

Recommendations	Actions to date	Continuous Improvements
1. Agree governance responsibilities	Sue Hardiman + Charles Ronaldson and Governance Group stood up.	
2. Complete impact assessment	S241 Risk issue register completed. Last updated 24/10/2017, right before expiry of class authorisations.	Impact of future renewals mitigated by application form being developed for consistency and ease of use for customers. Risk register requires updating prior to 2022 renewal period.
3. Define future state	Current and future state defined prior to expiry of class authorisations October 2017.	Refine future (now current) state prior to 2022 renewal period.
4. Develop roadmap	Phase 1 and phase 2 developed for improvements to s241 access. Phase 1 – expiry of class authorisation successful as at 01 November 2017. Phase 2 – Auditing underway with 3 of 8 completed.	Monitoring plan to be identified once audits are complete.
5. Derive a planned, resourced and risk-balanced delivery	Project team stood up with governance group to see out phase 1 of expiring class authorisation. Operational processing handed over to new team. Creating of application form for next renewal period added to documentation.	Documentation and storage of processes significantly improved and ongoing.
6. Develop a communication plan	Stakeholder relationship jointly managed by Exemption Assessments team for operational support and Contract Management and Support for technical support	Future stakeholder comms to be mapped out for 1-5 years for strengthening connections/working together (Trader Network newsletter, frequent contact with portals and representative bodies outside of audit contact).

Findings	Actions to date	Continuous Improvements
1.	Deadline met, very low impact to 'cut off' customers, nowhere near the potential hundreds we had planned for.	Prepare for 2022 renewal period, comms plan and schedule actions required.
2.	Governance responsibilities defined prior to 31 Oct 17 deadline.	
3.	Documentation significantly improved as well as storage and folder structure tidied up. Application form created. Guidance notes to gauge correctness of applicant answers created.	Ongoing documentation improvement and creation.
4.	Expired class authorisations. New process of standard terms allows NZTA visibility of exactly who has access. Currently 2199 entities authorised.	Automate process for NZTA and portal providers.

5.	Guidance for instances of misuse created for staff to take action on breaches and complaints instead of the adhoc actions taken in the past.	Aim to share guidance with Portals to seek feedback and input then formalise approached taken for misuse.
6.	Processes and procedures defined and documented during handover to new team.	Monitoring plan to take from after audits completed
7.	Class authorisations expired, applicants had to come directly to NZTA, 'authorised' list created and current number as at 17/8/18 2199 authorised entities.	
8.	Portals can only add access for their customers up to what NZTA have authorised.	Auditing of portals and their processes underway, if we can help in anyway or standard some processes we can gain this insight from audit results and better understanding of how each portal operates.
9.	Audit on portals in place and instances of misuse being approached inline with our documented guidance.	Audit results can determine future improvements.
10.	As above	As above
11.	User groups and access directly on MVR by NZTA staff leaves a trail to be investigated as necessary.	Further review of user groups and those who need certain access (user access and user end forms as per standard NTA onboarding and exiting)
12.	At present applicants describe their security set up and we are either satisfied or not and request tighter controls.	If audit results return need to standardise information security, password settings etc we can take action.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

SECTION 241 AUDITING PROCESS 2018

Roxane Whitcombe, Contract Management & Support

26/3/2018

VERSION 1

This document is to outline the process that Contract Management and Support will follow to audit the approved Section 241 portals.

Document version history

DATE	VERSION	AUTHOR	CHANGES
26/3/2018	Draft process	Roxane Whitcombe	
9/4/2018	Final Draft	Roxane Whitcombe	

Copyright information

This publication is copyright © NZ Transport Agency. Material in it may be reproduced for personal or in-house use without formal permission or charge, provided suitable acknowledgement is made to this publication and the NZ Transport Agency as the source. Requests and enquiries about the reproduction of material in this publication for any other purpose should be made to:

Manager, Information
NZ Transport Agency
Private Bag 6995
Wellington 6141

The permission to reproduce material in this publication does not extend to any material for which the copyright is identified as being held by a third party. Authorisation to reproduce material belonging to a third party must be obtained from the copyright holder(s) concerned.

Disclaimer

The NZ Transport Agency has endeavoured to ensure material in this document is technically accurate and reflects legal requirements. However, the document does not override governing legislation. The NZ Transport Agency does not accept liability for any consequences arising from the use of this document. If the user of this document is unsure whether the material is correct, they should refer directly to the relevant legislation and contact the NZ Transport Agency.

