information and privacy commission
new south wales

Desktop Review of Data Breach Policy (DBP) Compliance Report

May 2026

Contents

Executive Summary 3
1. Key Findings 4
2. Recommendations 4
3. Introduction 5
4. Observations and findings in respect of audit criteria 6
5. Abbreviations 12
6. Appendix A: Methodology 13
7. Appendix B: Legislation 15

Executive Summary

This report presents the key findings and recommendations from a desktop review of agency compliance with section 59ZD of the *Privacy and Personal Information Protection Act 1998* (PPIP Act). The review follows on from an earlier review which was published in October 2024 that examined the extent to which regulated entities had taken steps to meet the requirements of section 59ZD following commencement of the Mandatory Notification of Data Breach (MNDB) Scheme. Section 59ZD provides that all NSW public sector agencies must prepare and publish a Data Breach Policy (DBP).

Transparency and accountability are central to retaining and rebuilding public trust in the aftermath of a data breach. The NSW community expects that government agencies will handle their personal information safely and in accordance with the Information Protection Principles.

The DBP outlines how an agency intends to respond to a data breach incident, including the assigning of roles and responsibilities for managing a data breach. Importantly, it enables the broader NSW community to understand the current response mechanisms and how they align with the agency's obligation under the Information Protection Principles.

A DBP is an essential component of an agency's privacy governance framework. It provides the road map by which an agency will navigate its way through a data breach incident and ensure that in doing so, the agency complies with its obligations under the PPIP Act.

Having a robust DBP is not only essential for meeting regulatory and compliance obligations, but for also ensuring an effective and timely response to data breaches and maintaining community confidence in an environment where data breaches continue to rise.

Regularly reviewing and updating the DBP and ensuring that it is easily accessible on the agency's website enhances transparency and builds confidence and trust in the agency's ability to respond swiftly and effectively to a data breach.

While the findings detailed below are encouraging and reflect a welcome improvement on the previous report, the IPC will continue to engage with agencies across the regulated sectors to build agency capacity and maturity in policies and practices for data breach management. As a regulatory priority, the Privacy Commissioner will engage directly with agencies identified in the audit that have yet to prepare and publish a data breach policy despite a clear responsibility to do so. The responsibility under section 59ZD to prepare and publish a DBP is clear, is not optional, and should lead to visible action.

Sonia Minutillo

Privacy Commissioner

1. Key Findings

There has been an increase in agency compliance with section 59ZD

Seventy three percent of agencies had a publicly available DBP published on their website. This is a 17% increase from the finding of the previous audit.

However, 27% of agencies did not have a publicly available DBP on their website. Within this cohort, 27 agencies were found to not have a publicly available DBP in effect during each audit period.

Accessibility of DBPs has improved since the baseline audit

Of those agencies that had a publicly available DBP, 93% were found to be easily accessible. Though accessible, 7% of agencies were found to be partially compliant, with 6 to 10 navigations required within the agency's website to locate their DBP

Investment is required to improve and maintain currency of DBPs

Only 35% of DBPs reviewed included a publication or review date within the 12 months preceding this audit. The remaining 65% of sampled DBPs were either published or last reviewed more than 12 months ago or were subject to review cycles of between 2-5 years.

2. Recommendations

The recommendations made in this report are designed to bolster agency compliance with the MNDB Scheme and subsequent obligations. As an oversight agency, the IPC remains committed to assisting all NSW public sector organisations navigate the risk and harm/s associated with a data breach incident. This is reflected through the continual release of guidance materials, which aim to address emergent trends, patterns and agency limitations.

As the prevalence of data breaches increases, it is integral that agencies adapt and evolve their respective DBP frameworks to balance a proactive and reactive approach to data breach incidents. Further, the inclusion of an annual review cycle would ensure that a DBP remains current and effective. As a core element of an agencies response framework, it is imperative that this policy be viewed as a priority for all NSW public sector agencies.

Recommendation 1: Agencies that have not yet published a DBP should take immediate steps to prepare and publish a DBP in accordance with section 59ZD of the PPIP Act.

