



New Zealand Traveller Declaration

PRIVACY IMPACT ASSESSMENT

28/04/2022

Version 0.15

Contents

Document Management.....	3
Disclaimer and assumptions	3
Glossary.....	4
1. Introduction	6
2. Executive risk summary	7
3. Party roles	8
4. PIA scope	8
5. Personal information involved.....	9
6. Technical information	10
6.1 Information flows.....	10
6.2 Storage of the information	10
7. Support systems.....	11
7.1 Assisted Channels.....	11
7.2 Communication with travellers.....	13
7.3 Assurance and governance	14
7.4 Enforcement systems to support the NZTD objectives	14
8. Assessment of privacy impacts	14
8.1 Collection of personal information	15
8.2 Storage and Security	20
8.3 Access, correction and accuracy	21
8.4 Retention, use and disclosure.....	23
8.5 Offshoring of Information	26
8.6 Unique Identifiers	26
Appendix 1 - Project Risks.....	0
Appendix 2 – Non-Technical Controls and Control Validation	1
Appendix 3 – Technical Controls and Control Validation	3
Appendix 5 – Enforcement - TBC	8
Appendix 6 – Contact Centre identity verification processes.....	9
Identity verification processes.....	9
Identity Verification – Level 2 and 3 calls	9

Document Management

Version History

Version	Date	Author and role	Description
0.8	05/02/2022	Benjamin Scully	Author. Redrafted following shift in accountabilities for agencies (no longer s 11 reliance).
0.9	09/02/2022	Benjamin Scully	Responding to internal feedback.
0.10	21/02/2022	Benjamin Scully	Responding to external feedback (MBIE, GCPO and MOH).
0.11	27/03/2022	Benjamin Scully	Author. Redrafted following shift in cabinet decisions (March) and decision to rely on ABO more heavily.
0.12	31/03/2022	Benjamin Scully	Redrafting and responding to feedback on v 0.11 (8 sets of feedback).
0.13	01/04/2022	Benjamin Scully	Clean version. Only outstanding questions for project team remain.
0.15	28/04/2022	Benjamin Scully Kevin Linnane	Responses to OPC Questions from 13/04/2022 and 27/04/2022 as well as meeting on 12/05/2022.

Distribution List for External Distribution

Version # Sent	Date Sent	Recipient email address.	Reason for sending
0.9	11/02/2022	Total project list.	Feedback following completion of Accountabilities paper and new formulation of this PIA.
0.11	29/03/2022	Fiona W, Ed B, Siobhan H-P, Patrick T, Rebecca J, Mary G, Andrew N, Francesca H.	Consultation prior to OPC consultation. Each recipient responsible for their own team / org. review.

Disclaimer and assumptions

This PIA has been prepared by Customs, MOH, and MBIE (INZ and MIQ specifically).

This PIA has been prepared to review the purposes of information collection for and by the New Zealand Traveller Declaration (**NZTD**) applications, the uses and disclosures of that information, and the safeguards applied and required to manage those purposes, uses, disclosures and retention.

This PIA reflects the operation of the NZTD as it is currently envisaged. It is intended to be a “living document” and will be regularly updated to reflect changes that arise as the NZTD is progressively rolled out and adapted to respond to changes in the broader environment.

The assumptions applied in the development of this assessment are that:

- Relevant changes to the Air Border Order (**ABO**) will result in a review of any consequential privacy implications caused by those changes to the NZTD operating at that point in time, and that the change to the ABO will remain consistent.
- A version of this PIA will be made publicly available alongside the communication collateral deployed with the NZTD. This will support the public to understand the collection, storage, use and sharing of personal and third-party information. This is a transparency decision, intended to support public trust in the operation of the NZTD.

Glossary

Abbreviation	Meaning
ABO	The COVID-19 Public Health Response (Air Border) Order 2021 (promulgated through the Gazette Notice) available at New Zealand Legislation .
APP	Advance Passenger Progressing. Airlines must provide Advance Passenger Processing (APP) information to INZ about every passenger and crew member on their flights coming to or leaving New Zealand. Changes as part of tranche two will look to allow a broader set of agencies to interact with airlines before boarding travellers.
Approved System	System specified by the Director-General of Health and approved by the Director-General for the purpose of a COVID-19 provision. NZTD is an approved System.
COVID-19	The novel coronavirus, see: https://www.health.govt.nz/our-work/diseases-and-conditions/COVID-19-novel-coronavirus .
Customs	New Zealand Customs Service
Director-General Notice	A notice made by the Director-General of Health in accordance with cl 59 of the ABO, or made under another COVID-19 Order. DG Notices are available at https://gazette.govt.nz/
INZ	Immigration New Zealand (part of MBIE)
IPP	Information Privacy Principle under section 22 of the Privacy Act
MBIE	Ministry of Business, Innovation and Employment
MIQ	Managed Isolation and Quarantine (part of MBIE)
MIQF	Managed Isolation and Quarantine Facility

MOH	The Ministry of Health
MPI	The Ministry for Primary Industries
NBS	The National Border Solution - MOH application that contains the operational and process details for managing progress of travellers from arrival at the border, testing during their stay, progress of a travellers stay in MIQ, and any contact tracing requirements. It is also available to support some aspects of self-isolation in the community after arrival of travellers to New Zealand.
Nau Mai Rā	<p>The information collection system that was the Approved System prior to NZTD becoming operational (in accordance with the relevant Notice under the ABO). This collected traveller declarations, contact details and other information as required by the relevant ABO Notice. It securely transmitted that information to NBS.</p> <p>Nau Mai Rā became obsolete as at 11.59pm 31 March 2022 as specified in an ABO Notice.</p>
NZeTA	New Zealand Electronic Travel Authority
PIA	Privacy Impact Assessment
QFT	Quarantine Free Travel. Travel to NZ which does not require a stay in MIQ on arrival and which may or may not require self-isolation on arrival.
Specified Information	Information that is collected by NZTD as set out in section 23, 24 and 25 of the ABO and specified by a Director-General notice. Specified Information needs to be provided to an Approved System – in this case, NZTD.

1. Introduction

1. Reconnecting New Zealanders was an approach announced by the Government in August 2021, defining a staged re-opening of the border through different risk-based entry pathways. In September, the Government approved a business case for the development and implementation of the New Zealand Traveller Declaration (NZTD) as the key administrative tool for operationalising the risk-based entry pathways.
2. NZTD does this by providing an electronic platform for travellers to declare their COVID-19 health and travel information such as vaccination status, COVID-19 test results and previous travel, if required in the ABO settings current at their time of travel, prior to travelling to New Zealand. There will also be an assisted channel for those who are digitally excluded, or who need accessibility support.
3. The health and travel information required from travellers may change from time to time depending on health settings agreed by Cabinet in response to COVID-19 risks. The requirements are expected to be publicly specified in the ABO, Director-General Notice, or other COVID-19 Notice.
4. Due to the complexity of NZTD and the surrounding environment, the system is intended to be rolled out through three key tranches. The NZTD was piloted in February and March 2022 to check operational functionality through a limited and 'opt-in' basis.
5. Initially managing air border arrivals to New Zealand from quarter one 2022, NZTD will subsequently be rolled out to maritime arrivals in tranche two. NZTD replaces Nau Mai Rā at 11.59pm on 31 March 2022 and will integrate with the other existing control systems in place to mitigate the risk of COVID-19 - the Managed Isolation Allocation System (MIAS), and the National Border Solution (NBS).¹

	Tranche One From Q1 2022	Tranche Two June 2022 - March 2023 (indicative)	Tranche Three November 2022 – June 2023 (indicative)
Functionality	<p>Electronic process for completing a health declaration.</p> <p>Automated verification of NZ/AUS Government issued and EU DCC vaccination certificates.</p> <p>Manual checking of other vaccination and testing certificates.</p>	<p>More country vaccination certificates automatically verified (where recognised).</p> <p>Further integration with airport systems (eGate, primary lines).</p> <p>Policy and legislative work on potential for APP² integration to enable health and</p>	<p>Integration of health declaration and Passenger Arrival Card.</p> <p>Ability to support pre-COVID-19 traveller volumes.</p>

¹ Until 14 April, Nau Mai Rā passes will be accepted in limited circumstances. Affected passengers will be contacted directly.