More information

NZ Transport Agency

If you have further queries, call our contact centre on 0800 699 000 or write to us:

NZ Transport Agency
Private Bag 6995
Wellington 6141

This document is available on the NZ Transport Agency's website at www.nzta.govt.nz

BACKGROUND

The Motor Vehicle Register (MVR) records information about vehicles used on New Zealand roads and the persons responsible for their use. The primary purposes of the Motor Vehicle Register are:

- enforcement of the law
- maintenance of the security of New Zealand
- collection of charges imposed or authorised by an Act,
- administration and development of transport law and policy.

Access to personal information about registered owners outside of these primary purposes is primarily facilitated by legislation in section 241 of the Land Transport Act 1998 (separate one-off applications can be made for this information under section 236). Access under section 241 was originally managed by the Ministry of Transport (MoT) but it was transferred over through delegation to the New Zealand Transport Agency (NZTA) to administer. MoT setup a system of Class authorisation to reduce the administrative burden of individual applicants. NZTA has reviewed this type of access and managed an exit of class based authorised access when they expired on 31 October 2017. All customers now have individual access authorisations or utilise their membership as part of a representative body.

A health check review was performed by Ernst and Young in 2017. The findings of this review are contained in the review report.

NZTA MVR Third Party Access Report 20170811_FINAL.pdf
 s6(a)

Based on the findings and assessment completed, the control environment was seen as “partially effective”. To increase the control environment a more robust compliance and regulatory framework was required. The Contract Management and Support team have been identified to carry out the auditing of the third Party portals who have access to MVR registered persons information under s241.

RISK IDENTIFIED

MVR contains the name and address of the registered persons which is protected by the Land Transport Act 1998 & the Privacy Act 1993.

Ernst & Young identified the profile of this application as low risk in the review in August 2017.

However findings below identified for monitoring and reviewing the access of section 241 and any suspicious activity.

<p>6) Our assessment found that there are minimal clearly defined procedures in place for:</p> <ul style="list-style-type: none"> ▶ Managing end to end access (including granting, updating, reviewing and removing access). ▶ Monitoring 241 access to identify suspicious activity. <p>The risk implication of these findings is that third parties use their authorised access to MVR data inappropriately (i.e. not for its intended purposes) and this goes undetected. This could also lead to non-compliance with the Privacy Act 1993 which could result in potential reputational damage and legal action.</p>	<p>Medium</p>
--	---------------

<p>9) Data usage: Our assessment found that there is limited verification by NZTA over how the third parties are using and protecting MVR data or if they are complying with NZTA's terms and conditions. Some third parties are required to provide annual audit reports on access to MVR, however these are not reviewed by NZTA and the criteria for requiring audit reports have not been clearly defined.</p> <p>The risk implication is that third parties (including organisations, portal access providers and industry bodies) use their authorised access to MVR data inappropriately (i.e. not for its intended purposes) and this goes undetected.</p>	<p>Medium</p>
--	---------------

<p>10) Data handling/extraction: Our assessment found that NZTA has limited oversight or control over what third parties are doing with the personal information extracted from MVR, where the data is being stored or how it is being used and protected. There is an indication that queries are being made to MVR to replicate the data.</p> <p>The risk implication is that third parties (including organisations, portal access providers and industry bodies) use their authorised access to MVR data inappropriately (i.e. not for its intended purposes) and this goes undetected.</p> <p>This could lead to non-compliance with the Privacy Act 1993, which could result in potential reputational damage and legal actions.</p>	<p>Medium</p>
--	---------------

APPROVED PORTALS

Portal access providers – a sub group of third parties, who are able to grant access to MVR data via their portal (i.e. Carjam, TradeMe)

Portal	Trading name or prior name	contact person	email address(es)	Gazette link
Carjam Online Limited	CarJam	s9(2)(a)	s9(2)(a)	https://gazette.govt.nz/notice/id/2017-au3975
Centrix Group Limited	Centrix	s9(2)(a)	s9(2)(a)	https://gazette.govt.nz/notice/id/2017-au5050
Equifax New Zealand Information Services and Solutions Limited	previously known as Veda Advantage (NZ) Limited	s9(2)(a)	s9(2)(a)	https://gazette.govt.nz/notice/id/2016-au4445