Recognising that some agencies have now been found to be non-complaint with the obligation under section 59ZD across two audits, the IPC will undertake targeted engagement with these agencies to address this non-compliance.

Recommendation 2: Agencies are reminded that the DBP is distinct and separate to a PMP. Noting the Scheme has been in effect for more than two years, it is recommended that agencies immediately take steps to progress their DBP from a section referenced within a PMP, to a comprehensive standalone policy.

Recommendation 3: Agencies should independently review their websites to assess the accessibility of their DBP with the aim to improve accessibility and discoverability.

Recommendation 4: Agencies should consider the digital literacy of all members of the community and/or incorporate a streamlined approach to website navigation, such as by the creation of a dedicated policy repository.

Recommendation 5: Agencies should consider implementing an annual DBP review process. This would increase currency and safeguard against redundant MNDB response protocols.

Recommendation 6: Where an agency has been the subject of a suspected or eligible data breach incident, a post incident review should be conducted. This should include a review of the DBP to ensure it remains fit for purpose.

3. Introduction

The Mandatory Notification of Data Breach (MNDB) Scheme was established under Part 6A of the PPIP Act.

Under the MNDB Scheme, NSW public sector agencies are required to notify the Privacy Commissioner and affected individuals of an eligible data breach. This ensures that appropriate oversight is provided regarding the agency's assessment and notification processes.

An eligible data breach occurs where:

- *there is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or a loss of personal information in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of the information, and*
- *a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates*

The MNDB Scheme requires that an agency have a DBP that outlines the practices and procedures the agency will follow to comply with its obligations under the Scheme. The DBP informs both staff and the public about the steps that will be taken by the agency if it experiences a data breach. It is a requirement of the PPIP Act that all NSW public sector agencies have a published DBP.

The absence of a DBP inhibits the community's ability to review and/or understanding how the agency intends to respond to a data breach incident.

Prior to the commencement of the MNDB Scheme in November 2023, the Information and Privacy Commission NSW (IPC) published a suite of resources to assist NSW public sector agencies prepare for the commencement of the Scheme. This included the publication of guidance on preparing a DBP[1].

A baseline audit was published by the IPC in October 2024 to measure and assess the DBP compliance of a sample of 93 NSW public sector agencies.[2] This audit identified that 47% of agencies did not have a publicly available DBP. Noting the sustained and transparent promotion of the IPC's MNDB resources, this result raised significant concerns regarding sector awareness and understanding of the scheme.

The current DBP follow up audit seeks to measure growth in agency maturity and Scheme compliance since the baseline audit in 2024 by assessing the existence, accessibility and currency of an agency's DBP as the MNDB Scheme has transitioned into a mature state of operation.

Comprised of a sample of 120 agencies, across four regulated sectors, this review expanded upon the IPC's previous audit activity via the inclusion of 27 additional agencies. Importantly, this review provided an opportunity to assess whether there have been improvements in public sector agencies' awareness and/or understanding of the DBP obligations since the release of the first compliance report in October 2024.

[1] Guide - Mandatory Notification of Data Breach Scheme: Guide to Preparing a Data Breach Policy

[2] Desktop Review of Data Breach Policy Compliance (DBP) Report

4. Observations and findings in respect of audit criteria

2.1. Is the Data Breach Policy published in the agency's website?

Criterion	Result	
1	Existence – is the Data Breach Policy published on the agency's website?	• 88 (73%) agencies were assessed as compliant. • 32 (27%) agencies did not have a DBP published on their website.

Comments, findings and recommendations

Comments: Noting the mandatory obligation under section 59ZD of the PPIP Act, it is expected that all NSW public sector agencies have a DBP published on their website. In measuring the existence of DBPs on agency websites, agencies were assessed on a strictly 'compliant' or 'non-compliant' basis.

Findings: Compliance has improved since the previous audit, with 88 (73%) agencies having a DBP in effect. Of this figure, 18 agencies were found to have transitioned into a compliant state since the 2024 audit activity.

27% of agencies were assessed as non-compliant, with the DBP of 32 agencies not located (**figure 1**).