² Airlines must provide Advance Passenger Processing (APP) information about every passenger and crew member on their flights coming to or leaving New Zealand. This gives Immigration New Zealand advance notice about who is coming to New Zealand. Changes as part of tranche two will look to allow a broader set of agencies to interact with airlines before boarding travellers.

	<p>Automated risk assessment of a traveller's information against specified health criteria.</p> <p>Automated assigning of travellers to appropriate public health controls for their arrival. In some cases there will be 'conditional' and paper passes.</p> <p>Eligible travellers receive a notification to present at check-in and the border.</p>	<p>immigration boarding directives for all travellers.</p> <p>Incremental improvements to accessibility.</p>	
--	---	--	--

- This PIA is the first in relation to the NZTD project and only assesses Tranche 1. Tranches 2 and 3 will be assessed incrementally, as those developments are built, and implemented.

2. Executive risk summary

- The NZTD project is aligned with the suite of COVID-19 responses deployed at the border. This reflects the New Zealand Government's commitment to managing COVID-19. Privacy risks are similar in nature with those present elsewhere in the ongoing COVID-19 response.
- The following risks have been identified. Responsive controls have either been deployed or are in development. A detailed description of risks and controls can be found at **Appendix 1 Project Risks** and **Appendix 2 Controls and control validation**.

		Consequence				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Certain					
	Likely			R1		
	Possible				R4	
	Unlikely		R3	R2		
	Rare			R0		

- The Office of the Privacy Commissioner and the Government Chief Privacy Officer have been consulted and have provided comments on a draft PIA. The comments received from each of these agencies have been considered, and integrated. This final version of the PIA will, similarly, take Office of the Privacy Commissioner and Government Chief Privacy Officer feedback into account.

3. Party roles

10. Due to the scale and scope of government's COVID-19 response, the combined involvement and functions of several public sector agencies is necessary. Customs is leading the technical programme of work to develop the systems. MOH, Customs and INZ are contributing to associated policy decisions in consultation with other agencies, with the final decisions reflected in the ABO, and associated Director-General Notices.
11. Customs - leading the software development, technical build and deployment and administration of NZTD. Customs is also leading the response to complaints about the NZTD and may collect complaint information in this role. This PIA has been prepared by Customs. Both MOH and MBIE (INZ and MIQ) are supporting Customs in its role, which includes the ongoing identification and mitigation of privacy impacts and providing input to this PIA.
12. MOH – leading recommendations for the health settings and to the requirements on travellers that have a public health basis, with the final requirements to be incorporated into the relevant ABO and Notice provisions. The MOH will also maintain responsibility for the Health National Border System (NBS) where NZTD data will also be stored. Identifiable information is collected by the NBS to support the public health response to COVID-19, including management of border arrivals to meet applicable requirements under relevant Orders or Notices both at arrival and after arrival (including mandatory testing requirements at day 0/1 and 5/6) , contact tracing (which may reactivate in the case of a new variant at the borders) or to provide relevant public health related information, request participation in relevant surveys, and reporting and analysis (where reports produced will not contain any identifiable information)
13. INZ - outside of the technical build, INZ is providing a contact centre service for travellers who need support navigating the system, as well as contracting a third-party to provide surge and after-hours contact centre services. INZ also has oversight of Visa Application Centres which will offer an assisted fee-for-service channel to travellers who need it. Travellers can also nominate their own third-party, such as friends or family, to complete a declaration on their behalf. Finally, components of the NZTD system is being built on top of MBIE held systems.

4. PIA scope

14. The scope of this PIA includes:
 - a. The information collected from travellers for the NZTD;
 - b. How the information is to be collected, used, disclosed and stored.
15. This PIA does not review:
 - a. The choice of strategic direction of the NZTD, the policy analysis or legislative settings that reflect that direction;

- b. The creation of a vaccination certificate by MOH, the issuance of this token to New Zealanders and others who have been vaccinated in New Zealand (or later, in any other domicile) to be used to prove vaccination and testing status to foreign border authorities, or any associated privacy implications (as these are separately reviewed in independent PIA documentation such as the My Covid Record PIA);
- c. The creation of a vaccination certificate by Australia or other Sovereign Nations, the issuance of this token, or any associated privacy implications beyond the validation of a vaccination certificate by NZTD;
- d. The creation of a domestic vaccination certificate for New Zealanders and for travellers from other countries who may need a domestic vaccination certificate to attend events or visit certain venues in NZ;
- e. The National Border Solution, which is subject to its own PIA.³

5. Personal information involved

16. Much of the following information was collected via existing NBS and Nau Mai Rā processes. The Nau Mai Rā collection point has been replaced by NZTD, and the range of individuals the information will be collected from has changed under the upcoming changes to the ABO from 31 March 2022.⁴
17. This information can be described informally as falling into the following categories:
- a. Biographic or identity information;
 - b. Travel details;
 - c. Health information;
 - d. Contact information.
18. It is worth noting that this represents a limited expansion on information collected under the previous iterations of the ABO to facilitate previous pathway settings for QFT, and for the MIQF system if travellers need to quarantine when entering New Zealand. The primary distinction is that Nau Mai Rā, until the end of 2021, only collected information for QFT. This has been expanded under the ABO to capture those with no isolation conditions, which includes those required to meet self-testing requirements after their arrival or Pacific QFT. NZTD will collect information from all travellers regardless if they will need to quarantine or not. The only new information that the system will collect is:

³ A PIA for the NBS is available at [\[link\] placeholder for publication.](#)

⁴ Implemented by the COVID-19 Public Health Response (Air Border) Amendment Order (No 3) 2022 (SL 2022/76)

- a. Travel History which is already collected on the arrival card and required under the ABO.
- b. Proof of vaccination which is required under the ABO for persons 17 years or over who are not New Zealand citizens, and is already being collected by a number of air carriers;
- c. Proof of COVID-19 test which is required under the ABO;
- d. Date and time of departure, which is already collected under s 12 of the Customs Act.

19. A complete table of information collected by NZTD is attached at **Appendix 4**.

6. Technical information

6.1 Information flows

20. Information is captured from the traveller⁵ through two primary channels. These are the Web User Interface and the Bulk Loading Interface of the declaration system. The Web User Interface is the standard path of capture that travellers will use. There is also a paper based declaration system as a backup (**Control 10**) – this is being assessed through a separate short form PIA.
21. The Bulk Loading Interface has been established to more easily raise declarations on behalf of NZDF, RSE, Refugee and humanitarian travellers and to also support the Decision Review Process.
22. Information captured through each of these channels enters the platform through a series of application programming interfaces that receive, retrieve and process the information that is provided by travellers.
23. At various points in the process, the system will store the declaration in a database as a record of the declaration at that point. Similarly, the declaration will be sent to NBS at certain stages in its lifecycle in order to support health purposes discussed below at IPP 1.