Information Logistics Company Limited	InfoLog	s9(2)(a)	https://gazette.govt.nz/notice/id/2017-au5301
Lemon Check Limited	Lemoncheck	s9(2)(a)	https://gazette.govt.nz/notice/id/2016-au5489
Limelight Software Limited	Motorcentral		https://gazette.govt.nz/notice/id/2013-au3031
PODcom Limited	PODcom		https://gazette.govt.nz/notice/id/2017-au6762
Trade Me Limited	MotorWeb		https://gazette.govt.nz/notice/id/2016-au5580

SECTION 241 PROCESS

Solution strawman design from "project plan - s241stage 2"

S241 System - Stage 2 Option 1

Conceptual Strawman Design

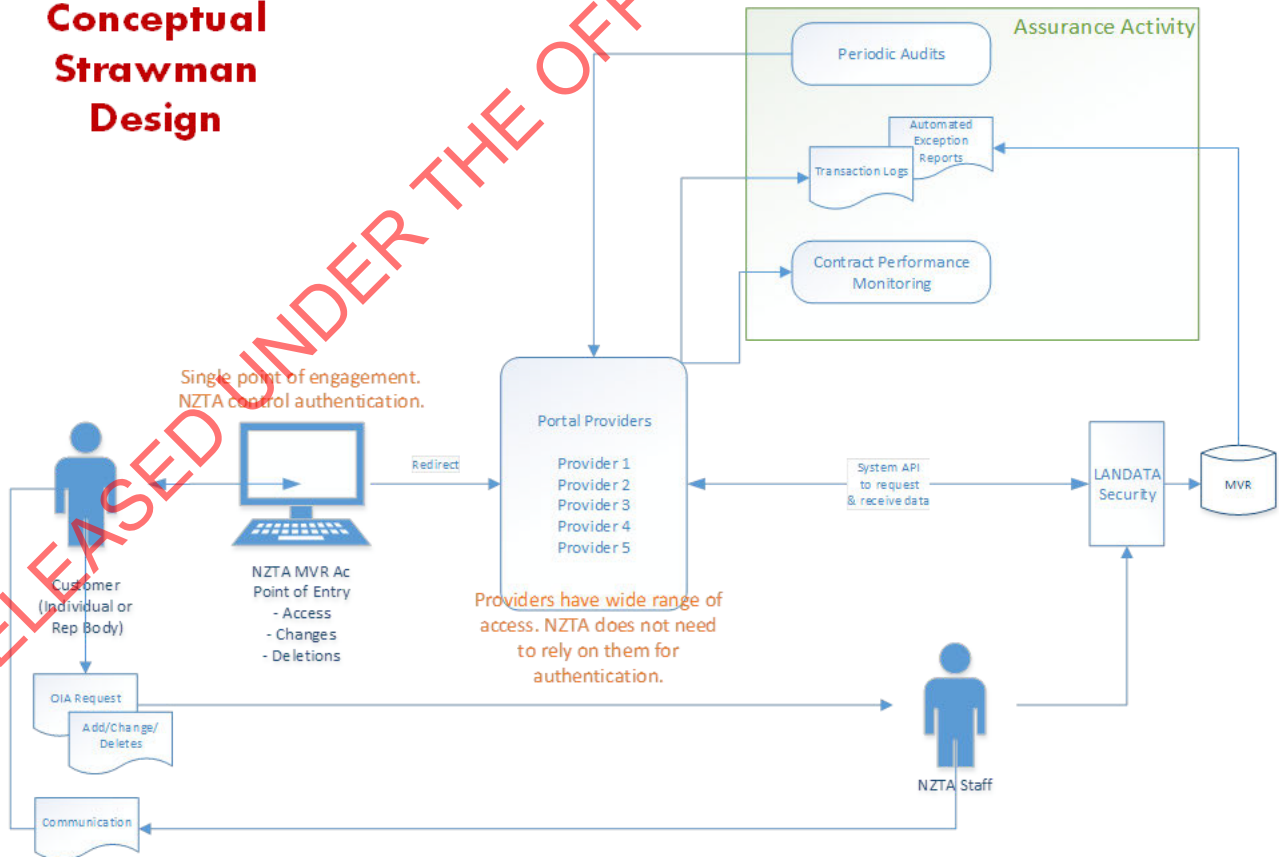


TABLE TOP AUDIT OF PORTALS

SEND LETTER

1. A letter is to be sent to providers from the Transport Agency Assessments team requesting the required information to audit.