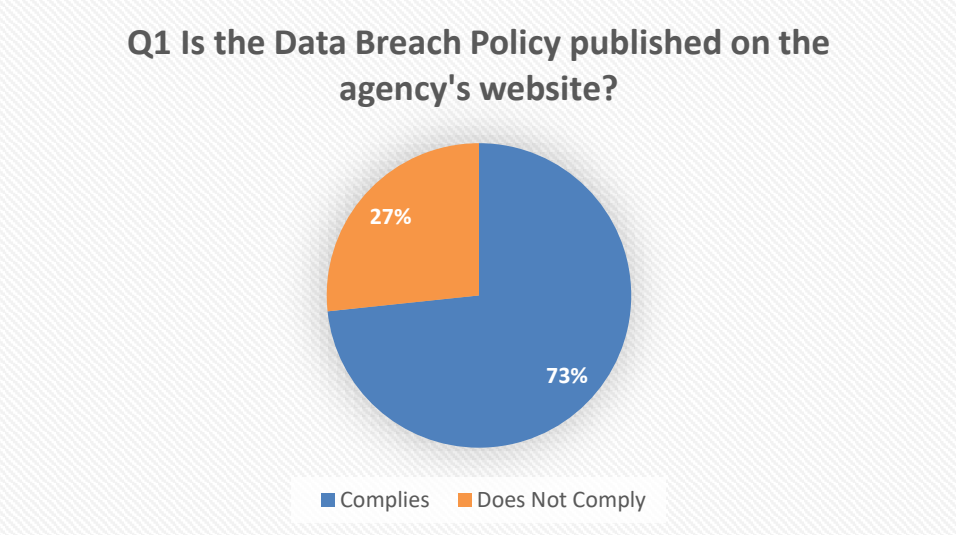


Figure 1

Recording a compliance rate of 90%, the university sector was identified as the most compliant. Consistent with the 2024 review, non-compliance appears to be concentrated within the Council sector, with 13 Local Government Areas (LGA) not having a published DBP (**figure 2**).

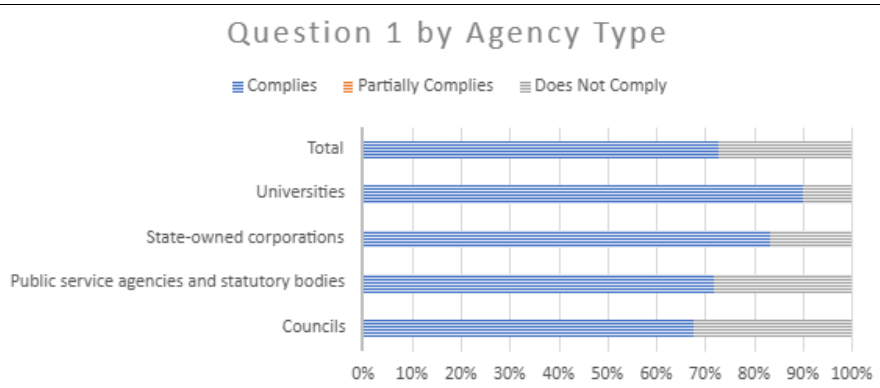
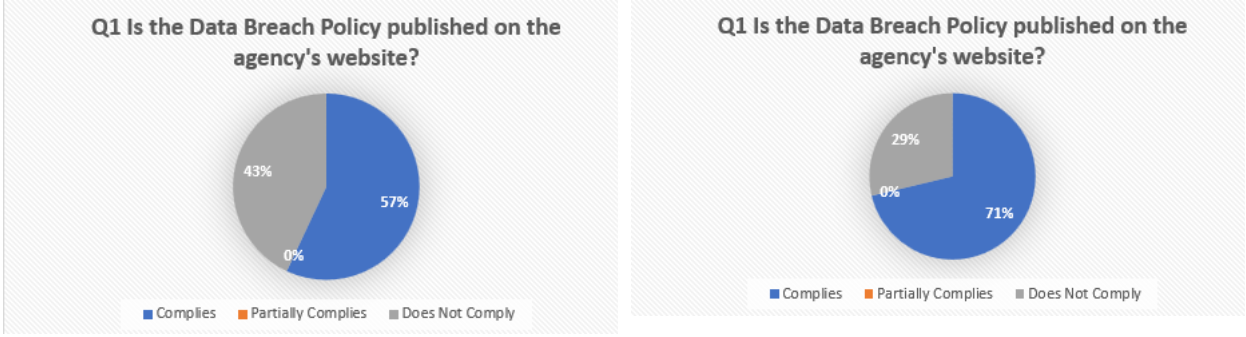