6.2 Storage of the information

24. The information specified in accordance with clauses 23, 24 and 25 of the ABO (and detailed in the relevant [Notice](#)) is primarily stored in the MBIE Azure Cosmos DB.

⁵ Including through a support person, or on their behalf, as discussed at IPP 2 below.

Storage	Information
MBIE Azure Cosmos DB	Declaration Object Data extracted from the document Risk Assessment Results
MBIE Azure Object Store	Supporting Documents
Customs Azure Cosmos DB	Document metadata Data extracted from the document
Customs PostgreSQL DB	Declaration Object Health Rules Risk Assessment Results
Ministry of Health NBS	Declaration Object Risk Assessment Results

7. Support systems

25. The NZTD Contact Centre is being established as a standalone line that is serviced by the existing Immigration Contact Centre (ICC). To support 24/7 services, an external provider has been contracted to provide after hours and over-flow capability. At an architecture level, Business-to-Consumer has been selected to connect to the contact centre user interface, enabling the contact centre to access the traveller declaration.

7.1 Assisted Channels

26. A traveller will call the contact centre, the contact centre will login to the user interface, search using the declaration tracking number (all tracking numbers are 7 digits, randomly generated and allocated) or passport number, name, date of arrival or date of birth, and find the declaration and be able to assist. The UI will display all the relevant information that the traveller provides. This ensures that queries can be responded to.⁶

27. Processes – extracting datasets for Call Centre Agents

- a. The NZTD system includes an internal User Interface (UI) for call centre agents to be able to look up Declarations when supporting a caller.⁷ Access to the internal UI will be securely authorised (using standard Active Directory processes). External Contact Centre staff will be set up to access the system using “customer accounts” within the Active Directory.

⁶ A similar process is currently being developed for those reviewing decisions, so that they have all relevant information necessary for that review.

⁷ At the moment only the base declaration data is able to be viewed. It is hoped that in the near future this will be extended to support the viewing of uploaded documents.

- b. CSAs will be able to search for a specific NZTD using a combination of fields, including reference number, passport number, name and date of birth.
- c. The UI displays all information provided by the traveller, so that the CSAs can troubleshoot issues. The UI will include the status, outcome, and any reasons for a verification decision by the Verification Service team, and reasons from the rules engine, in order for CSAs to assist a client understand why they got a particular outcome, or what it means.
- d. The functionality to edit an email address, and resend notifications is being developed.

28. Verifying ID – an SOP for verifying the identity of the caller has been developed and is attached below at **Appendix 6**.

29. Description of contact centre systems

- a. The systems components that are used within ICC, are as follows. The external delivery partner will run their own systems which provide equivalent functionality.
- b. Vodafone’s Genesys telephony system platform; this holds call log data including date/time, CSA details, call metrics (call volumes, length of call, abandoned calls, wait time), caller ID (the incoming phone number and the outcome (disposition)
- c. Voice recordings are stored in the Verint system with a 24 month retention period (set across all MBIE contact centres). All staff can access their own calls. Leadership and Quality Assurance analysts can access all calls. Access is for training, performance management, responses to privacy requests or to investigate complaints, and to generate “customer insights”.
- d. Screen recordings are stored in the Vodafone system (these record all screens on display to the CSA during the call time and may include any personal information on the screens). These are stored for 2 months, and are accessible to the Quality Assurance Team, managers, system administrators, and the CSA. They are used for training, performance management, responses to privacy requests or complaints
- e. Nexidia – an Insights Analytics tool that also supports the Quality Assurance programme analyses the voice recording data for quality, customer insights, customer sentiment; all reporting is anonymised. Once the Contact Centre send the Decision Review Team an email of the review request (containing declaration ID and some background – No personal information in the email), the Decision Review Team will use the Internal Web Interface to view the declaration and review the decision. If the decision is to be changed, the Decision Review Team will use the Bulk Upload process to create a new declaration for the traveller with the correct outcome. Nexidia also selects calls to send to QAs, who then send assessments to CSAs and Team Lead.

30. MBIE is also analysing options on a customer relationship management system, for recording call history. Either part of the NZTD system, or independent. The objective is to improve customer experience, so that a brief caller history can be retained, so callers are not required to repeat themselves if they call frequently. Options for this are still being considered.
31. A contract between MBIE and Datacom Connect as a Telephony as a Service (TaaS) provider is being established. Datacom Connect is already an existing TaaS panel provider, so entering into an agreement of additional services; section 11 of the Privacy Act applies. Key aspects of the Contract are
- a. Coverage during agreed hours, plus overflow capacity
 - b. Service provided in accordance with MBIE training and escalation processes
 - c. Agreed reporting metrics
 - d. System components will be security accredited by MBIE
 - e. Staff will be security vetted (criminal history record check)
 - f. Work from anywhere framework – specifies home working environment, and all to be based in NZ
 - g. BYOD: Staff will use their own personal PCs subject to specified technology requirements
 - h. Service to be delivered in accordance with MBIE Code of Conduct (CSAs required to sign acknowledgement of Code of Conduct, MBIE Privacy Policy, and ICT Acceptable usage policy)
 - i. Service Provider will develop their own quality standards, policies, and procedures, aligned with settings prescribed by MBIE
 - j. Any Data held by the Service Provider will be returned on termination of agreement

7.2 Communication with travellers

32. Clear communication with travellers will be critical to the execution of NZTD.
33. Prospective travellers will need to understand that NZTD is a prerequisite for travel, so that they do not attempt to board an aircraft without knowing about their obligations. This has logical implications around travellers being well informed when they purchase carriage on an Airline, and feeling equipped to navigate the NZTD system.
34. All travellers will be advised of their privacy rights and interests consistent with [IPP 3](#). This will be achieved through **Control 2**.

7.3 Assurance and governance

35. Existing assurance of privacy controls and technical controls are recorded at **Appendix 1** and **Appendix 2**. An Interim System Security Certificate (ISSC) was completed in late 2021 to provide security assurance.
36. The responsible governance group is the Border Executive Board (BEB), comprised of the Customs Comptroller (Chair) and the Chief Executives / Director Generals of MBIE, Ministry of Primary Industries, Ministry of Transport, Ministry of Foreign Affairs and Trade, and MOH.
37. Reporting to the BEB is the Joint Executive Board (JEB) comprising the Customs Comptroller, Chief Executive of MBIE, and Director-General of MOH.
38. The NZTD Steering committee reports to the JEB. The Steering committee is made up of appropriate senior managers from MBIE and Customs. It is to the Steering Committee that the NZTD programme team report.

7.4 Enforcement systems to support the NZTD objectives

39. The enforcement of the NZTD should provide a meaningful disincentive for non-compliant behaviour, reflecting New Zealand's national interest and public health imperatives. By enforcing the NZTD this will help New Zealand to enable an enforcement response where travellers have not made a declaration, or where document fraud or gaming of the system has occurred. This will help:
 - a. keep risk offshore
 - b. retain the integrity of the risk-based approach as agreed by Cabinet and contained in the ABO.
 - c. enable the safe and efficient scaling up of the border re-opening
 - d. incentivise compliance
40. Information about enforcement is described further at **Appendix 5**.

