RSI Privacy and Data Protection Policy

1. Introduction
Protecting your privacy is important to RSI Pty Ltd ('we'; 'us'). The following will help you understand how we collect, use, disclose, hold and safeguard your personal information.

Our main purpose
We are an organisation which registers and inspects vehicles on behalf of the Secretary of the Department and Transport (DTP) as the person responsible for the State of Victoria's Roadworthy Scheme, and the information is, amongst other things, used for that purpose by the Secretary. The Secretary of the Department can be contacted on telephone (03) 9655 6666.

Personal information can come from people seeking to register vehicles, and to ascertain the roadworthiness of their vehicles. (Our Services)

2. Collection of personal information

What sort of personal information do we collect and hold?
The personal information we collect and/or hold includes information set out in Attachment 1.

Anonymity and Pseudonymity
Wherever possible, we will give you the option of dealing with us anonymously or by pseudonym.

Why do we collect and hold personal information?
If you wish to access or use our Services, it will be necessary for us to collect some personal information from you.

We only collect the information that we need to provide our Services, administer accounts, monitor our compliance with our obligations and satisfy our legal obligations. Obviously, the main consequence of not collecting this information is our inability to provide such Services.

How do we collect personal information?
We collect information directly from people in various ways, including by via our inspectors interactions with you or your representatives.

Unsolicited information and information from third parties
In limited circumstances we may receive personal information which we have not specifically asked for. In these circumstances, we will determine whether it is necessary for us to retain that personal information.

If you provide us with information about another person, you must: ensure that you have their consent to do so; and tell them that you are disclosing their personal information to us and where they can obtain a copy of this privacy policy – see section 8.

3. How we use your personal information

To provide you with the Services you want
We use the information provided by you to provide our various Services, and to perform administrative functions such as receipting, billing and handling complaints.

To ensure the Secretary of the Department and Transport's Roadworthy and Registration (Dealer Certification) Scheme functions properly
We may need to use your personal information to answer any enquiry from the Secretary of the Department and Transport's or Safe Transport Victoria, providing them with registration and inspection information, and informing the Secretary, and any other relevant government regulator such as Digital Victoria (CIRS), OVIC, the Australian Cyber Security Centre and OIAC, of any data breaches or incidents, and associated complaints.

To deal with your enquiries and complaints
We may need to use your personal information to answer an enquiry or complaint a person makes in respect of our Services.

To provide you with information about products and services which we believe may be of interest
We may use your personal information to inform you about other products and services, discounts, special offers, competitions and invitations to special events that we think might benefit you. Where we send you an offer relating to the products and services of other organisations, we keep control over the information. We do not give, rent or sell your personal information to other organisations so that they can direct market to our customers.

To allow you to decline product offers ('Opt-Out')
We recognise the importance of providing you with choices by giving them an easy means to 'Opt Out' from receiving marketing offers. Let us know if you do not want to receive these offers by contacting us on (03) 9646 3362.

To obtain your feedback
We may contact you from time to time in order to seek your opinion on how we do things and on matters relating to passenger transport, including road safety and other motoring related issues.

4. Who we disclose your personal information to
Unless we have told people otherwise at the time of collection or subsequently, or a legal exemption applies, we will only disclose your personal information to third parties:

a) where it is relevant for the purpose and uses described above;
b) where they are our contractors and business partners;

c) as otherwise described below.

This includes:

The Secretary of the Department and Transport or officers of Safe Transport Victoria
We may disclose your personal information to the Secretary of the Department and Transport or officers of Safe Transport Victoria to ensure the proper operation of Victoria's roadworthy scheme, and any other relevant government regulator such as Digital Victoria (CIRS), OVIC, the Australian Cyber Security Centre and OIAC, including the uses set out above.

Third parties like claims processers, insurance providers, statutory investigators etc
We may also disclose your personal information to a third party to assist us to deal with complaints, disputes or conflict arising from or as a consequence of your access to, or use of, the Services, and to enforce our rights, prevent unlawful activity.

Contractors
We may contract with other parties to provide some of part of our Services on our behalf.

Business Partners
In some cases, we work with other parties to seek to improve our Services, or develop new or improved products or services.

Disclosing your personal information interstate and overseas
We will not disclose information to entities located interstate and in countries outside Australia without your prior written consent, and, where the information relates to the roadworthy scheme, the Secretary of the Department's consent.