Figure 2

While an agency's geographical location does not preclude them from the legislative obligation, this is considered when dissecting the dataset. Of the 13 Council's identified as non-compliant, the majority were classified as rural or remote.

Comparatively, the number of agencies that had a published DBP has grown by 17% between the 2024 and 2026 audit period (**figure 3**).



2024 **2026**

Figure 3

Though the increase in compliance is encouraging, it remains evident that a small proportion of NSW public sector agencies remain non-compliant with the obligation to create and publish a DBP distinct from an agency's Privacy Management Plan (PMP). The 2026 audit observed that, in five of the sampled agencies, the DBP was represented as a section within another policy, generally this was the PMP developed pursuant to section 33(c)(1) of the PPIP Act. The inclusion of the DBP in another document or policy does not align with the obligations to prepare and publish a DBP under section 59ZD.

Recommendation 1: Agencies that have not yet published a DBP should take immediate steps to prepare and publish a DBP in accordance with section 59ZD of the PPIP Act.

Recognising that some agencies have now been found to be non-complaint with the obligation under section 59ZD across two audits, the IPC will undertake targeted engagement with these agencies to address this non-compliance.

Recommendation 2: Agencies are reminded that the DBP is distinct and separate to a PMP. Noting the Scheme has been in effect for more than two years, it is recommended that agencies immediately take steps to progress their DBP from a section referenced within a PMP, to a standalone policy.

2.2. Is the Data Breach Policy easily locatable on the agency's website?

Criterion	Result	
2	Accessibility - Is the Data Breach Policy easily locatable on the agency's website?	• Of those agencies with a published DBP, 82 (93%) had an easily accessible DBP. • 6 (7%) agencies were found to be partially compliant.

Comments, findings and recommendations

Comments: Section 59ZD requires that the agency make its DBP publicly available by publishing to the agency's website. This is achieved by publishing the DBP via the agency's website. By making its DBP easily discoverable, an agency contributes to and promotes transparency, as well as building trust and confidence in its management of a data breach.

Where an agency was assessed as 'compliant' for criterion 1, consideration was then given to the accessibility of their DBP. Accessibility was measured through the number of navigations or click throughs required from the agency's homepage to locate the document.

Findings: Despite the variability in website design and layout observed across the sectors, the audit identified a high rate of compliance across all sectors. Overall, 82 (93%) of the sampled agencies that had a published DBP were determined to have an accessible DBP, with the majority requiring between 1 to 2 navigations to locate the DBP.

Partial compliance was found across both the public service and university sector, with 6 (7%) agencies requiring more than 5 navigations (**figure 4**).

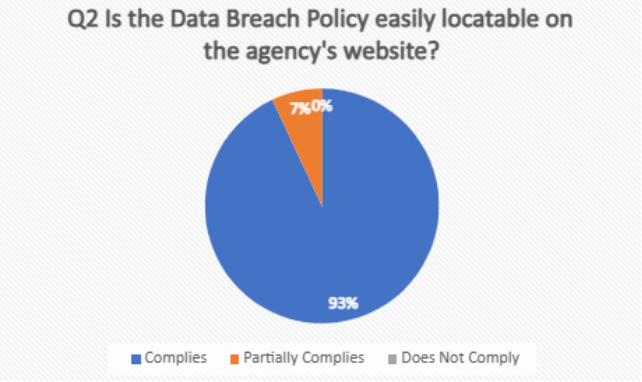


Figure 4

Contrasting presentation styles were identified, reflecting the variability in website design and layout observed across the sectors. A significant portion of agencies were found to have alphabetised their respective policy repositories, facilitating ease of access to policy documents including the DBP.