8. Assessment of privacy impacts

41. This section advises on the privacy impacts of the NZTD in consideration of the IPPs of the Privacy Act by reviewing the collection, storage, use and disclosure of personal information for the purposes of the project.
42. The NZTD business case approved by Cabinet in August 2021 signalled the use of automated risk assessments to assign travellers to their risk-based entry pathway. This will help facilitate traveller volumes through a phased re-opening of the border and to accurately and consistently apply the non-discretionary rules-based health criteria that is to be agreed by Cabinet under Reconnecting New Zealand.

43. There will be assisted channels available for human intervention to address any technical issues that may arise during the processing of a declaration, and to ensure there is human oversight of the process.

8.1 Collection of personal information

IPP 1 – Purpose of collection of PI

Personal information shall not be collected by any agency unless:

- the information is collected for a lawful purpose connected with a function or activity of the agency; and
- the collection of that information is necessary for that purpose.

Operation of the ABO

The collection will occur under the authority of the ABO Amendment Order.

The ABO Amendment Order's purpose is *"to support a public health response to COVID-19 that furthers the purpose of the Act by imposing requirements and restrictions in relation to persons who arrive in New Zealand by air."* The Act that is referred to is the [COVID-19 Public Health Response Act 2020](#).

The NZTD is a defined system under the COVID-19 Public Health Response (Air Border) Order 2021 ('Air Border Order'). Clause 60 provides that the NZTD system is administered by the chief executive of the New Zealand Customs Service ('chief executive') and is to provide the following:

- (a) features to enable the chief executive to identify which COVID-19 provisions are likely to apply to a person who travels to New Zealand before, on, and after the person's arrival in New Zealand;
- (b) features to enable the chief executive to collect evidence of the person's compliance with the COVID-19 provisions that apply to the person;
- (c) features to enable the person to make a traveller declaration for the purposes of clause 23(3);
- (d) features to enable the chief executive to issue NZTD traveller passes for the purposes of clause 12.

The Air Border Order uses schedules to categorise types of travellers based on categories such as purpose of travel, whether a person is a citizen of New Zealand, and places that a person has or will visit in the 14 days prior to arriving in New Zealand. To determine whether a traveller is subject to a COVID-19 provision under the Air Border Order, first you need to determine what schedule applies to the traveller and then whether that schedule applies the COVID-19 provision. From 11.59 pm 31 March 2022, clauses 12 (must have traveller pass) and clause 23 (must make traveller declaration) will apply to essentially all travellers. This is subject to a limited exemption for any person who arrives in New Zealand due to an unplanned landing because of an emergency, such as a mechanical fault or a deep-sea rescue or New Zealand Defence Force members returning from service.

Clause 23(3) and 23(3A) provide that a person must make a traveller declaration through the NZTD system, except for in the alternate circumstances specified by the Director-General of

Health. As at 25 March 2022, those alternative circumstances are limited to separate arrangements for aircrew and to accommodate transitional arrangements (or backup arrangements such as the paper pass) from the Nau Mai Rā system to NZTD for traveller declarations.

Clause 23(2) provides that a person making a traveller declaration must include the information and confirm the matters that are specified by a Director-General notice. As at 11 am 25 March 2022 the relevant Director-General notice is [‘Specified Information and Form of Traveller Pass for New Zealand Traveller Declaration System’](#) (Notice Number 2022-go1081), Director-General notices are subject to update and change. That notice also specifies the form of a traveller pass that may be issued by the NZTD system, which includes that the pass may include information on a traveller’s entry pathway into New Zealand. This might include that a traveller is required to undergo testing on arrival, entry without undertaking isolation or quarantine, or other arrival pathway as may be applicable under the Air Border Order.

Clause 60(3) of the Air Border Order provides the circumstances in which a traveller may be refused a traveller pass having made a declaration through the NZTD. These circumstances include where a person has made an incomplete declaration, where they have not produced satisfactory evidence of compliance with a COVID-19 provision (for example they have provided an inappropriate vaccination certificate or PDT result as against the requirements specified by the Director-General), or where there are reasonable grounds to believe a traveller declaration is false or misleading.

If a traveller arrives in New Zealand without having made a traveller declaration or without a traveller pass, unless exempt, this is an infringement offence under the Air Border Order.

44. The collection by the NZTD is established under the Air Border Order.

- a. Clause 3 of the Air Border Order sets out the purpose of the Order AS: “to support a public health response to COVID-19 that furthers the purpose of the Act by imposing requirements and restrictions in relation to persons who arrive in New Zealand by Air.”
- b. Information collection is authorised under clauses 23 to 25 of the Air Border Order.
- c. Clause 24(1) provides that: “The purpose of this clause is to enable the Director-General to collect information to support a public health response to COVID-19 that is consistent with the purpose of the Act.”
- d. As the information being collected by NZTD is about being able to assess and manage the health risk posed by, and to, identifiable individuals, this requires the collection of those people’s information in accordance with the Notice requirements.

Other legislative provisions may be relevant to collection as well, such as section 53 of the Customs and Excise Act 2018.

45. Agencies also need to use the information that is collected to support the ongoing development and improvement of the NZTD system. Improvements such as fixing bugs, and increasing the efficiency for travellers, industry partners and border officials.

IPP 2 – Source of Personal Information

IPP 2 of the Privacy Act requires that an agency shall collect information directly from the individual concerned, unless an exception applies. Broadly, the exceptions under IPP2(2) are:

- (a) that non-compliance would not prejudice the interests of the individual concerned;
- (b) that compliance would prejudice the purposes of the collection;
- (c) that the individual concerned authorises collection of the information from someone else;
- (d) that the information is publicly available;
- (e) that non-compliance is necessary to avoid prejudice to maintenance of the law, for the enforcement of a pecuniary penalty law, for the protection of public revenue, for the conduct of court or tribunal proceedings, or to prevent or lessen a serious threat to the life or health of an individual; or
- (f) that compliance is not reasonably practicable in the circumstances of the particular case;
- (g) that the information will not be used in a form in which the individual concerned is identified or will be used for statistical/research purposes and not published in a form that could reasonably be expected to identify the individual concerned.

46. Core information will be collected directly from the individual when they engage with NZTD (or use an NZTD paper form), such as completion of the mandatory data fields or submission of relevant certificates to support the NZTD declaration. The individual will instigate the collection process by accessing the web portal, using an assisted channel, or authorising another person to complete the health declaration process on their behalf.
47. NZTD provides for formal assistance to support travellers, but informal scenarios are also envisaged.
48. Formal scenarios where someone may represent another person with a legal authority are as follows:
- a. Parent acting on behalf of a child under the age of 18.
 - b. Someone with Enduring Power of Attorney or who has been appointed to be a Welfare Guardian by the Family Court (or the equivalent in the traveller's native country).
 - c. A travel agent assisting the traveller.
 - d. By using the assisted channel - who will support travellers to make the declaration where they do not have internet capability, where disabilities or language capability prevent them from easily using the online process, where they experience technical difficulties with the system or process or where they choose to use that option. If the traveller requires assistance, NZTD requires that the permission to act on behalf is confirmed within the platform. The border agencies and MOH are reliant on this representation of authority being confirmed is true, and view any action on such

reliance as appropriate (noting that a fraudulent or duplicitous representation would breach the ABO).

- e. The Bulk Loading Interface that has been established to more easily raise declarations on behalf of NZDF, RSE, Refugee and humanitarian travellers and to also support the Decision Review Process.

49. Fundamentally this is still collection from the individual. For example, someone listening to the traveller directly and putting their information into the NZTD is not a breach of IPP2.