Sharing non-personal information
We may share non personal, aggregate, or summary information about people with our business partners or other third parties.

5. Security of personal information
We use technology, documented employee procedures and internal monitoring to help ensure that your personal information is protected and secure. For example, our employment agreements and our Employee Handbook impose clear confidentiality requirements on our employees and contractors, whilst our Information Technology Policy provides for the security of information including personal information in various ways.

Our employees and contractors can only make use of such information to perform their functions.

Further, we only allow access to those employees and contractors who have a genuine operational need to conduct their employment responsibilities. A list of such people is maintained by us, and is reviewed regularly every 12 months, and updated every time such a person leaves employment with RSI – at which their access is removed within 24 hours.

The personal information that we hold is identified in the Table at Attachment 1, and recorded and stored in the manner set out that Attachment. The information is also protected using the security measures listed in Attachment 1, including the information held electronically, which is protected through the use of encrypted passwords and storage on secure servers housed in controlled environments to protect against loss, misuse or alteration of your information.

Incidents relating to data breaches and data incidents are to be handled in accordance with point 8 of this document, and Security Incidents, as defined in the Dealer Certification Scheme Agreement between BusVic and the Department of Transport and Planning, are to be handled in accordance with point 9 of this document.

Risk management principles have been applied to generate this document, including identifying the personal information captured, the risks that may apply, both to physical records and electronic records, assessing the risks and applying appropriate security measures. The outcome of such a risk process is set out in Attachment 1. This process and the attached document will be reviewed annually to ensure that it remains adequate for the risks being faced.

Further, a formal review of our RSI's business IT systems will be organised by RSI-GM annually.

The assets, including computers and databases, are owned by us. An asset register is used for all device's used to access information which may include personal information.

If there was business disruption and an issue with RSI's business IT systems, RSI has separate devices that can be utilised to ensure inspection and registration services continue.

How long do we keep information?
We will keep your information for as long as it is necessary to continue to provide our Services or to service an account.

Our employees and training
We provide training and communications programs designed to educate employees about the meaning of relevant privacy legislation, and this privacy policy.

6. Information quality and your rights of access and correction

Quality
We use technology, documented employee procedures and internal monitoring to help ensure that personal information is accurate and kept up-to-date.

Access
For security purposes, when you contact us to request access to your personal information, you will need to provide us with enough information to enable us to verify your identity. Depending on the nature of the request, we may ask you to complete a form and in some cases, as permitted by law, we may charge you a service fee for providing this information.

Where we charge a fee, this will be to cover costs such as postage or materials involved in providing you with access to your information. We will inform you of any relevant charges at the time of your request. We will generally provide you with access to your personal information that we hold about you, but sometimes that will not be possible, in which case, we will give you a written notice explaining why.

Correction
If you believe that any information we hold about you is inaccurate we ask that you contact us to let us know. You can contact us on (03) 9646 3362. We will take reasonable steps to correct your information, but if we don't correct your personal information we will give you a written explanation as to why.

7. How to complain about a possible breach of privacy
If you believe that we have breached your privacy or you have any questions in relation to this privacy policy you can contact us on (03) 9646 3362. We will promptly acknowledge your complaint, investigate it and determine the steps we will undertake to resolve your complaint within a reasonable time. We will contact you if we require any further information and will provide you with our determination once it is made.

8. Notification of data breaches and incidents

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse; a data incident an unauthorised action (including threat of, or attempt at, such action) by a person (whether known or unknown) that is, or if successfully completed, reasonably likely to be an attack, penetration, denial of service, misuse of system access, unauthorised access or intrusion (hacking), virus intrusion or scan of systems, networks, technology, content or websites), that results in, or if successfully completed is reasonably likely to result in, a data breach or adversely affect an on-line system. Data breaches and incidents can be caused or exacerbated by avariety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

All staff will follow the data breach response plan (response plan) set out in the BAV Human Resources Handbook applicable as at the relevant date.

In addition, RSI General Manager must immediately notify the Secretary of DTP if the GM becomes aware that there has been, or suspects that there may have been, a data breach or data incident, and must provide the Secretary with all information of which he is aware about: a. the nature and circumstances (including time and place) of; and b. the person or persons responsible for – the data breach or data incident or suspected data breach or data incident.

