Data Breach

Purpose

This policy outlines the approach of the National Heavy Vehicle Regulator (**NHVR** or **the Regulator**) to identifying, reporting, and managing Eligible Data Breaches in compliance with the *Mandatory Data Breach Notification* (**MDBN**) scheme under the *Information Privacy Act 2009* (Qld) (**IP Act**).

Background

The MDBN scheme includes requirement for the NHVR to undertake the following in response to a data breach, including an Eligible Data Breach:

- immediately take all reasonable steps to contain and mitigate the data breach
- if the NHVR does not know if the data breach is an Eligible Data Breach, assess within 30 days whether there are reasonable grounds to believe that the data breach is an Eligible Data Breach
- notify other affected agencies
- if the NHVR knows or assesses the data breach as an Eligible Data Breach, notify the Office of the Information Commissioner (OIC) and any individuals whose personal information is the subject of the data breach, unless an exemption to notification applies.

The MDBN scheme also requires agencies to prepare and publish a *Data Breach Policy*.

Scope

This policy applies to all employees, contractors, and third-party service providers of the NHVR.

Policy statement

1. The NHVR is committed to safeguarding the Personal Information it receives and handles and is committed to complying with the IP Act.
2. The NHVR will ensure that all employees, contractors, and third-party service providers are made aware of their responsibilities in data protection and breach management.
3. The NHVR is committed to being transparent in its data handling and breach management, promptly informing affected individuals about breaches and their potential impacts.
4. The NHVR will adopt a proactive stance on data protection by implementing preventive measures, providing regular training, and monitoring systems for vulnerabilities to reduce breach risks.
5. The NHVR will promote collaboration among all stakeholders, including employees, contractors, and third-party service providers, to ensure a coordinated response to data breaches.
6. The NHVR is dedicated to learning from data breaches and near misses, conducting post-incident reviews to identify lessons learned and enhance policies and procedures.

Approach

Eligible Data Breach

7. A **data breach** is unauthorised access or disclosure of information held by the NHVR or the loss of personal or non-personal information held by the NHVR where unauthorised access or disclosure is likely to occur.
8. Personal Information is held by the NHVR if the Personal Information is contained in a document in the possession or under the control, of the NHVR.
9. An **eligible data breach** always involves Personal Information and involves an actual or potential loss of unauthorised access to, or unauthorised disclosure of Personal Information, which is likely to result in serious harm to one person or more (criteria for assessment outlined below).

Preparedness

10. Preparation is the foundation of the NHVR's data breach response, which ensures a proactive approach to security of Personal Information and, in the event of data breach, reduces triage and response times and positions the NHVR to take timely action.
11. The NHVR has an established approach to the management of Personal Information, the underpinning principles of which are contained in the *Privacy Policy*.
12. The NHVR has an established approach to cyber and information security, as well as risk management. These approaches are aligned to the ACSC Essential Eight, ISO:27001:2022 – Information Security Management Systems, and ISO:31000:2018 – Risk management.
13. The NHVR is positioned to comply with obligations under the IP Act, including the following relating to the MDBN scheme:
    a. take all reasonable steps to contain a data breach and mitigate the harm caused by the data breach

b. conduct an assessment within 30 days of knowing or reasonable suspecting an eligible data breach

c. provide written notice of the data breach to any other agency affected by the breach

d. provide statement about the eligible breach to the Information Commissioner and affected individuals and/or publish on the NHVR's website (as applicable)

e. maintain a register of eligible data breaches.

14. The NHVR also:

a. undertakes regular security audits and assessments to identify potential vulnerabilities

b. has access controls and monitors systems, as necessary

c. provides awareness and training, as necessary, of NHVR employee about identifying and reporting data breaches

d. has an establish approach to handling and escalating any suspected data breaches.

Identification

15. The NHVR has established processes to identify and report data breaches and suspected data breaches, which include:

a. technical controls, such as intrusion detection systems, encryption, etc

b. monitoring services, geared towards checking, observing, tracking, recording and/or evaluating use of the information and technology services, facilities, and devices, as necessary

c. conducting audits and reviews, to identify vulnerabilities and ensure compliance with data protection standards

d. providing awareness and training sessions for NHVR employees to understand how to identify, respond to, and manage data breaches, with evaluations to improve awareness and response capabilities.