50. Informal scenarios

- a. Someone can help the traveller - this is contemplated in scenarios such as digitally confident family members or travelling companions are very likely to help less digitally confident members. There are appropriate tick-boxes in the NZTD digital form where this occurs.

IPP 3 – Collection of information from subject

IPP 3(1) of the Privacy Act requires that where an agency collects personal information directly from the individual concerned, the agency shall take reasonable steps to ensure that the individual knows:

- (a) the information is being collected;
- (b) the purpose of collection;
- (c) all intended recipients of the information;
- (d) name and address of the agency collecting the information and name and address of the agency holding the information;
- (e) whether collection is authorised or required by law – and the particular law, and whether it is mandatory or voluntary for the individual to supply the information;
- (f) consequences of not providing the information; and
- (g) their rights of access to (IPP6) and rights to correction (IPP7) of the personal information.

Under IPP 3(2) this should be done prior to collection, or as soon as practicable after collection.

51. There are potentially significant consequences for travellers for not providing the information – including not being able to travel – so the communications work is being navigated carefully.

52. The components of this strategy are as follows:

- a. A campaign to notify travellers about NZTD and their obligations.
- b. An IPP 3 compliant process within NZTD, showing the traveller a privacy statement before the traveller uses the NZTD platform to provide information. The wording for this statement will be layered to incorporate the broader NZTD privacy statement (**Control 1**).

- c. A traveller declaration that they have read the privacy statement prior to submission of their information (**Control 1**).

53. NZTD will be compliant with 3(2) as the NZTD privacy statement will be provided to the traveller prior to their entry of information into the platform.

54. If a traveller partially completes their NZTD and returns later after saving it, their acceptance of the privacy declaration will remain saved – consistent with IPP3(3) they will not need to resubmit the privacy declaration prior to finishing their NZTD declaration.

55. The following is a brief demonstration of IPP 3(1) compliance

Requirement	Compliance overview
(a) the information is being collected	Traveller submitted
(b) the purpose of collection	Privacy statement states. Explicit NZTD purposes and the ABO.
(c) all intended recipients of the information	MOH and MBIE (MIQ and INZ) and Customs
(d) name and address of the agency collecting the information and name and address of the agency holding the information	Parties' addresses and contact information is provided.
(e) whether collection is authorised or required by law – and the particular law, and whether it is mandatory or voluntary for the individual to supply the information	Required under the ABO.
(f) consequences of not providing the information	<p>Significant – the traveller is unable to travel: they may be prevented from boarding their plane.</p> <p>It is noteworthy that if health settings change (similar to during the Alpha or Delta waves) later, travellers may need to spend time in a MIQF if unable to (or don't) provide evidence establish conditions are met for QFT or Self Isolation. This would only occur in response to Cabinet directives.</p>
(g) their rights of access to (IPP6) and rights to correction (IPP7) of their personal information.	<p>Travellers are able to resubmit their declaration if it is erroneous.</p> <p>Rights to correct should mostly be unnecessary. However, this is covered in the Privacy Policy.</p>

56. NZTD will initially be built and deployed in English. As the system is rolled out, it is expected that additional languages will be added, particularly as our borders open up to more travellers. The system is being designed for delivery in English for Tranche One with capability for additional languages being developed as the system is rolled out. This functionality will assist travellers for whom English is not a first language to understand their rights under IPP 3.

IPP 4 – Manner of Collection

Under IPP 4(1) Personal information shall only be collected by an agency

- (a) by lawful means; and
- (b) in the circumstances of this project, are by means that are
 - (i) fair, and
 - (ii) do not intrude unreasonably on the personal affairs of the individual concerned.

Particular care should be taken with regard to collection of personal information from children or young persons.

57. NZTD information is being collected lawfully under the ABO, which specifies which information is mandatory and which system collects it (the NZTD).

58. Care has been taken to ensure only necessary information is required, this is consistent with the provisions of the relevant Notice and uses are limited appropriately. Alleged fairness issues, such as rights of unvaccinated people (in particular, the right that unvaccinated New Zealander's will be able to enter regardless of vaccination status) to travel or the status of natural immunity are not considered as this PIA does not address the underlying policy decisions or strategic direction of NZTD (3. *PIA Scope*). It is noteworthy that many of the components where this arises (e.g. vaccine status, pre departure testing) are reflective of government strategy.

59. Accessibility considerations are being implemented to provide equitable access to NZTD and mitigate undue difficulty for marginalised or vulnerable. NZTD is being designed within the [Web Accessibility Standard 1.1](#) for ease of use. Further, there are two assistance channels available to travellers who require support to access the NZTD:

- a. NZTD enables an authorised third party to complete the group declaration on behalf of a traveller and the third party confirms they have been authorised when making the submission.
- b. The Assistance Channel will support travellers to make the declaration where they do not have internet capability, where disabilities or language capability prevent them from easily using the online process, where they experience technical difficulties with the system or process or choose to use the assistance channels.

8.2 Storage and Security

IPP 5 – storage and security of personal information

IPP 5(a) An agency holding personal information must ensure that information is protected by such security safeguards as are reasonable in the circumstances, against:

- loss;
- unauthorised access, use, modification or disclosure; and
- other misuse

IPP 5(b) This is also required when the information is transferred to a third party.

60. Access to information and resources will be granted to only those individuals whom have a specific business purpose to access the information. Access to the information will be granted in accordance with existing role based access control and user management policies and procedures. All access to information and resources is logged and can be audited. NBS is subject to RBAC and Audit of all access and activity by authorised users. Access to the information will be granted in accordance with existing role based access control and user management policies and procedures within the MBIE, Customs and Health domains only.
61. Security Certification and Accreditation has been undertaken by both Customs and MBIE Security Teams. This process has involved third party review of security controls and penetration testing. All high severity issues have been resolved. Microsoft Azure Storage is being used. Data is stored and replicated across two geographically separate regions on Australia's East Coast.
62. Of the many aspects of privacy to the public and the message the public is receptive to, security and the expectation their personal information will be secure is very significant. All data captured by the NZTD will be encrypted during transport between systems and while stored. Agencies have policies and controls in place which prevent data from being accidentally disclosed including disabling use of non-approved USB storage devices on machines. Similarly, policies also exist to ensure software systems (including cloud services) are kept up to date in terms of security updates and configuration. All production systems have Disaster Recovery services, processes and procedures in place to support service recovery in the event of a major failure of primary systems. All data is protected by regular system backups.

8.3 Access, correction and accuracy

IPP 6 – access to personal information

Where an agency holds personal information, the individual concerned shall be entitled

- IPP 6(1)(a) to obtain confirmation of whether the agency holds personal information about them; and
- IPP 6(1)(b) to have access to their personal information.

Under IPP 6(2), if an individual is given access to their personal information, they must be advised that, under IPP 7, they may request correction of that information.

Under IPP 6(3), IPP 6 is subject to Part 4 (Access to and correction of personal information) of the Privacy Act.

IPP 7 – correction of personal information

Under IPP 7(1), where an agency holds personal information, the individual concerned is entitled to request correction of that information.

Under IPP 7(2), the agency must then take such steps that are reasonable in the circumstances (considering the lawful purpose of use of the information) to ensure that the information is accurate, up to date, complete and not misleading

Under IPP 7(2A), when making this request or at any later time, the individual may also provide the agency with a statement of the correction sought (**Statement of Correction**) and request that the Statement of Correction is attached to the information if the agency does not make the correction.

