PICKERINGS Group of Companies

DATA BREACH RESPONSE PLAN

Bundaberg Motors Pty Ltd ACN 098 931 849

Key Definitions

1. **APP** – means the Australian Privacy Principles as set out under the Privacy Act.

2. **Eligible Data Breach** – An Eligible Data Breach will have occurred where:

   (a) There is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by Pickerings; and

   (b) The access, disclosure or loss is likely to result in Serious Harm to any of the individuals to whom the information relates.

3. **My Health Records Act** – means the *My Health Records Act 2012* (Cth).

4. **Personal Information** – means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

   (a) Whether the information or opinion is true or not; and,

   (b) Whether the information or opinion is recorded in a material form or not.

5. **Pickerings –** means Bundaberg Motors Pty Ltd ACN 098 931 849

6. **Privacy Act** – means the *Privacy Act 1988* (Cth).

7. **Privacy Officer** – means the person specified in **Schedule 1** of this Response Plan, being the person acting as Picking's first point of contact for advice and action on privacy matters and who is responsible for carrying out functions to assist Pickerings in complying with Australian privacy legislation.

8. **Response Plan** – means *this* document and all information and procedures contained herein.

9. **Serious Harm** – In determining what constitutes "Serious Harm", regard should be given to:

   (a) The kind or kinds of information being dealt with (for example, Pickerings could potentially take action to remediate the risk to an individual arising from a data breach involving information that can be re-issued, such as a compromised password, but cannot change permanent information such as the individual's date of birth or medical history);

(b) The sensitivity of the information (for example, the unauthorised access of a person's medical records may place an individual at a high risk of serious harm);

(c) Whether the information is protected by one or more security measures (for example, if Pickerings' detection and prevention systems detect an attack on its IT networks, Pickerings should consider whether the network security mechanisms would have been likely to have prevented the attacker from accessing the relevant personal information);

(d) If the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome;

(e) The persons, or kinds of persons, who have obtained, or who could obtain, the information (for example, access by, or disclosure to, a known and trusted party is less likely to cause serious harm than access by, or disclosure to, an unknown party);

(f) If a security technology or methodology:

(i) was used in relation to the information; and

(ii) was designed to make the information unintelligible or meaningless (for example, through encryption) to persons who are not authorised to obtain the information;

(g) The likelihood that the persons, or the kinds of persons, who:

(i) have obtained, the information; and

(ii) have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;

have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology referred to in paragraph (f) above;

(h) The nature of the harm; and

(i) Any other relevant matters-

(i) Please note that not all of the matters listed above will necessarily be relevant in all circumstances. Whilst in some circumstances one of the above matters may be determinative in reasonably identifying whether serious harm is likely to be caused to any individuals, in other cases, it may be reasonable to reach a conclusion considering a number of the relevant matters as a whole.

(ii) Additionally, the above list of matters is not exhaustive, and any other matters that may be relevant to the particular circumstances should be considered when reaching a reasonable conclusion of whether any individuals may be at risk of incurring serious harm as

result of any unauthorised access, unauthorised disclosure or loss of personal information.

Overview:

On 22 February 2018, a mandatory data breach notification regime (**Regime**) came into force under the Privacy Act. The Regime will apply to Pickerings as it is an APP entity subject to the APPs, including the security obligations set out in APP 11.1. The Regime requires Pickerings to take certain steps in response to Eligible Data Breaches of the Personal Information it holds.

To comply with the Privacy Act and Regime, Pickerings has adopted the following plan to be followed in the event that it suspects that there has been an Eligible Data Breach.

Data Breach Response Procedure

1. If any staff member of Pickerings suspects that an Eligible Data Breach may have occurred, that staff member must immediately notify the Privacy Officer of the suspected breach.

2. The Privacy Officer will, as soon as possible (but no later than 30 days after becoming aware of the suspected Eligible Data Breach), assess whether there are reasonable grounds to believe that an Eligible Data Breach has (or may have) occurred (**Assessment**). In completing the Assessment, the Privacy Officer should complete an entry in the Data Breach Register contained in **Appendix A** of this Response Plan.