For some agencies, a 'title word' search was required to locate the DBP, either via the website's internal search function or, in a smaller number of cases, via an external search engine. Although, this search strategy returned a positive result and enabled the DBP to be located, it does suggest that website layout for some agencies does not facilitate ready access to the DBP.

When publishing a DBP, it is important to consider both the digital literacy and familiarity of the broader community with the layout and design of government agency websites.

Ensuring that individuals are aware of and/or afforded the opportunity to access an agency's policy and procedural documentation is crucial to maintaining public trust and organisational accountability.

Access limitations were found to exist amongst the Public Service and University sectors, with more effort required to successfully locate the DBP. Notably, where a Public Service agency's website is administered through a centralised interface considerable effort was required to locate the DBP. For these agencies a title word search inclusive of the agencies name was required. The absence of a distinct policy tab on the relevant website reduced the overall accessibility of the DBP.

In comparison, agencies located within the Council and State-owned Corporation (SOC) sectors recorded a higher rate of accessibility (**figure 5**). This may be reflective of the widespread adoption of a dedicated and alphabetised policy repository/library by these agencies. This type of streamlined approach to website navigation is consistent with the obligation to promote and facilitate open access to government information

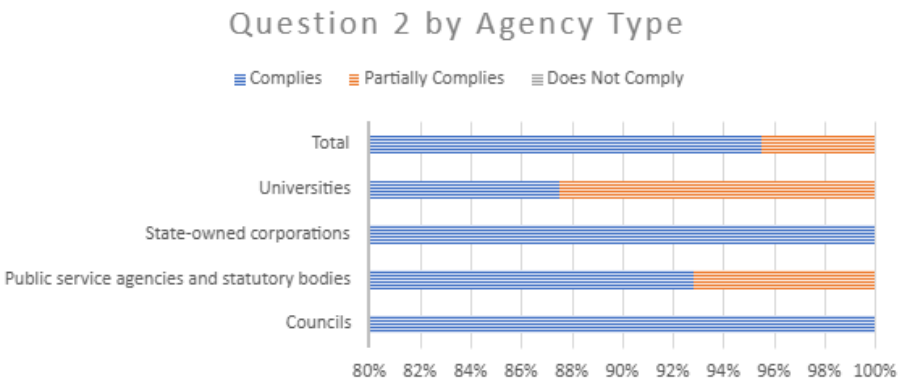


Figure 5

Following the notification of a data breach incident, an affected individual may elect to review the agencies DBP. As the entity responsible for minimising the potential harm associated with the incident, it is important that access to the data breach management framework be accessible and considerate of the various search methodologies by the broader community.

Recommendation 3: Agencies should independently review their websites to assess the accessibility of their DBP with the aim to improve accessibility and discoverability.

Recommendation 4: Agencies should consider the digital literacy of all members of the community and/or incorporate streamlined approach to website navigation, such as by the creation of a dedicated policy repository.

2.3. Does the Data breach Policy include a publication or review date within the last 12 months?

Criterion	Result	
3	Currency – Does the Data Breach Policy include a publication or review date within the last 12 months?	• 31 (35%) agencies were found to be compliant. • 58 (65%) agencies had a publication or review date outside of the 12-month audit period.

Comments, findings and recommendations

Comments: To ensure that its DBP remains effective and fit for purpose, it is vital that agencies adopt a process for continuous improvement. The DBP should be subject to regular testing and review to ensure that the DBP operates as intended when activated during a data breach incident. Regular periodic review, as well as review post-data breach incidents, ensures that the agency's DBP remains fit for purpose and considers any emerging patterns or vulnerabilities associated with a data breach incident.

To examine the currency of a DBP, the sampled agencies were assessed against 'compliant' or 'non-compliant' criteria.

Findings: Noting the absence of a mandatory requirement, only 31 (35%) agencies had proactively reviewed and/or published a DBP within the 12 months preceding this audit.