16. The NVHR's Cyber Security Incident Response Plan includes the process for initating a Cyber Security Incident Response Team, as linked to identification and triaging of data breaches.

17. Those approaches and teams will be leveraged, in the event of eligible data breach, to the extent necessary.

Containing, Assessing, and Managing Data Breaches

18. The NHVR's approach to eligible data breaches is as follows:

a. containment: immediate actions to restrict access to affected systems and prevent further unauthorised access (examples include isolating servers, disabling compromised accounts, and enhancing security measures)

b. assessment: evaluate to determine the breach's nature, scope, and eligibility. In terms of assessing whether a data breach is an eligible data breach, consideration includes the kind of Personal Information accessed, disclosed or lost, the sensitivity of the Personal Information, the persons who have obtained, or who could obtain, the Personal Information, the nature of the harm likely to result from the data breach (see Appendix 1 for data breaches that generally are, or are not, eligible data breaches)

c. management: procedures for notifying affected individuals and authorities, which include enquiries to identify the breach's cause, implementing corrective actions, and undertaking a post-incident review.

Notification

19. The NHVR must:

a. notify the Information Commissioner as soon as practicable after forming the belief that a data breach is an eligible data breach

b. as soon as practicable after forming a reasonable belief that a data breach is an eligible data breach, take the steps set out in the IP Act to notify particular individuals and provide them with the information required.

20. The NHVR will consider each breach to determine whether notification is required, erring on the side of caution that notification should be provided. The NHVR will use best endeavours to ensure notifications include all information listed in sections 51 and 53 of the IP Act (as applicable).

21. If the NHVR cannot directly notify each individual or each affected individual, it will publish the information required by the IP Act on the NHVR's website for a period of at least 12 months. The NHVR will advise the Information Commissioner how to access the notice.

22. After notification requirements are complete, the NHVR will record details of the eligible data breach in the NHVR's Data Breach Register.

23. The NHVR will comply with the above notifications requirements, except where the following exemptions arise under the IP Act:

a. compliance with the reporting obligation(s) would likely prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal

b. the eligible data breach involves more than one agency, and another agency is undertaking the notification obligations

c. the NHVR has taken specified remedial action under section 57 of the IP Act

d. compliance would be inconsistent with a provision of an Act of the Commonwealth or a State that prohibits or regulates the use or disclosure of the information

e. compliance would create a serious risk of harm to an individual's health or safety

f. compliance is likely to compromise or worsen NHVR's cybersecurity or lead to further data breaches.

Responding to Incidents Involving Another Entity

24. In the event of an eligible data breaching involving another agency, the NHVR will seek to establish and oversee procedures for collaborating with that other entity. Key components will likely include:
    a. a plan detailing how information will be shared with other entities, including timelines for notifications and updates
    b. clearly defined roles for NHVR employees and representatives of the other entity in managing the breach response, specifying the primary point of contact for each party.

Requirements Under Agreement with Third Parties

25. The NHVR seeks to ensure that contracts between the NHVR and other parties include obligations related to privacy compliance, which will include terms from 1 July 2025 in relation to data breaches, with appropriate consequences for non-compliance.
26. As part of the NHVR's approach to contract management the NHVR will take reasonable steps to ensure compliance with those contractual obligations.

Post-Incident Review

27. The NHVR will conduct a comprehensive post-incident review after a data breach to evaluate the response and identify opportunities for improvement. This includes:
    a. a review process for identifying and addressing any root causes that contributed to the breach
    b. documentation of findings and recommendations for improvements
    c. conducting reviews for each significant breach to enhance training and policy updates
    d. summarising reviews in regular audits of data protection practices.

Testing and Review Schedule

28. The NHVR will review this Policy annually or following a significant event to incorporate lessons learnt.
29. Testing procedures will include:
    a. conducting simulated data breach scenarios to test the response plan (which may be included as an aspect of broader disaster management or organisation resilience testing)
    b. performing drills that involve key personnel to practice their roles in a data breach response
    c. periodically reassessing the review and testing schedule to ensure it remains appropriate based on changes in regulations, organisational structure, or emerging threats
    d. reviewing the Data Breach Register regularly and keep updated to ensure accuracy and completeness.