3. When conducting the Assessment, the Privacy Officer will consider what personal information the breach involves, what the cause of the breach was, the extent of the breach, what harm could be caused by the breach and whether/how the breach may be contained.

4. If, after completing the Assessment, the Privacy Officer considers that there are reasonable grounds to believe that an Eligible Data Breach has taken place, the Privacy Officer will (and may consult any relevant personnel in doing so) consider and advise the management of Pickerings (**Management**) of whether:

    (j) Any serious harm has been, or is likely to be, caused to any individuals as a result of the Eligible Data Breach; and

    (k) If it is likely that no serious harm has yet been caused to any individuals, whether any action can be taken to reduce the likelihood of, or eliminate the possibility of, any harm being caused to any individuals.

5. The Privacy Officer will inform Management of, and will be responsible for implementing, any action that may be taken to reduce the likelihood of, or eliminate the possibility of, serious harm being caused to the relevant individuals.

6. If the Privacy Officer deems that no action can be taken to remedy the Eligible Data Breach, please proceed to paragraph 8.

7. If, as a result of the action referred to in paragraph 5 above, the Privacy Officer and Management are satisfied that a reasonable person would conclude that:

(a) There has been no unauthorised access to, unauthorised disclosure of, or loss of, the personal information; or

(b) The unauthorised access to, unauthorised disclosure of, or loss of, the personal information, would not be likely to result in any serious harm to any relevant individuals,

Pickerings will not need to take any further steps.

8. If, following the Privacy Officer's Assessment, it is concluded that an Eligible Data Breach has occurred and no remedial action can reasonably prevent the risk of serious harm being caused to any individuals (or if directed to do so by the Privacy Commissioner), then the following steps will be taken.

9. The Privacy Officer will prepare a statement (**Statement**) setting out:

(a) Pickerings' name and contact details;

(b) A description of the Eligible Data Breach;

(c) The kind or kinds of information disclosed, lost and/or to which unauthorised access was obtained;

(d) Recommendations about the steps that individuals should take in response to the Eligible Data Breach; and

(e) If there are reasonable grounds to believe that one or more other entities have committed an Eligible Data Breach in relation to the information, then the identity and contact details of those entities may be included.

A template version of the Statement is attached in **Appendix B** of this Response Plan.

10. The Privacy Officer will, as soon as practicable after preparing the Statement:

(a) Provide a copy of the Statement to the Privacy Commissioner;

(b) If practicable to notify the contents of the Statement to the individuals about whom the information relates and/or any individuals who are at risk from the Eligible Data Breach, take reasonable steps to notify the contents of the Statement to these individuals (a template Statement notification to be provided to affected individuals is attached in **Appendix C** of this Response Plan); and

(c) If it is not practicable to notify the individuals under 10 (b) above, then the Privacy Officer will:

(i) Arrange for a copy of the Statement to be published on Pickerings' website (if applicable); and

(ii) Take reasonable steps to publicise the contents of the Statement.

Exceptions to requirement to notify

1. **Eligible data breaches of other entitles**

   (a) If Pickerings takes the steps above (meaning the preparation of the Statement and the notification of its contents to the relevant individuals) and the access, disclosure or loss constituting the Eligible Data Breach is an Eligible Data Breach of one or more other entities, then the other entities will not be required to take these steps. Similarly, if another entity takes the steps above and the entity's Eligible Data Breach is also a breach of Pickerings, then Pickerings will not be required to take these steps.

   (b) This exception is intended to apply in circumstances where, for example, Pickerings and another entity jointly and simultaneously hold the same particular record of information (e.g. due to an outsourcing arrangement), and it seeks to avoid the doubling-up of the notification obligations.

2. **Data breaches concerning health records**

   (a) If an unauthorised access to, disclosure of, or loss of personal information has been, or is required to be, notified under section 75 of the My Health Records Act, then the mandatory data notification regime will not apply in relation to such access, disclosure, or loss of information.

   (b) The purpose of this exception is to avoid imposing a double notification requirement if any unauthorised access, unauthorised disclosure, or loss of personal information has been, or is required to be, notified under the My Health Records Act.

3. **Enforcement related activities**

   (a) The Regime provides an exception to the requirement to take the steps above in relation to enforcement related activities. However, this exception will not apply to the conduct of Pickerings, as it is not an enforcement body within the meaning of the Privacy Act.

4. **Inconsistency with secrecy provisions**

   (a) For the purposes of the Regime, "secrecy provision" means a provision of a law of the Commonwealth that prohibits or regulates the use or disclosure of information.

   (b) If compliance by Pickerings with the requirement to provide the Privacy Commissioner with the Statement or to notify the affected individuals of the contents of the Statement would be inconsistent with any secrecy provision (other than any secrecy provisions prescribed by the *Privacy Regulation 2013* (Cth), Pickerings will not be required to take those steps.

   (c) This exception is likely only to apply in very limited circumstances.

5. **Declaration by Privacy Commissioner**

(a) If the Privacy Commissioner becomes aware that there are reasonable grounds to believe that there has been an Eligible Data Breach by Pickerings, or if Pickerings informs the Privacy Commissioner of such grounds, the Privacy Commissioner may declare that:

(i) Pickerings is not required to prepare a Statement (and is therefore not required to provide one to the Commissioner or to notify any individuals); or

(ii) Pickerings and any other entities that have been involved in the eligible data breach, must notify any affected individuals within a specified period of time.

(b) The Privacy Commissioner is only permitted to make either of the declarations above if they are satisfied that it is reasonably practicable to do so, having regard to the public interest, any relevant advice provided by an enforcement body or the Australian Signals Directorate of the Defence Department, and any other relevant matters.

(c) The Privacy Commissioner may make either declaration on its own initiative or upon the application of Pickerings. If Pickerings applies for a declaration, the Privacy Commissioner will not be required to make the declaration and must provide written notice to Pickerings if they refuse the application.

(d) If Pickerings makes an application to the Privacy Commissioner for a declaration in accordance with the paragraphs above, then Pickerings will not be required to prepare a Statement or to notify any individuals of the contents of the Statement until the Privacy Commissioner has responded to the application.

Contracting with third parties

1. Ideally, Pickerings should ensure that its privacy obligations are included in any and all contracts or agreements with third party service providers, contractors, marketing agencies etc. (including those located overseas, if any) (together, **Third Party Providers**).

2. The sample contract clause provided in **Appendix D** of this Response Plan should be inserted by Pickerings in all future contracts with Third Party Providers.

3. In the event third party contracts are already on foot, or if existing contracts prove difficult to amend, it is recommended that Pickerings request Third Party Providers sign the Privacy Acknowledgement and Undertaking provided in **Appendix E** of this Response Plan.

PICKERINGS
Group of Companies

Schedule 1

Privacy Officer Information:

Name	
Position / Title	**PRIVACY OFFICER**
Contact Phone Number	
Email	
Company/Organisation Address	**Bundaberg Motors Pty Ltd ACN 098 931 849**
Address for Service	

APPENDIX A

Data Breach Register

To be completed in accordance with procedure set out in Response Plan

Date of Incident	Details of Incident	Date became aware of incident	Is serious harm suspected?	Date Assessment commenced	Date Assessment due (30 days from awareness)	OAIC and affected individuals notified?	Date Incident closed

Appendix B

[To be printed on Pickerings' letterhead]

Australian Privacy Commissioner
Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

[insert date]

Dear Sir/Madam,

NOTIFICATION OF ELIGIBLE DATA BREACH

We are writing to notify you that Bundaberg Motors Pty Ltd (**Pickerings**) has reason to believe that an eligible data breach has occurred in relation personal information held by Pickerings.

In particular, we advise of the following details in relation to the suspected eligible data breach:

(a) [insert a description of the eligible data breach];

(b) [insert a description of the kind or kinds of information concerned];

(c) [insert a description of what [insert client name] has done in response to the eligible data breach];

(d) [insert Pickerings' recommendations about the steps that individuals should take in response to the eligible data breach].

[If there are reasonable grounds to believe that one or more other entities has committed an eligible data breach, then this may be included as a fifth point above, along with identity and contact details of this entity]

[NB: Select one of the two following paragraphs, as applicable]

[We confirm that Pickerings is currently taking reasonable steps to notify any individuals about whom the information relates and/or any individuals who may be at risk from the eligible data breach of the content of this notification.]

OR

[It is not practicable for Pickerings to notify the individuals about whom the information relates or any individuals who may be at risk from the eligible data breach. However, we confirm that Pickerings is in the process of publishing this notice on its website and is currently taking reasonable steps to publicise the contents of this notice].

If you have any questions or require any further information, please contact [insert name of Privacy Officer] using the details below.

Regards,

[Sign-off]

Appendix C

[To be printed on Pickerings' letterhead]

Dear [insert "name" or "valued customer" or otherwise an appropriate greeting],

We are writing to you to let you know that on the [day] of [month], [year], Pickerings experienced a data breach. As a result [insert **preliminary** details of the Eligible Data Breach]. Upon becoming aware of the data breach, Pickerings] immediately [insert **preliminary** details of action taken, e.g. closed the data breach and investigated the breach].

The data breach

[insert **full** details of the breach & related specifics, e.g. Our investigations indicated that a third party was able to gain access to our data systems through a third-party provider.]

What data was involved?

[insert **full** details of the kind of information involved, e.g. We have determined that the attack was able to access customer names, emails and encrypted passwords. We are confident that no credit card information was accessed.]

What we are doing in response

[details of the action taken by the organisation, e.g. We are notifying individuals of the data breach, stopped the data breach, and investigating the matter.]

What steps you should take

[insert recommended steps the user should take, e.g. The passwords accessed were encrypted and were not revealed. However, we recommend that you change your account's password and on other accounts where you use the same password.]

Other parties involved *(delete if not applicable)*

[if the data breach affected other entities: We believe the data breach also affected [other organisation name]. For more information, contact them at [contact details for other organisation].

Need to know more?

[insert at a minimum: (1) Privacy Officer contact information; (2) Office of the Australian Information Commissioner website and contact information; and, (3) company contact information]

[Insert client sign off]

Appendix D

Privacy

[Contractor] agrees to:

(a) comply with the *Privacy Act 1988* (Cth) (**Privacy Act**) (including the Australian Privacy Principles) in relation to any and all personal and sensitive information that it may collect, receive, have access to, hold, use, store, disclose and destroy in connection with this [Agreement / Contract]; and

(b) notify Bundaberg Motors Pty Ltd immediately if it has reasonable grounds to believe that an eligible data breach under the Privacy Act has or may have occurred, and take all steps necessary to assist Bundaberg Motors Pty Ltd to comply with Part IIIC (notification of eligible data breaches) of the Privacy Act; and

(c) indemnify Bundaberg Motors Pty Ltd on demand from and against any liability incurred by Bundaberg Motors Pty Ltd as a result of [Contractor]'s breach of the Privacy Act.

Appendix E

PRIVACY ACKNOWLEDGEMENT AND UNDERTAKING

.....,

of .....[address]

undertakes Bundaberg Motors Pty Ltd ACN 098 931 849 (**Pickerings**) the following:

1. I/It will comply with the *Privacy Act 1988* (Cth) (including the Australian Privacy Principles) in relation to any and all personal and sensitive information about Pickerings' customers that I/it may collect, receive, have access to, hold, use, store, disclose and destroy; and
2. I/it will comply with Pickerings' privacy policies and procedures as communicated to me/it from time to time;
3. I/It will not disclose any personal information about Pickerings' customers to any third parties without prior consent from Pickerings;
4. I/It will notify Pickerings immediately if it has reasonable grounds to believe that an eligible data breach under the Privacy Act has or may have occurred, and will take all steps necessary to assist Pickerings to comply with Part IIIC (notification of eligible data breaches) of the *Privacy Act 1988* (Cth); and
5. I/it will indemnify Pickerings on demand from and against any liability incurred by Pickerings as a result of my/its breach of the Privacy Act.

DATED: .....

SIGNED: .....
For and on behalf of .....