In comparison, 57 (65%) agencies had not reviewed their DBP (**figure 6**).

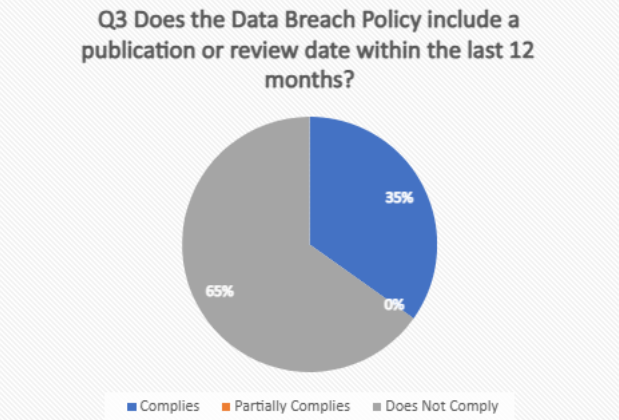


Figure 6

Compliance appeared to be consistent across the NSW Public service, SOC and Council sectors, at 55% 50% and 50% respectively. In the context of universities, this rate decreases to 25%, with only 3 of the twelve agencies having a DBP that was reviewed or published in the preceding 12 months (**figure 7**).

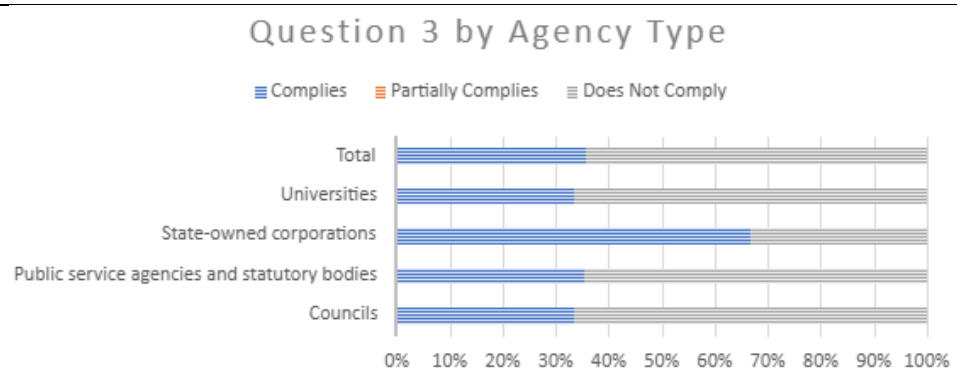


Figure 7

Overall, it appears that 25 (15%) agencies have not reviewed their DBP since 2023, with a further 19 (11%) of agencies reviewing or first publishing their respective DBP policies in 2024.

The frequency of review cycles varies, with most agencies appearing to operate on a two-year basis. In the context of the Council sector, this extends to a review cycle of between four to five years. While consideration to an agencies cyclic review period was given, where the nominated timeframe resided outside of the scope, it was deemed non-compliant with the criterion. This ensured that the data collated throughout the audit remained an accurate depiction of the agency review process.

A robust and effective DBP is integral for all NSW public sector agencies. The policy outlines how an agency intends to prepare for and respond to an incident of unauthorised access to and disclosure of personal information. By introducing either an annual or post incident DBP review process, an agency would benefit from the key learnings derived from such procedures, primarily as it presents an opportunity to strengthen internal controls on both a proactive and reactive basis.

Recommendation 5: Agencies should consider implementing an annual DBP review process. This would increase currency and safeguard against redundant MNDB response protocols.

Recommendation 6: Where an agency has been the subject of a suspected or eligible data breach incident, a post incident review should be conducted. This should include a review of the DBP to ensure it remains fit for purpose.

5. Abbreviations

The following table lists the commonly used abbreviations within this report.

Acronym or abbreviation	Explanation
PPIP Act	*Privacy and Personal Information Protection Act 1998*
IPC	Information and Privacy Commission NSW
MNDB Scheme	Mandatory Notification of Data Breach Scheme
DBP	Data Breach Policy
PMP	Privacy Management Plan

6. Appendix A: Methodology

This review was undertaken in accordance with the Privacy Commissioner's functions pursuant to section 36 of the PPIP Act.