The GM must also provide to the Secretary, in a manner and within the time reasonably specified by the Secretary: a. such further information about a data breach or data incident, or suspected data breach or data incident, as the Secretary requires; and b. all reasonable assistance requested by the Secretary to investigate, or mitigate the effects of, a data breach or data incident, or suspected data breach or data incident. Where the Secretary requires, the GM must notify a data breach or data incident, or suspected data breach or

data incident to the Privacy Commissioner and such other persons that the Secretary directs and shall do so in accordance with the Secretary's reasonable directions (whether or not the GM is required to make the notification under a Privacy Law).

Data security practices and processes
The GM will implement practices and processes to ensure compliance with this clause and under Privacy Law. The data and current protections are as set out in Attachment 1. Without limitation, such practices and processes: a. sufficiently identify and protect against risks of complete or partial loss, destruction or corruption, or unauthorised (whether malicious or accidental) access, disclosure, alteration or deletion, of scheme personal information; b. be consistent with good industry practice; and c. ensure that up-to date protection against viruses, malware and other threats to the security and integrity of scheme personal information are maintained.

The GM must immediately inform the Secretary if they become aware of any complaint concerning the RSI's handling of personal information relating to the Scheme and promptly comply with any reasonable directions of the Secretary in relation to: i. the handling, management or protection of personal information by the Licence Holder; ii. any actual or alleged interferences with privacy or breaches of Privacy Law in relation to scheme personal information; iii. a complaint concerning the handling of scheme personal information; and iv. an investigation or the exercise of other functions by the Privacy Commissioner.

9. Security Incident Response in relation to Registrations
The GM will also follow the requirements for Security Incidents as defined and provided for in the Dealer Certification Scheme Agreement between us and the Department of Transport and Planning – and set out in Attachment 2 for ease of reference.

10. Availability and revisions of this privacy policy
We will ensure this privacy policy is available at https://www.busvic.asn.au/road-safety-inspections-0.

We may change this policy from time to time. If we do so, we will issue a notice via our website https://www.busvic.asn.au/road-safety-inspections-0. Please check for updates and changes.

ATTACHMENT 1

Personal Information - Inspection and Registration of Vehicles

VEHICLE INSPECTIONS			
Personal Information	**Recorded in**	**Stored**	**Security measures**
Presenter/Customer Name Presenter/Customer Address Presenter/Customer Licence No. (**Bus, Truck and Car**)	Ticker Sheet	Kept in compactor in RSI's main building.	<u>After hours</u>: Locked. Key entry. Only GM/ two administrator officers in front office have key. Building has alarm system. <u>During work hours:</u> Access is monitored by administration assistants in the front office.
Presenter Name RSI Inspector Name (**Bus, Truck and Car**)	Certificate of Roadworthiness - **Pass**	VicRoads eCerticate system Attached to Ticker Sheet.	Information input directly into eCertifcate system in real time. See security measures for Ticker Sheet.
Presenter Name Presenter Phone Number (**Bus, Truck and Car**)	Certificate of Roadworthiness - **Fail**	VicRoads eCerticate system Attached to Ticker Sheet.	Information input directly into eCertifcate system in real time. See security measures for Ticker Sheet, which applies to both Certificate and attached Ticker Sheet.
Individual Presenter Name Presenter Address Presenter Phone Number	Certificate of Roadworthiness from VicRoads Roadworthy Book - **Pass**	Kept in compactor in RSI's main building.	See security measures for Ticker Sheet, which applies to both Certificate

RSI Inspector Name and Signature Company Phone No. **Corporate** Presenter Name RSI Inspector Name and Signature Company Phone No. (Bus only: Customers nominate a specific employee as the 'presenter' of vehicle for that customer – the name of the presenter, and a photograph of their licence are kept in a separate hard copy RSI folder. In these circumstances, it is the corporate name of the presenter, its address and corporate phone number that appears on the bus certificate of roadworthiness.) (**Bus, Truck and Car**)			and attached Ticker Sheet.
Individual Presenter Name Presenter Address Presenter Phone Number Presenter Licence Number Presenter Signature RSI Inspector Name and Signature Company Phone No. **Corporate** Presenter Name (RSI Inspector manually writes on Certificate; and 'On file' where Presenter's Licence is to go.) RSI Inspector Name and Signature Company Phone No.	Certificate of Roadworthiness from VicRoads Roadworthy Book - **Fail**	Kept in compactor in RSI's main building.	See security measures for Ticker Sheet.

