Third Party Providers Privacy Risk and Assurance Framework

The type of personal information the provider may access when providing goods or services to the Ministry has been divided into five categories.

	None	***Limited***	***Moderate***	***Substantial***	***Extensive***
What access to personal information	Goods and service providers who do not require access to personal information to perform the contract. The provider should not need site access, and if they do, there is very limited potential for them to inadvertently or intentionally hear or see personal information. For example, provision of office supplies (stationary, food equipment) or office repairs (printer/lighting)	Goods and service providers who do not require access to personal information to perform the contract. However due to the nature of their work the service providers could potentially inadvertently or intentionally hear or see personal information (i.e. they come on Ministry sites). A breach of this type of information would have minimal impact on persons involved and limited short terms media coverage.	Service providers who have access to personal information in the scope of their work. However, they only receive partial information about Ministry staff or stakeholders. A breach of this type of information may have an impact on an individual, including emotional harm. National media coverage may occur.	Service providers who have access to detailed and/or sensitive personal information. This includes sensitive health information and information about vulnerable children and their families. A breach of this information may result in significant emotional harm or affect personal safety. This category includes all providers who have access to Ministry systems.	Service providers who have access to highly sensitive personal information. A breach of this information may result in ham to Ministry stakeholders, or high profile legal proceedings against the Ministry, or the Ministry being excluded from cross-government work programmes. This category includes all providers who have access to Ministry systems.
Examples	No access to any personal information held by the Ministry.	May overhear discussions about children accessing special education services, Ministry HR discussions or teacher payroll information.	Access to sensitive information such as staff addresses, bank account numbers, teacher's payroll information, student addresses.	Student achievement information. Staff employment information including disciplinary records, EAP information, salary information.	Information about individuals subject to protection/ harassment/family court orders. Health information. Social Services interventions. Information provided to the CAP Teams and Social Sector Trials.

Assurance Map

Each provider is assessed according to two criteria (type of information and volume of information accessed over the course of their contract). This puts them into one of four categories and determines the amount of assurance over personal information they will be required to provide.

Volume

2,000 +					
251-2000					
101-250					
21-100					
1-20					
	None	Limited	Moderate	Substantial	Extensive

Extent of access to personal information

Dark blue: High level of assurance required
Medium blue: Medium level of assurance required
Light blue: Low level of assurance required
Green: Very low level of assurance required

Assurance Requirements

Assurance Map Outcome	Form of Assurance Required
Green: Very low level of assurance required	Contract includes clauses requiring: • Compliance with the Privacy Act 1993. • Compliance with the Health Information Privacy Code and other relevant codes relating to the handling of personal information. • Right for the Ministry to audit provider when requested.
Light blue: Low level of assurance required	During the contracting process the provider will be required to sign a form confirming they: • Understand and will conform to the requirements of the Privacy Act, Health Information Privacy Code and other relevant codes. • Understand the significance of personal information and have appropriate controls in place to manage personal information. • Will report all privacy incidents to the Ministry's Privacy Officer within 24 hours of the incident occurring. The contract must include clauses requiring: • Compliance with the Privacy Act 1993. • Compliance with the Health Information Privacy Code and other relevant codes relating to the handling of personal information. • Right for the Ministry to audit provider when requested.
Medium blue: Medium level of assurance required	During the contracting process the provider will be required to sign a form confirming they: • Understand and will conform to the requirements of the Privacy Act, Health Information Privacy Code and other relevant codes. • Understand the significance of personal information and have appropriate controls in place to manage personal information. • Will report all privacy incidents to the Ministry's Privacy Officer within 24 hours of the incident occurring. During the contracting process, the provider will be required to: • Provide the Ministry with a copy of their privacy policy for the Privacy Officer to review. If they do not have one, they will be required to describe their plans to develop one and any mitigating controls currently in place. • Provide evidence that privacy is adequately included in their assurance plan (for example, internal audit reports). The contract must include clauses requiring: • Compliance with the Privacy Act 1993. • Compliance with the Health Information Privacy Code and

	other relevant codes relating to the handling of personal information. • That the Ministry has the right to audit the provider when requested. • When requested, the provider will complete a privacy survey. • The provider cannot sub-contract without getting permission from the Ministry first. • The provider will report all privacy incidents to the Ministry's Privacy Officer within 24 hours of the incident occurring.

Dark blue: High level of assurance required	During the contracting process the provider will be required to sign a form confirming they: • Understand and will conform to the requirements of the Privacy Act, Health Information Privacy Code and other relevant codes. • Understand the significance of personal information and have appropriate controls in place to manage personal information. • Will report all privacy incidents to the Ministry's Privacy Officer within 24 hours of the incident occurring. During the contracting process, the provider will be required to: • Provide an up-to-date privacy framework which includes a staff training programme and a breach reporting process. The Ministry has the right to audit and request random spot checks regarding privacy management. • Provide the Ministry with a copy of their privacy policy, which includes breach/incident definitions and a Privacy Officer, for the Ministry Privacy Officer to review. If they do not have one, they will be required to describe their plans to develop one and any mitigating controls currently in place. • Provide evidence that privacy is adequately included in their assurance plan (for example, internal audit reports). The contract must include clauses requiring: • Compliance with the Privacy Act 1993. • Compliance with the Health Information Privacy Code and other relevant codes relating to the handling of personal information. • That the Ministry has the right to audit the provider when requested. • When requested, the provider will complete a privacy survey. • The provider cannot sub-contract without getting permission from the Ministry first. • The provider will report all privacy incidents to the Ministry's Privacy Officer within 24 hours of the incident occurring. • That the Ministry has the right to audit and request random spot checks regarding privacy management • That the Ministry has the right to review the privacy framework following a privacy incident. • That the Ministry has the right to hold mandatory privacy meetings/ workshops between the Ministry and the provider once a quarter or following a privacy incident. • That the provider holds periodic assurance reporting on the effectiveness of the privacy framework.

Acknowledgement

Thanks to the Department of Corrections for the use of their Privacy Assurance Framework