, including specific population groups where relevant e.g. children and young people, Māori, and Pasifika			
Document compliance with your privacy obligations e.g. keeping records of privacy policy and process reviews, risk and impact assessments, breaches, and complaints			

Privacy Commissioner
Te Mana Mātāpono Matatapu

Building Capability and Awareness			
Key objectives			
• Organisation has a role list with privacy training needs identified and training records for employees. • Appropriately trained people are available to deliver the training. • Training is received as part of induction and/or prior to gaining system access. • Trends identified in reporting of breaches and near misses are used to uplift capability in areas that need it (e.g. via training, refreshers, or targeted sessions).			
Action examples	**Position responsible**	**Due**	**Status**
Identify the training needs of all staff and use this information to develop a training programme			
Ensure staff receive induction training prior to accessing personal information			
Develop and maintain staff training records including completion dates, attendance rates, and training material for each group			
Keep a log of staff who need training refreshers and specialised privacy training for their role e.g. frontline staff, privacy function, trainers			
Participate in Privacy Awareness Week			

Privacy Commissioner
Te Mana Mātāpono Matatapu

Breach Management			
Key objectives			
• The organisation has a fully tested incident response plan. This means the plan is practiced in a mock situation. • The timeframe for deciding to report a breach, and reporting a breach, complies with OPC expectations. • Incident log records both actual breaches and near misses. • Staff know how to identify a possible breach and escalate to the appropriate person or team.			
Action examples	**Position responsible**	**Due**	**Status**
Assign roles and responsibilities for managing breaches and incidents			
Create and test an incident response plan			
Create and maintain an incident log for breaches and near misses			
Develop procedures and systems to facilitate the reporting of security incidents and breaches			
Undertake trend analysis on breach reports to understand themes and issues			
Report outputs of trend analysis to groups with oversight of privacy governance			

Privacy Commissioner
Te Mana Mātāpono Matatapu

Responding to requests and complaints well			
Key objectives			
• Complaints and access and correction request information is easily accessible to individuals • Organisation has clear escalation pathways for complaints and established processes for managing individual requests			
Action examples	**Position responsible**	**Due**	**Status**
Establish processes for individuals to easily access and correct their personal information			
Establish processes for receiving and responding to privacy enquiries and complaints			

Privacy Commissioner
Te Mana Mātāpono Matatapu

Assessing Risk			
Key objectives			
• Organisation has evidence of privacy assessment process, training, and completion of assessments. • There are policies and procedures on when and how PIAs/PRAs are completed, and who completes them. • Evidence that assessments have been used to design or review systems, products, services, processes or initiatives that use personal information.			
Action examples	**Position responsible**	**Due**	**Status**
Implement risk management processes to identify, assess and manage privacy risks across the business			
Adopt a 'privacy by design' approach			
Ensure staff training includes the need to consider a privacy risk assessment at the start of any project involving personal information			

Privacy Commissioner
Te Mana Mātāpono Matatapu

Measure and Monitor			
Key objectives			
• Systems and processes are in place for monitoring privacy practice, including performance indicators that are monitored for completion and reviewed when necessary. Measurement outcomes are regularly reviewed by the organisation's governance function to ensure they remain fit for purpose. • The organisation can demonstrate where performance has improved, and where monitoring has led to changes in practice/process/structure that have improved privacy outcomes. • Processes are in place to hear from staff about privacy issues.			
Action	**Position responsible**	**Due**	**Status**
Create channels for staff to provide feedback on privacy processes			
Measure your performance against your privacy management plan			
Establish processes for monitoring your privacy programme			
Select and use measures to communicate the state of your organisation's privacy practices and the effectiveness of your privacy programme			