Under IPP 7(2B), where the agency is not willing to correct the information following a correction request, the agency must take reasonable steps to attach the Statement of Correction provided by the individual so that it will always be read alongside the information.

Under IPP 7(3), where the agency has corrected the information, or attached a Statement of Correction to the information, the agency must (if reasonably practicable) inform each person or agency to whom the information has been disclosed of those steps taken.

63. Individuals are advised they can view and request correction of any personal information in the privacy statement, and are directed to contact the agencies.

- a. Anything held in the declaration app is the responsibility of MBIE to provide.
- b. Anything held in the NBS is the responsibility of the MOH to provide.
- c. Anything held in Customs' systems, including review, or complaints, will be the responsibility of Customs to provide.

64. The agencies will work together to facilitate any appropriate access and correction requests.

65. Under usual circumstances, the information should be accurate at the point in time when the individual traveller submits their NZTD documentation. Risks with respect to IPP 7 are further mitigated by having an established call centre who can support any travellers, especially in the event of an issue where a traveller may face difficulty boarding.

IPP 8 – accuracy of personal information to be checked before use

An agency that holds personal information shall not use or disclose that information without taking steps that are (in the circumstances) reasonable to ensure that the information is accurate, up to date, complete, relevant and not misleading. These steps should be taken having regard to the purpose for which the information will be used (IPP1).

66. The collection will occur under the authority of the ABO. The purpose of collection is addressed above at the assessment of IPP 1.

67. NZTD has three classes of information that are being collected, each present slightly different accuracy risks.

- a. Biographic information and contact information - agencies will primarily rely on the accuracy of the information being provided by travellers with respect to their own personal information. It is possible that travellers may submit incorrect details (either accidentally or deliberately).
- b. Travel details. These are built into existing systems, but similarly, agencies are reliant on self-declared information being up to date, relevant and not misleading.
- c. Health information as specified in an ABO Notice for the specific pathway- the foundational purpose of NZTD is to enable validation of traveller's vaccination status and Covid-19 test, if required. Vaccination and COVID-19 testing information is verified.

8.4 Retention, use and disclosure

IPP 9 – agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purposes for which it may lawfully be used.

68. The NZTD will retain declarations and all directives arising from the NZTD until the end of the pandemic. The EU DCC document will be verified cryptographically and purged once the traveller crosses the border, or 7 days after the arrival date of the declaration the documents were uploaded in support of (whichever is the earlier).

69. Information retained on the National Border Solution (hosted by MOH) will be retained until the repeal of the COVID-19 Public Health Response Act 2020. The ABO does not signal a limitation on the timeframe for retention of this order, so information will be kept for the duration of the COVID-19 pandemic. This supports the ABO requirements and purposes set out above.

70. The main reasons to keep the information include:

- a. To support the ABO requirements and to support a public health response to COVID-19. Information will be retained in the NBS in an identifiable format for a time frame that aligns to the revocation of the COVID-19 Public Health Response Act 2020.
- b. Pandemic planning and response – de-identified information should be retained beyond the current pandemic.
- c. Enforcement of breaches – the parties wish to retain non-cryptographically verified vaccination and testing documentation. This is because certificates that are not digitally verifiable (i.e. do not have a cryptographically signed payload) that are submitted as part of the pre-travel documentation submitted by travellers will need

to be manually verified, and subsequently will need to be retained as it could be relevant to an alleged breach of the ABO.

- d. Technical – to support further development and improvement of NZTD . Information will need to be used to support process improvement and the release train for Releases 2 and 3. Agencies (whom) will need to store the data for a period of time and use it as example data for delivering those technologies and for making process improvements. Depending on what it is that agencies are trying to improve downstream, it may be necessary to gain access to raw data – for example, matching NZTD with travel documents by using biographic information.

Retention of EU DCC information

The European Union has set standards for vaccination certificates – these are EU Digital COVID Certificates (EU DCC).

New Zealand is now a third party country to the EU DCC Framework. This means that New Zealand and the EU recognise the status of each party's issued vaccination certificates - that the certificates validly provide proof of vaccination status, testing status or COVID-19 infection and recovery status.

This means that EU DCC certificates will be treated equivalently at the border as vaccination certificates issued by New Zealand for New Zealanders or those vaccinated in New Zealand, and New Zealand issued vaccination certificates will be treated as EU DCC certificates by nations using the EU DCC standards.

The effect of this equivalency status means that NZTD will not retain information from the EU DCC. Countries outside the EU may also be part of the EU Trusted Framework - the data retention requirements would extend to these countries. Consequently, NZTD will not retain information from EU DCC passes regardless of their nationality (though will retain information about EU DCC holders that they provide separately). The fact that an EUDCC was presented by the traveller will be recorded, but not the details held in the certificate itself.

The underlying reason for not needing to retain the EU DCC document is that these have cryptographically signed payload and therefore can be cryptographically verified - there would be no chance of the data contained being tampered with, so no infringement or enforcement issues arise.

At Tranche 1 – Pilot, the EU DCC document will be verified cryptographically and not retained. The only exception to this would be in the scenario where a user submitted an EU DCC that was too poor quality for the system to recognise, or the user had attempted to tamper with it. In this exception case, where the EU DCC is fraudulent, the document would no longer meet the EU conditions around data retention and therefore be acceptable to retain.

More information about the EU DCC can be found at the European Commission's website here: [European Union Digital COVID Certificates](#).

IPP 10 – limits on use of personal information

Personal information obtained in connection with one purpose, shall not be used for any other purpose unless the agency reasonably believes an exception applies. Exceptions are set out at IPP10(1), which broadly states:

- (a) that the purpose of use is directly related to the purpose of collection;
- (b) that the information will not be used in a form in which the individual concerned is identified or will be used for statistical/research purposes and not published in a form that could reasonably be expected to identify the individual concerned;
- (c) that the use for that other purpose is authorised by the individual concerned;
- (d) that the source is a publicly available publication, and it would not be unfair to use the information in the circumstances;
- (e) that the use for that other purpose is necessary to avoid prejudice to maintenance of the law, for the enforcement of a law imposing a pecuniary penalty, for the protection of public revenue, or for the conduct of court or tribunal proceedings; or
- (f) that the use for that other purpose is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of any individual.

71. The information is to be used consistently with the purposes set out in the ABO, being to support a public health response to COVID-19 that furthers the purpose of the Act by imposing requirements and restrictions in relation to persons who arrive in New Zealand by air and managing applicable conditions after their arrival (and as further described in the NBS PIA) and used for directly related purposes. These purposes are described at the analysis of IPP 1 above.

IPP 11– limits on disclosure of personal information

An agency shall not disclose personal information to any other agency or person unless the agency believes, on reasonable grounds, that:

- (a) the disclosure purpose is in connection with (or directly related to) the purpose for which the information was obtained;
- (b) the disclosure is to the individual concerned;
- (c) the disclosure is authorised by the individual concerned;
- (d) the source of the information is a publicly available publication, and in the circumstances would not be unfair;
- (e) the disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency; for enforcing a law imposing a pecuniary penalty; for the protection of the public revenue; or for the conduct of proceedings before any court or tribunal;
- (f) the disclosure of the information is necessary to prevent or lessen a serious threat to public health, or public safety, or the life or health of an individual;
- (g) the disclosure is necessary to enable an intelligence and security agency to perform any of its functions;
- (h) the information is to be used in a form in which the individual concerned is not identified, or for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or
- (i) the disclosure is necessary to facilitate the sale or other disposition of a business as a going concern.