(Explanation above applies here too.) (**Bus, Truck and Car**)			
Individual Presenter Name Presenter Address Presenter Phone Number RSI Inspector Name and Signature Company Phone No. **Corporate** RSI Inspector Name and Signature Company Phone No. (Customers nominate a specific employee as the 'presenter' of vehicle for that customer – the name of the presenter, and a photograph of their licence are kept in a separate hard copy RSI folder. In these circumstances, it is the name of the corporate name of the customer, its address and corporate phone number that appears on the bus certificate of roadworthiness.) (**Bus**)	Bus Certificate of Roadworthiness - **Pass**	RSI's IT system – Codeworthy – Webbrowser/App (Device)	See below.
Individual Presenter Name Presenter Address Presenter Phone Number Presenter Licence Number Presenter Signature RSI Inspector Name and Signature **Corporate** Presenter Name (RSI Inspector manually writes on Certificate; and 'On	Bus Certificate of Roadworthiness - **Fail**	RSI's IT system – Codeworthy – Webbrowser/App (Device)	See below

file' where Presenter's Licence is to go.) RSI Inspector Name and Signature Company Phone No. (Explanation above applies here too.) (**Bus**)			
Customer's default name Presenter's Name Customer's Garage Address/Which is Possible Personal Address (e.g., sole trader) Customer's Corporate Address/Possible Personal Address (e.g., sole trader) Customer's Company Phone Number/Possible Personal Phone Number (e.g., sole trader) **(Bus)**	Bus Certificates of Roadworthiness	RSI's IT system – Codeworthy – Webbrowser	Edit access restricted to GM, 2IC and two administration officers. View access all inspectors.
Customer's default name Presenter's Name Customer's Garage Address/Which is Possible Personal Address (e.g., sole trader) Customer's Corporate Address/Possible Personal Address (e.g., sole trader) Customer's Company Phone Number/Possible Personal Phone Number (e.g., sole trader) **(Bus)**	Bus Certificates of Roadworthiness	RSI's IT system – Codeworthy – App (Device)	Inspectors access via android security pattern. At Port Melbourne: Locked in cupboard overnight – GM and administration officers have access with key. Off-site – Kept in vehicles overnight.
Photographs of Bus Certificate of Roadworthiness – which may include personal information set out above. Presenter Name Presenter Address Presenter Phone Number	Bus Certificates of Roadworthiness	RSI's IT system – Codeworthy – Sharepoint	

Presenter Licence Number **(Bus)**			
Photographs of Certificate of Roadworthiness and Bus Certificate of Roadworthiness (Bus, Truck, Car) – which may include personal information set out above. Presenter Name Presenter Address Presenter Phone Number Presenter Licence Number **(Bus, Truck and Taxi)**	Certificates of Roadworthiness	'I' Drive	Access restricted to GM, 2IC and two administration officers.
Presenter's Name Customer Credit Card details except CVC No. Presenter's name RSI Inspector's Name	Specific RSI Form	Paperwork kept with Inspector	Regional testing: This information is provided to RSI's administration assistants by the RSI Inspector who collected it, used by the assistant to issue an invoice and obtain CVC directly from customer, then the Form is destroyed. Form kept in car/hotel room. Receipt created and affixed to invoice.
Presenter's Name Customer Credit Card details and CVC No.	In person	In person	Port Melbourne testing. RSI's administration assistants' complete transaction using EFTPOS.
VEHICLE REGISTRATIONS			

Presenter Name Presenter Address Presenter Phone Number Presenter Licence Number Presenter Signature	Dealer On-Line Authority to Register Form (printed out) Dealer Vehicle Registration Form Ad-hoc Authority to Act on behalf of Registrant Form.	Cupboards in RSI main facility.	RSI Building locked overnight; alarm system.

ATTACHMENT 2

11.16 Security Incident Response
(a) If the Provider or any Associate suspects or is advised that there may have been a Security Incident, the Provider:

(i) must take (including by ensuring any impacted Associates take) all reasonable steps to immediately contain the suspected Security Incident (e.g. stop the unauthorised practice, recover the records, shut down the system etc); and
(ii) must promptly undertake or have appropriate Associates undertake (including by ensuring any impacted Associates promptly undertake) a Security Incident Assessment.

Security Incident Assessment
(b) The Security Incident Assessment must assess whether Scheme Personal Information has been used, disclosed or accessed in a manner inconsistent with the Purpose. If it has, the Provider must provide the Secretary with a Security Incident Notification in accordance with the timeframe specified below. Any Security Incident Notification under the Security Incident Response must include the particulars of the Security Incident and the Provider's (proposed) response, including immediate containment and risk minimisation measures, as appropriate.