Between 17 February and 24 February 2026, a desktop review of 120 NSW public sector agencies was undertaken.

A representative sample of 120 agencies were selected for inclusion across four regulated sectors. The sample size was increased from the 2024 review to encompass a greater number of agencies within the NSW Government and Council sectors. This change reflects the larger size of these sectors and the facts that these sectors are responsible for a greater proportion of notified data breaches under the Scheme.

The audit reviewed the DBP existence, accessibility and currency of the following agency t7pes:

- 52 NSW Government agencies (standalone)
- 6 State-owned corporations
- 10 Universities
- 52 Councils (metropolitan, regional and rural)

To assess agency compliance, the audit focused upon the following three (3) key elements:

- **Existence**: Whether the agency had published a DBP following the 2023 implementation of the MNDB Scheme.
- **Accessibility:** The overall accessibility of the DBP - calculated through the number of navigations required to view the DBP.
- **Currency**: DBP currency – whether the document had been subject to a review within the preceding twelve (12) month period.

To calculate compliance, agencies were assessed against the following rubric:

Existence	Complies	Partially complies	Does not comply
Is the Data Breach Policy published on the agency's website?	Yes, document is published on the agency website	N/A	No, unable to identify document published on the agency website
Accessibility			
Is the Data Breach Policy easily locatable on the agency's website?	Document located within 5 navigations from the homepage or the 'Privacy' page	Document located within 6 to 10 navigations from the homepage or the 'Privacy' page	Document located within 10 or more navigations from the homepage or the 'Privacy' page
Currency			
Does the Data Breach Policy include a publication or review date within the last 12 months?	Document includes a publication or review date within the last 12 months	N/A	No publication or review date within the last twelve 12 months.

Where an agency was assessed as non-compliant for DBP existence, the agency was excluded from the accessibility and currency assessment criterion.

Limitations

Consistent with the approach adopted for the 2024 review, this review focuses on sector-wide compliance rather than individual agency compliance. As such it was determined that a desktop review remains the most appropriate and efficient method to measure compliance levels across the sectors. This approach enabled the IPC to measure any improvements or deteriorations in compliance rates across the sectors as measured against the baseline data presented in the 2024 review.

The approach was limited to a desktop review, with no direct engagement/s conducted. This is consistent with the methodology deployed during the 2024 baseline compliance audit. Consideration was only afforded to the existence, accessibility and currency of a DBP, with the content of the DBPs not reviewed.

Due to the holistic and/or remote nature of the review, the following limitations are acknowledged:

- Whether the DBP was publicly available between the 17 February and 24 February 2026 audit period.
- Th absence of a legislative requirement to review and/or annually update a DBP.
- Exclusion of an agency's Privacy Management Plan (PMP). The focus remained on the DBP, irrespective of whether it was referenced within an agency's PMP.
- Forfeiture of complete scoring. Where an agency is identified as non-compliant for 'existence', an assessment for 'accessibility' and 'currency' is not possible.
- Potential impacts upon an increased data set. The audit increased the sample size by 27 agencies.

It is further acknowledged that a DBP published and/or reviewed outside of the audit timeframe will not be reflected within this report.

Audit chronology

Date	Event
16 February 2026	Desktop Audit commenced
23 February 2026	Desktop Audit completed
25 February 2026 – 9 March 2026	Analysis and Report Drafting
9 March 2026 – 20 May 2026	Final Report Review Period
27 May 2026	Final Report Published

7. Appendix B: Legislation

Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)

Part 4 Division 2 Functions of Privacy Commissioner

36 General functions

(2) In particular, the Privacy Commissioner has the following functions-

(e) to provide assistance to public sector agencies in preparing and implementing-

(ii) data breach policies under section 59ZD

Division 6 Other requirements for public sector agencies

59ZD Public sector agency to publish data breach policy

(1) The head of a public sector agency must prepare and publish a data breach policy.

(2) The policy must be publicly available.