This principle is subject to IPP 12.

72. For completeness, the information collected by NZTD and passed to the MOH for NBS is consistent with the purpose for which it is collected – namely, supporting a public health response to COVID-19 that furthers the purpose of the Act by imposing requirements and

restrictions in relation to persons who arrive in New Zealand by air and managing applicable conditions after their arrival (and as further described in the NBS PIA). The information collected by NZTD and passed to MBIE is consistent with the purpose for which it is collected – enabling the identification of the appropriate pathway status (from no isolation to self-isolation to managed isolation) and associated risk management requirements for individual passengers.

73. NZTD will share a traveller's vaccination status with the airline at the time of check-in (prior to boarding). This is to support airlines implement any public health policies and support Airlines to meet their ABO obligations under clause 54 of the ABO. It will also streamline the process and user experience for travellers so they do not have to present the same information to multiple parties for the same journey. Paper based forms will not be shared in this fashion.

8.5 Offshoring of Information

IPP 12 – disclosure of personal information outside New Zealand

An agency may only disclose personal information to a foreign person or entity (**recipient**) in reliance on IPP11(a), (c), (e), (f), (h), or (i) if:

- (a) the individual concerned (whose personal information it is) authorises the disclosure after being informed that the recipient may not be required to protect the information in a way that, overall, is comparable to the Privacy Act;
- (b) the recipient is carrying on business in New Zealand and the agency believes the recipient is subject to the Privacy Act;
- (c) the agency believes on reasonable grounds that the recipient is subject to privacy laws that (overall) provide comparable safeguards to the Privacy Act;
- (d) the agency believes on reasonable grounds that the recipient is a participant in a prescribed binding scheme (as defined in [insert specific regulation] the Privacy Act);
- (e) the agency believes on reasonable grounds that the recipient is subject to the privacy laws of a prescribed country (as defined in [insert specific regulation]); or
- (f) the agency believes on reasonable grounds that the recipient is required to protect the information in a way that (overall) provides comparable safeguards to the Privacy Act – for example, under a contractual agreement between the agency and the recipient.

74. There is no intention for NZTD to disclose or provide to any agent or recipient based outside of New Zealand any personal information for processing.

8.6 Unique Identifiers

IPP 13 – Unique identifiers

Agencies shall not assign unique identifiers to individuals unless it is necessary for that agency to carry out its functions. Agencies shall not require individuals to disclose any unique identifier unless that disclosure is related to the purpose it was assigned.

75. Passport numbers will be retained in NZTD. These are not being assigned by NZTD and are related to the purpose for which they were assigned – namely to facilitate international travel. Passport number is a search field for the contact centre.

76. NZTD reference number will be used to search for applicants.

Appendix 1 - Project Risks

Risk #	Risk Rating	Reasoning	Mitigations / Controls	Residual Risk
R0	Med	Mandatory nature of making travellers provide the Specified Information poses a risk without a clear and lawful basis.	C0 – ABO sets out the information required of Travellers. C1 – NZTD Privacy Statement sets out the purpose (IPP 1 of the information) as well as IPP 3 requirements. Travellers should clearly understand the requirement and rationale behind it.	Very Low.
R1	High	Travellers may not sufficiently understand: <ul style="list-style-type: none"> • NZTD requirements • Their legal and privacy rights • Consequences from NZTD. 	Controls are: C1 – NZTD Privacy Statement C2 – Communications Strategy C6 – Assistance Channel processes and policies.	Med.
R2	High	Excess retention – breach of IPP 9, and potentially breach our EU DCC obligations and thereby lose equivalency status.	C3 – NZTD Retention Policy C4 – EU DCC Conditions	Low
R3	Low	Accessibility and equality of experience for Travellers pose a risk of collection of information being unfair, or perceived as unfair. The risk to the project as a whole is not high – the risk is to the relationship between NZTD agencies and the individual.	C2 – Communications strategy C6 – Call Centre processes and policies.	Very Low
R4	High	Privacy breach of any principle lowers public, airline partner and Ministerial trust in NZTD. This could occur through any specific privacy breach – such as	All relevant controls and technical controls.	Med.

		unauthorised use or disclosure, employee browsing, system error, access to information not being provided etc.		
--	--	--	--	--

Appendix 2 – Non-Technical Controls and Control Validation

Control	Control Description and implementation	Validations	Effectiveness
<p>C0 – ABO</p> <p>The Order sets the purpose for information collection.</p>	<p>Passive control.</p> <p>A copy is available here.</p> <p>COVID-19 Public Health Response (Air Border) Order 2021 (SL 2021/427) (as at 25 March 2022) – New Zealand Legislation</p>	<p>The Order is in place, signed on 25 March 2022.</p> <p>Prior to signing it was reviewed by the Parliamentary Council Office, public sector drafting experts.</p>	<p>High</p> <p>In place</p>
<p>C1 – NZTD Privacy Statement and Declaration</p> <p>A NZTD privacy statement is available at Privacy New Zealand Traveller Declaration.</p> <p>When using NZTD, travellers are required to acknowledge this statement.</p>	<p>Passive control.</p> <p>Control owner: Customs Information Sharing and Privacy.</p>	<p>Drafted with input from legal and technical teams.</p> <p>Consultation with Legal/ Privacy SMEs at MBIE and MOH.</p>	<p>High.</p> <p>In place</p>
<p>C2 – NZTD Communications Strategy</p> <p>A communications strategy has been developed with</p>	<p>Passive control.</p> <p>Control owner: NZTD project team.</p>	<p>Working closely with the travel industry and also targeting informal assistance channels such as family and friends.</p>	<p>High.</p> <p>In place</p>

accompanying documentation and public information.			
C5 – Enforcement policy Clear standards for enforcement as envisaged by the parties.	Passive control. Control owner: Customs Policy	RIS approved by RIS panel. Consulted with agencies including MOH and Ministry of Justice Enforcement policy reflected in operational policies and procedures Compliance and enforcement table developed by legal and Customs operations	High. In Place
C6 – Assistance Channel processes and policies. <ul style="list-style-type: none">• Access• Correction• Accessibility• Verifying ID	Active control. Will require ongoing involvement from INZ.	Attached at Appendix 6 below.	High In place
C7 – Governance Structure The Boarder Executive Board (BEB) is responsible for the programme. The Joint Executive Board (JEB) reports to the BEB. The Steering Committee reports to the JEB.	Passive control. Control owner: BEB	Terms of reference are established – set out the purpose and principles of the BEB, as well as the overarching governance structure.	High. In place
C8 – Assurance plan PIA controls will be reviewed in an ongoing fashion.	Passive control. Control owner: Project Team	PIA controls are earmarked in the programme assurance framework. PIA controls are earmarked for ongoing review – including potentially through Audit NZ.	Low. Not yet in place

C9 – Party MOU An MOU	Passive control. Control owner: Customs Policy team	Drafted with input from legal and privacy. Signed out by SRO for CE Signature on 31/03/2022.	Med. Imminently in place.
C10 – Paper form And conditional NZTD traveller pass for those able to submit their information but cannot upload their health documentation	Active control Control owner: NZTD Project Team	Paper based form has been developed for scenarios in which an individual is unable to complete the minimum information requirements for their NZTD declaration online or who was not aware of the requirements when they arrive check-in	High In place.

