Independent privacy evaluation for [Provider name] and [Service name]

[Date]

V1.1 February 2025

# Contents

[About this guidance 1](#_Toc185247823)

[Structure of the evaluation 2](#_Toc185247824)

[Introduction 4](#_Toc185247825)

[Evaluation details 4](#_Toc185247826)

[Privacy evaluation 5](#_Toc185247827)

[Information used to inform your evaluation 13](#_Toc185247828)

[Appendix A – Additional evidence 14](#_Toc185247829)

# About this guidance

As regulator, the Digital Identity Services Trust Framework Authority (the Trust Framework Authority) assesses and accredits providers, and their services, against the Trust Framework rules and regulations.

Independent privacy evaluators play a role in the evaluation of providers seeking accreditation under the Digital Identity Services Trust Framework (the Trust Framework).

Independent privacy evaluators provide an evaluation on whether the provider meets the requirements of:

* section 9(e) of the [Digital Identity Services Trust Framework Regulations 2024](https://www.legislation.govt.nz/regulation/public/2024/0197/latest/whole.html#LMS989657); and
* service standards and processes set out in Part 4 of the [Digital Identity Services Trust Framework Rules 2024.](https://www.dia.govt.nz/diawebsite.nsf/Files/Trust-Framework/$file/DISTF-Rules-2024.pdf)

The Trust Framework Authority will make the final assessment and accreditation decision.

If you have questions about the evaluation process or this guidance, or need assistance, please contact [TFA@dia.govt.nz](mailto:TFA@dia.govt.nz).

# Structure of the evaluation

This template is for use by independent privacy evaluators. Text in blue provides guidance for completing the evaluation and can be removed from the final version.

The provider will:

* select an Independent Evaluator to use from the list of approved evaluators supplied by the Trust Framework Authority on the [independent evaluators](https://www.dia.govt.nz/Trust-Framework-for-Digital-Identity-Independent-evaluators) webpage
* agree pricing with the Independent Evaluator
* send the completed Trust Framework Authority privacy application form and attachments to the Independent Evaluator
* respond to any questions or requests for additional information from the Independent Evaluator
* submit the completed evaluation and all materials used to complete the evaluation to the Trust Framework Authority for assessment.

The Independent Evaluator will:

* agree pricing with the provider
* receive a completed Trust Framework Authority privacy application form and attachments from the provider
* ask for any follow up information needed to complete the evaluation from the provider
* use the application form and attachments to complete the evaluation
* need to request additional information from the provider or ask for clarification from the provider.

**Inputs to the evaluation**

When completing your evaluation please save copies of all documentation that you use. This should include:

* Any additional documents that you request from the provider.
* Any screen shots you take of the provider’s system(s).
* Notes you make of discussions or interviews with representatives from the provider.

These must be listed in the section on information used to inform your evaluation, and given to the provider for them to submit to the Trust Framework Authority as part of their accreditation application .

**Sections of the evaluation**

|  |  |
| --- | --- |
| Section | Description |
| Evaluation details | Summary details about the evaluation, such as the name of the Independent Evaluator, organisation they work for, and date that the evaluation is completed. |
| Privacy evaluation | Detailed evaluation of the information provided in the privacy application form and attachments. |
| Information used to inform your evaluation | A summary of all inputs used by the Independent Evaluator to inform their evaluation. |

# Introduction

This document records the privacy evaluation for [Provider name] for [Service name].

## Evaluation details

| Evaluation details | |
| --- | --- |
| Provider |  |
| Date submitted |  |
| Service name |  |
| Services applied for |  |
| Evaluator |  |
| Evaluator Organisation |  |
| Date evaluation completed |  |
| Template version | V1.1 |

# Privacy evaluation

#### Responsible person

|  |  |  |  |
| --- | --- | --- | --- |
| Aim | Evaluation checklist | Yes/No | Comments |
| Meet Rule 12(5): The provider has a nominated person responsible for privacy | The provider has supplied the name of an appropriate person as the nominated person responsible for privacy. |  |  |

#### Privacy training

This question will be answered by questions 2 and 3 of the TF Authority privacy application form.

| Aim | Evaluation checklist | Yes/No | Comments |
| --- | --- | --- | --- |
| Meet Rule 12(6): All staff and contractors with access to personal information of service users receive regular training on privacy policies | 1. Staff are required to complete privacy training. 2. The training covers both employees and contractors. 3. That training is relevant to the job the staff member does, and the level of the information they must handle. (The more sensitive the information, the more detailed the training requirements). 4. The training must at least cover:  * lawful purposes and uses for personal information collected and held by the provider * how to handle requests for access or correction * processes regarding storage and disclosure of information * what to do if there is a privacy complaint or incident, including reporting them to the designated privacy contact. |  |  |