Responsibilities

The following positions are responsible for implementing this policy.

Position	Responsibilities
CEO	• Sponsor of this Policy.
Privacy Officer	• Oversees compliance with this Policy. • Promotes awareness of this Policy. • Leads privacy related aspect of data breach enquiries, liaising with the NHVR's Data and Technology Division, as necessary. • Provides notifications to the Information Commissioner and any affected persons, in the event of eligible data breach. • Arranges publication on the NHVR's website, as may be

	required.

Definitions

The following terms are specific to this policy.

Term	Definition
Data breach	As defined in numbered paragraph 7
Eligible data breach	As defined in numbered paragraph 9
Information Commissioner	Queensland Information Commissioner
Personal Information	Means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: (a) whether the information or opinion is true or not (b) whether the information or opinion is recorded in a material form or not.

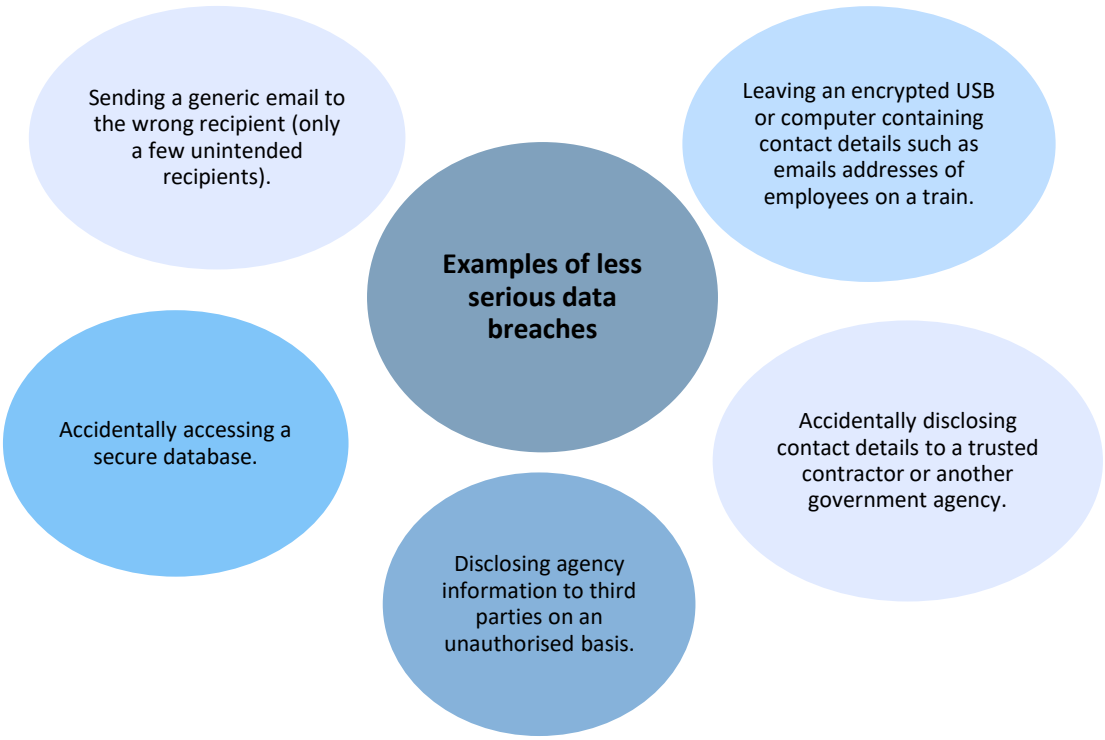
Related legislation and documents

- *Heavy Vehicle National Law Act 2012*

APPENDIX 1

A **Data Breach** can happen in various ways. Examples include by malicious actions of third parties, internally due to human error, or a failure in information handling or security systems. However, not all data breaches will be an Eligible Data Breach and engage the MDBN. See Figure 1 for examples.

Figure 1:



An **Eligible Data Breach** is a Data Breach that involves Personal Information (and may occur internally within the NHVR or involve the unauthorised access and/or disclosure of Personal Information by or to external parties) and any impacted individuals may be seriously harmed. See Figure 2 for examples.

Figure 2: