

Policy manual

PRIVACY POLICY

DATA BREACH RESPONSE POLICY

1.23

Data breaches of personal information are regulated by the Privacy Amendment (Notifiable Data Breaches) Act 2017

What is a data breach? A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.

What is unauthorised access? Unauthorised access of personal information occurs when personal information is accessed by somebody who is not permitted to have access to it. This could include an employee or contractor to whom we have not given permission to access.

What is unauthorised disclosure? Unauthorised disclosure of personal information occurs when confidential information is disclosed to outside parties in a way that is not permitted under the Privacy Act

What is loss of information? Loss of personal information refers to the accidental or inadvertent loss of personal information held by use in circumstances which are likely to result in unauthorised access or disclosure. For an instance, if one of our employees leaves personal information on public transport

To whom do we report data breaches? As required by the Privacy Amendment (Notifiable Data Breaches) Act 2017, we shall report to the Office of the Australian Information Commissioner (OAIC) any data breach that, in the opinion of a reasonable person, is likely to result in serious harm.

How do we assessing the seriousness of a data breach? In assessing whether the data breach is likely to result in serious harm, we shall consider the following information:

- The kind or kinds of information breached;
- The sensitivity of the information breached;
- Whether the information is protected by one or more security measures;
- The persons or kinds of persons who have obtained, or who could obtain the information;
- If a security technology or methodology was used, and whether the technology or methodology was designed to make the information unintelligible or meaningless to persons who are not authorised to access the information;
- The nature of the harm and;
- Any other relevant matters.

What do we advise if we suspect a data breach has or may have occurred?

- Any staff member who has a reasonable suspicion or know that a data breach has occurred must contact **immediately** the Facility Manager

- The Facility Manager will investigate the seriousness of the breach and if the breach is serious, contact the CEO at the earliest possible opportunity.
- The CEO will use his discretion in determining whether the data breach or suspected data breach requires to be escalated to the Board of Directors. In making this determination, the CEO will consider the following questions:
 - Are multiple individuals affected by the breach or suspected breach?
 - May there be a real risk of serious harm to the affected individuals?
 - Does the breach indicate a systemic problem?
 - Could the breach attract stakeholder attention?
- The CEO will decide whether the breach is an “eligible data breach” that requires notification to the Office of the Australian Information Commissioner as per the Privacy Amendment (Notifiable Data Breaches) Act(2017)

How do we respond to a data breach?

- The Facility Manager, in conjunction with the CEO if necessary, will take urgent steps to contain the breach as far as possible and will conduct an initial investigation and collect information about the breach promptly, including the date, time, duration, and location of the breach; the type of information involved in the breach, how the breach was discovered and by whom, the cause and extent of the breach, a list of the affected individuals or possibly affected individuals; the risk of serious or other harms.
- The Facility Manager, in conjunction with the CEO if necessary, will determine whether to notify affected individuals and how to notify them.
- In conjunction with the CEO, the Facility Manager will consider whether security needs be updated, make appropriate changes to policies and procedures and revise staff training practices if necessary