#### Privacy statement

|  |  |  |  |
| --- | --- | --- | --- |
| Aim | Evaluation checklist | Yes/No | Comments |
| Meet Rules 12(1) and 12(11). | 1. The provider must have a privacy statement. 2. The privacy statement must be made available to users in accordance with IPP3 and must be appropriate for the service. 3. The contents of the privacy statement are consistent with IPP3. |  |  |

#### Documents to provide

#### Privacy policy

| Aim | Evaluation checklist | Yes/No | Comments |
| --- | --- | --- | --- |
| Meet Rule 12(6) and 12(7) | 1. The provider has supplied a copy of their privacy policy/policies that has been supplied to their personnel. 2. Personnel will be informed of any changes to that policy/those policies. 3. The privacy policies are appropriate, and include the:  * lawful purposes and uses for personal and organisational information collected and held by the provider; and * processes to amend or update a user’s personal or organisational information when requested by that user; and * processes regarding storage and disclosure of information; and * privacy complaints and incidents procedures. |  |  |

#### Privacy Incident Response Plan

| Aim | Evaluation checklist | Yes/No | Comments |
| --- | --- | --- | --- |
| Meet Rules 12(8), 12(9), Regulation 20 and part 6 of the Privacy Act | 1. The provider has a documented privacy incident response plan and maintains that plan. 2. The plan must reflect both what to do in the case of a notifiable breach and less significant breaches or near misses. 3. The plan must at least:  * clearly assign roles and responsibilities when an incident occurs * set out escalation and notification processes * describe processes to contain and assess the incident * ensure that the Privacy Commissioner and affected individuals are notified of any notifiable privacy breaches (in accordance with the Privacy Act 2020) * ensure that any privacy breaches related to an accredited service are reported to the TF Authority as soon as the provider is practically able to do so. |  |  |

#### Privacy Incident Register

| Aim | Evaluation checklist | Yes/No | Comments |
| --- | --- | --- | --- |
| Meet Rules 12(10) and 12(9) | 1. The provider has a Privacy Incident Register and provides instructions for personnel to record privacy incidents. 2. The incident register is reviewed regularly and applicable processes and policies are updated accordingly. |  |  |

#### Privacy Impact Assessment

Assessed by either reviewing an existing Privacy Impact Assessment and asking questions and validating controls, or developing a Privacy Impact Assessment for the provider

| Aim | Evaluation checklist | Yes/No | Comments |
| --- | --- | --- | --- |
| Meet Rule 12(2): TF provider must complete a PIA | The provider must complete a Privacy Impact Assessment (PIA) for the digital identity service for which they intend to apply for accreditation and supplied it to the independent assessor. |  |  |
| Ensure that the provider is properly aware of and accepts the responsibilities set out in the PIA | The Privacy Impact Assessment has been formally approved by the provider. |  |  |
| Contents of the PIA cover matters set out in Rule 12(3), and matters required under the Privacy Act | The PIA clearly describes:   * the service or services being provided * information already held and new information to be collected * the specific purpose/s for which the personal information is collected and/or used * the information flows (either in diagram or text format) * how information will be stored, accessed, and disposed of by the accredited provider * the privacy risks that the service creates or may create (at a minimum, the privacy risks noted elsewhere in this assessment) * what controls are in place to mitigate those risks. |  |  |
| Meet Rule 12(4) Ensure the PIA is reviewed and updated | 1. The PIA includes a date by which the PIA must be reviewed, which is no later than 2 years after the date on which the PIA was last reviewed. 2. The PIA states that the PIA will be reviewed earlier than that set date if there is a change to the digital identity service. 3. The provider has a mechanism to ensure that the review will happen as stated in the PIA. 4. Check the status of the actions in the Privacy Impact Assessment. |  |  |
| [Meets s32 of the Privacy Act 2020](https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23365.html?search=qs_act%40bill%40regulation%40deemedreg_privacy_resel_25_h&p=1) | If there is a relevant Code of Practice, the specific Code of Practice is sufficiently taken into account within the PIA. |  |  |

# Information used to inform your evaluation

| **No** | **Question** | **Information used to inform your evaluation** | |
| --- | --- | --- | --- |
| **Information supplied by the provider** | **Additional information gathered by the evaluator as part of the evaluation** |
| 1 | Responsible person | Application response |  |
| 2 | Privacy training | Application response |  |
| 4 | Privacy statement | Application response |  |
| 5 | Privacy Policy | Application response |  |
| 5.1 | Privacy Incident Response Plan | Application response |  |
| 5.2 | Privacy Incident Register | Application response |  |
| 5.3 | Privacy Impact Assessment | PIA |  |
| 5.4 | Assessment against IPPs | PIA |  |

Appendix A – Additional evidence

The following evidence was provided to support the evaluation, which is relevant to this evaluation.

You may include here any of the following that are not recorded in separate documents:

* Any screen shots you take of the provider systems.
* Notes you make of discussions or interviews with representatives from the provider.