Details of the letter to include the following:

- a. Queries completed over 12 months in excel format
- b. Refer to each Portal for conditions and required information.
The record should detail plate queries & reason for query
- c. Any unauthorised breaches that are known
- d. A deadline for the queries to be sent to the Transport Agency.

Link to auditing spreadsheet MASTER which details some if not all of the above

[Section 241 Portals Spreadsheet - 2018 proposed auditing.xlsx](#)

REQUEST INFORMATION TEAM

s6(c)

EXCEPTIONS

Exceptions are:

1. Omitted plate's queries from Portal report but are found in Information team spreadsheet (MVR queries).
2. Multiple queries on the same plate
3. Anomalies in Volume of queries, times
4. Complaints
5. Breaches of Contract

Where exceptions are found – an email to be sent from the Transport Agency Assessment's team to the Portal requiring further information/explanation regarding what/why query occurred and for what purpose.

NEXT STEPS

If response is not satisfactory the TA Assessment Team to review access granted and next steps required.

Review queries more frequently due to heightened risk.

TRAINING MATERIAL TO BE REVIEWED

Request annually the portal to provide a copy of

1. The training material used to authorise staff who access this information under s241
2. Full list of user/business's/clients authorised by the portal to access the S241 information.

Review and identify any concerns

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

3. To confirm the level of access that the user has, take the customer number from INQUIRER field and enter into the **WEBUSER** screen in MVR:

Quick Navigate | WEBUSER | Maintain Motochek Web Users | 2.30v12

Inquire

Customer No

New Password

Confirm Password

Type of Business

Email Address

Customer Status

Terms Accepted

Access Type

Access Level

Bank Account Status

Expiry Date

If the access is **Public Standard**, no registered person details would have been released. Any other access type would have resulted in registered person details being released

Note: If the customer name is that of a portal i.e. Trade Me, Information Logistics or CarJam we will need to contact the portal directly to establish what access the user had and who the user was.

Yes, the user has access to registered person information: Move to next step

No, the user is Public Standard: Investigation complete – there was no breach via Motochek or Portal. Complainant should be notified of the outcome and educated about the release of personal information.

4. Confirm what authorisation the user holds and the specified purposes for access. This can be found by searching the user's name online at <https://gazette.govt.nz/>.

Note: Motor Vehicle Traders, Financial Service Providers & Service Stations hold "Class Authorisations". The company themselves may not have an authorisation but if they act in the capacity of a company that has a class authorisation they may still have access to registered person details.

Yes, the personal information was accessed outside of the authorisation/specified purposes: Move to next step

No, they are entitled to this information in accordance with their authorisation: Investigation complete – there was no breach via Motochek or Portal. Complainant should be notified of the outcome and educated about the release of personal information.

5. Gather any further information from the complainant that you may not already have. For example, who, when, why. How did the complainant become aware that the details had been accessed from the MVR?
6. Contact the entity that has accessed the information (or the portal) to establish what the reason for accessing the MVR was. If available, we should be requesting supporting documents as to why the information was accessed.

Yes, the personal information was accessed outside of the authorisation/specified purposes: Move to next step

No, they are entitled to this information in accordance with their authorisation: Investigation complete – there was no breach via Motochek or Portal. Complainant should be notified of the outcome and educated about the release of personal information.

7. Based on the information we have obtained in step 1-6, it will be clear whether the information accessed was legal. If it is determined that the access was in line with the user's authorisation, there is no further action to be taken and the complainant should be notified of the outcome and educated about the release of personal information. If the query is outside of the specified purposes, we now need to advise all appropriate parties of the breach.

Stage Two

1. Contact the Panel – Alan Malthus, Kevin O'Kane & [REDACTED] s9(2)(a) [REDACTED]. Include any relevant documents, information and [REDACTED] meeting to discuss further, if required.
2. Contact our Privacy Officer, Christie Baird. Include any relevant documents, information and findings we hold.
3. If you believe the user had intended to obtain and use the personal information for malicious/criminal purposes, contact **Name**, from the NZ Police. Include any relevant documents, information and findings we hold.
4. Contact **TBA (Robyn Elston)** to arrange meeting for advice on how to proceed. Include any relevant documents, information and findings we hold.

Note: Upon receiving advice from **TBA**, you will be guided on the next step. For example, further investigation, possible revocation or education plan for user.