Appendix 3 – Technical Controls and Control Validation

Control	Control Description and implementation	Validations	Effectiveness
TC 1 – User Management and Access Control Prevents unauthorised individuals accessing data.	Network control. Authentication Authorisation	Assessed in ISSC.	High In place
TC 2 – Data Protection Data is encrypted in transit and rest.	Security control.	Assessed in ISSC.	High In place
TC 3 – Security Monitoring Cloud is monitored for breaches, component failure, programming error, and misconfiguration.	Network Control.	Azure Network Watcher is implemented on the Azure cloud. Assessed in ISSC.	High In place

TC 4 – Privileged Access Controlling access rights of users, restricting room for bad actors.	Network control. Authorisation.	Contractors must obtain organisational clearance. Multi-factor authentication is in place. Assessed in ISSC.	High In place
TC 5 – Solution Design Design was peer reviewed by Solution Architects. External 3 rd party has been contracted.	Design control.	Ongoing Security Architecture reviews. Secure Configuration reviews. Assessed in ISSSC.	High In place

Appendix 4 – Information collected by NZTD

All of the datafields that end up in NBS are essentially used for the following purposes: *To support the public health response to COVID-19, including management of border arrivals to meet applicable requirements under relevant Orders or Notices both at arrival and after arrival (for example post arrival testing), contact tracing or to provide relevant public health related information, request participation in relevant surveys, and reporting and analysis (where reports produced will not contain any identifiable information).*

Information to be set out in Director-General notice.	What the information could be used for depending on settings.
Full name (as per passport details)	Biographic information used to: <ul style="list-style-type: none"> • Validate identity of the traveller • Assign NHI or match to existing NHI – the NBS will perform NHI Matching, if an NHI isn't found the NBS will decide whether to create one or not. • Manage the traveller on arrival in New Zealand in accordance with assigned traveller risk assessment category including by searching for MIQ Booking Records.
Date of birth	Biographic information used to: <ul style="list-style-type: none"> • Validate identity of the traveller.

	<ul style="list-style-type: none"> • Assign NHI or match to existing NHI – the NBS will perform NHI Matching, if an NHI isn't found the NBS will decide whether to create one or not. • Manage the traveller on arrival in New Zealand in accordance with assigned traveller risk assessment category including by searching for MIQ Booking Records. • Rules or risk assessment (age delineation of those under 17 vs over 17).
<p>Passport details:</p> <ul style="list-style-type: none"> - Number (of the passport intended to be used to enter New Zealand) - Passport Expiry date - Nationality on passport 	<p>Biographic information used to:</p> <ul style="list-style-type: none"> • Validate identity of the traveller. • Risk / Rules assessment.
<p>Contact email (for traveller or their guardian)</p>	<p>Contact information used for</p> <ul style="list-style-type: none"> • communication for personal Traveller Health processes such as but not limited to; NHI identification, Change of risk classification, Self Isolation requirements, • Contact tracing • MOH arrival testing regime – contacting people who have entered New Zealand through the self-testing pathway.
<p>Contact phone number (for traveller or their guardian).</p>	<p>Contact information used for</p> <ul style="list-style-type: none"> • communication for personal Traveller Health processes such as but not limited to; NHI identification, Change of risk classification, Self Isolation requirements, • Contact Tracing
<p>NZ Contact Address</p>	<p>Contact Tracing</p> <p>Potentially enforcement</p>
<p>Emergency Contact Name</p>	<p>Contact Tracing</p>
<p>Emergency Contact Relationship</p>	<p>Contact Tracing</p>

Emergency Contact Phone number	Contact Tracing
Emergency Contact Email (if any)	Contact Tracing
Flight Number	Flight details used for: <ul style="list-style-type: none"> resource planning (such as management of testing on arrival) and implementation and checking of traveller risk assessment settings
Scheduled Date and Time of Departure	Flight details used for: <ul style="list-style-type: none"> resource planning (such as management of testing on arrival) and implementation and checking of traveller risk assessment settings
Scheduled Date of Arrival	Flight details used for: <ul style="list-style-type: none"> resource planning (such as management of testing on arrival) and implementation of traveller risk assessment settings Confirm that the traveller is entering New Zealand on the date that they had the NZTD approved for – the declaration is valid for the single journey. Checking of traveller risk assessment ratings.
Travel History	Part of traveller risk assessment process – to assign category. Statistical analysis to assist with public health planning Contact tracing (in the event of a heightened risk from a location incorporated into the history)
Proof of negative COVID-19 Test	Health status
COVID-19 vaccination status, and proof of vaccination if claiming to be vaccinated or if required by Government settings (i.e. foreign nationals)	Health status

Acknowledged Privacy Terms	Assigned by the system to manage the entry of the Traveller to New Zealand and the management of that individual after arrival depending on the category assigned (MIQF, Self-Isolation or Quarantine Free Travel)
Confirmation submitted on own behalf	Privacy
Consent to act as authorised representative confirmed	Privacy

Appendix 5 – Enforcement

Offence	Enforcement
Failure to have a 'travel pass' before a traveller arrives in New Zealand	Low risk infringement offence under the COVID-19 Public Health Response (Air Border) Order/

Appendix 6 – Contact Centre identity verification processes

Identity verification processes

Call type	Identity verification requirement	Authorisation requirement if third party caller (whether or not the caller submitted on behalf)
Level 1 - General enquiries, with no THDS look up	No requirement to verify caller identity	No authorisation required
Level 2 - Technical troubleshooting, to assist with completion of the declaration Requires look up of THDS, but no personal information provided to caller (who may or may not be the traveller)	Identity verification required	Low level of authorisation/consent
Level 3 - Provision of personal information to caller - Includes: <ul style="list-style-type: none"> • status update • reiterate outcome or reasons for outcome 	Identity verification required	For third parties, authorisation can be explicit (if traveller is present) or inferred

Identity Verification – Level 2 and 3 calls

Confirm with caller they consent to you looking up the Declaration

	Identity verification and authorisation	Call type
Is the caller the applicant?	<p>Client provides one of the following</p> <ul style="list-style-type: none"> • Passport number; or • Travel Dec unique ID <p>Confirm with client</p> <ul style="list-style-type: none"> • Full name (including any middle name/s); and • Date of birth <p>If the caller cannot provide passport or unique NZTD ID then, ask for:</p> <ul style="list-style-type: none"> • Full name (including any middle name/s); and • Date of birth <p>AND two of the following:</p> <ul style="list-style-type: none"> • Address in NZ • Email address • Phone number • Nominated emergency contact • Expected flight details 	If identity is verified, can answer Level 2 and 3 enquiries
Third party (friend, family or	<p>Verify the client</p> <p>Search for the relevant Travel Declaration using search parameters, and confirm the caller can identify</p>	Level 2 call type

<p>travel agent) – authorisation</p>	<ul style="list-style-type: none"> • Full name (including any middle name/s); and • Date of birth <p>AND two of the following:</p> <ul style="list-style-type: none"> • Address in NZ • Email address • Phone number • Nominated emergency contact • Expected flight details <p>Identify the caller Ask for and record (once note-taking feature is available)</p> <ul style="list-style-type: none"> • Name • Phone number • Relationship to traveller 	<p>For technical trouble shooting, no additional authority is required</p> <p>Level 3 call type</p> <ul style="list-style-type: none"> • To clarify outcome: ask for Date [or details] of email re outcome (if sent) – if known, can provide further information to clarify that outcome to assist traveller with next steps OR • To provide status update: ask for date submitted, if known can give status information (received / assessment in progress / completed)
---	---	---