(c) The Security Incident Assessment must:
(i) be undertaken reasonably: the standard is how a reasonable and impartial person would assess the situation.
(ii) be completed as quickly as possible and within 10 Business Days maximum.
(iii) not delay the taking of appropriate remedial action to minimise the extent of the Security Incident.

(d) The Security Incident Assessment should cover whether the information was lost or stolen or misused. If there may be criminal activity involved, the police should be notified as soon as possible. In this case, the Provider must provide advance warning to the Secretary, by email marked "Urgent" or telephone, before the notification to police. The advance warning does not need to be a formal Security Incident Notification.

(e) The Security Incident Assessment should identify who or what was responsible for the Security Incident, plus any Associate involved in the Security Incident, and whether any identified Associate has been involved in any previous Security Incident. Such Associate information should not be included in the Security Incident Notification.

(f) The Secretary may contact the Security Representative, seeking information about the Security Incident, including information about Associate involvement in the Security Incident on a confidential basis, and the Security Representative must cooperate. The Provider is responsible to ensure that its contractual relationships with Associates allow this provision of information to the Secretary. The Provider acknowledges that the Secretary may apply Scheme Personal Information access

restrictions or other technical controls to individual Associates, if the Secretary considers that is appropriate.

(g) If the Secretary rates the information as 'Official: Sensitive' or higher and the Provider is required to notify OVIC or OAIC, the Provider must complete a Regulator Incident Notification Form with as much detail as possible including all planned rectification and notification activities and provide it in draft form to the Secretary within 10 Business Days after the Security Incident. The Provider must not notify the relevant regulator until after providing the draft notice to the Secretary (preferably at least 5 Business Days after if regulator timeframes allow), or until the Secretary gives written consent to the Provider to proceed, whichever is sooner.

(h) Following OVIC or OAIC notification, should the regulator contact the Provider or its Associate directly, the Provider must immediately notify the Secretary by email of the contact and provide the details of the regulator contact and any requests made, and provide the draft response to the Secretary within 3 Business Days after the date the relevant regulator makes direct contact. The Provider must not respond to the relevant regulator until at least 5 Business Days after providing the draft notice to the Secretary, or until the Secretary gives written consent to the Provider to proceed, whichever is sooner.

(i) The Provider (including its Associates) must be careful not to destroy any evidence relating to the potential Security Incident.

(j) If the Provider or Secretary consider that customer notification is warranted, they will consult on the format and timing for that notification, and act in good faith to reach an agreed approach. The Provider will use reasonable endeavours to ensure that it and its Associates act consistently with that agreed approach.

Timeframe for Security Incident Notification

(k) If the Scheme Personal Information was stolen, or may be affected by a Cyber Attack, or if a large number of Scheme Personal Information records containing Personal Data are affected (>100), the Provider's Representative must email the Secretary a Security Incident Notification within 24 hours of first becoming aware of the relevant fact or incident. The Provider must promptly comply with any directions from the Secretary in response to that Security Incident Notification.

(l) Otherwise, the Provider should take appropriate remedial action and investigate the incident and provide the Secretary with a Security Incident Notification within 10 Business Days.

Cyber Attack

(m) In the event of a Cyber Attack, the Provider must allow (and must ensure that its Associates allow) the Secretary and other government bodies such as Digital Victoria (CIRS), OVIC, the Australian Cyber Security Centre and OAIC, and third parties nominated by the Secretary to have full visibility of and be involved in incident response, incident analysis, incident recovery and post-incident reviews, as well as

request and receive copies of breached data sets.

(n) The Secretary reserves the right to recover from the Provider the cost of the involvement of any of these parties, or any remediation activity that the Secretary reasonably chooses to undertake as a result of the Cyber Attack.

(o) The Provider must take all reasonable steps to minimize the impact of the Cyber Attack and to prevent a continuation, expansion or repeat of the Cyber Attack.

Incident rectification report

(p) The Provider must provide the Secretary with an incident rectification report within 60 days after a Security Incident Notification, outlining its progress in rectifying issues raised in the Security Incident Notification (and must continue to provide incident rectification reports at intervals of 60 days until all issues raised in the Security Incident Notification are rectified to the Secretary's satisfaction).