w. TassieCare.com
a. Suite 2 Level 1 35 Oldaker Street Devonport TAS 7310
p. (03)6421 6066
Registered NDIS Provider
405 007 0192
ABN 30 647 885 809

Management of Data Breach Policy and Procedure

Purpose

To meet legislative compliance requirements as a mandatory reporter of eligible data breaches to the Office of the Australian Information Commissioner (OAIC) and any individuals potentially affected by a data breach. Our organisation must inform relevant authorities of any breach, limit and reduce risks to the business, and ensure continuous improvement in the maintenance of data held by our organisation.

Scope

All Team Members must maintain the confidentiality of all data relating to participants and other staff members. This policy relates to all personal data regarding both participants and team members.

Definitions

Term	Definition
Data breach **(Eligible data breach)**	Unauthorised access to or unauthorised disclosure of personal information or personal information is lost in circumstances where unauthorised access to or unauthorized disclosure of the information is likely to occur.
Likely (likely to result in serious harm)	To be interpreted to mean more probable than not
Reasonable person	A reasonable person is a person who is adequately informed, based on information immediately available or following reasonable enquiries, or an assessment of the data breach. OAIC's guidance states that: *the reasonable person is not to be taken from the perspective of an individual whose personal information was part of the data breach or any other person. Generally, entities are not expected to make external enquiries about the circumstances of each individual whose information is involved in the breach.*

Likely to result in serious harm	An assessment as to whether an individual is likely to suffer 'serious harm' because of an eligible data breach depends on, among many other relevant matters: • the kind and sensitivity of the information subject to the breach • whether the information is protected and the likelihood of overcoming that protection • if a security technology or methodology is used concerning the information to make it unintelligible or meaningless to persons not authorised to obtain it - the information or knowledge required to circumvent the security technology or methodology • the persons, or the kinds of persons, who have obtained, or could obtain, the information • the nature of the harm that may result from the data breach.
Potential forms of serious harm	It could include physical, psychological, emotional, economic and financial harm and harm to reputation.
Remedial action	There are several exceptions to the notification obligation. An entity can take effective remedial action to prevent unauthorised access to or disclose information when it is lost or prevent any serious harm resulting from the data breach. An entity takes such remedial action; an eligible data breach will not be taken to have occurred. Therefore, an entity will not be required to notify affected individuals or the OAIC.
Suspicion of an eligible data breach	If TassieCare services merely suspects that an eligible data breach has occurred, but there are no reasonable grounds to conclude that the relevant circumstances amount to an eligible data breach; we must undertake a "reasonable

	and expeditious assessment" of whether there are reasonable grounds to believe that an eligible data breach has occurred.
Assessment time frame	Within 30 days after the day, it became aware that the grounds caused it to suspect an eligible data breach.
Personal Information	Personal information includes a broad range of information, or an opinion, that could identify an individual. Personal information will vary, depending on whether a person can be identified or identifiable in the circumstances. For example, personal information may include: • an individual's name, signature, address, phone number or date of birth • sensitive information • credit information • staff member record information • photographs • internet protocol (IP) addresses • voiceprint and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique) • location information from a mobile device (because it can reveal user activity patterns and habits).

Policy

TassieCare services views data breaches as having severe consequences, so the organisation must have robust systems and procedures in place to identify and respond effectively.

TassieCare services will delegate relevant team members with the knowledge and skills required to become a Data Breach Response Team member.

Team Members are required to inform the Director or their delegate of the potential, or suspected, data breach immediately. Within forty-eight (48) hours, the Director is to complete a Data Breach Process Form. Plus, ensure that, as a regulated entity, they notify the particular individuals and the Commissioner about

eligible data breaches as soon as practicable (no later than thirty (30) days after becoming aware of the breach or suspected breach).

If a staff member becomes aware that there are reasonable grounds to believe that there has been an eligible data breach, TassieCare services is required to promptly notify any individuals at risk of being affected by the data breach and the OAIC.

TassieCare services will undertake the following when an eligible data breach has occurred:

1. Prepare a statement that, at a minimum, contains:
    a. TassieCare services contact details:
        i) If relevant, the identity and contact details of any entity that jointly or simultaneously holds the same information, in respect of which the eligible data breach has occurred, e.g. due to outsourcing, joint venture or shared services arrangements. If information of this sort is included in the statement, the other entity will not need to report the eligible data breach separately.
    b. a description of the data breach
    c. the kinds of information concerned
    d. the steps it recommends individuals take to mitigate the harm that may arise from the breach (while the entity is expected to make reasonable efforts to identify and include recommendations, it is not expected to identify every recommendation possible following a breach).
2. Provide a copy of the prepared statement to the OAIC using the online Notifiable Data Breach Form.
3. Undertake such reasonable steps to notify affected or at-risk individuals of the contents of the statement. Individuals will be notified by email, telephone, or post, depending on the situation; if direct notification is not practicable, TassieCare services will publish the statement on its website and take reasonable steps to publicise its contents.

Procedure

Stage 1. Assess and determine the potential impact

- Once notified of the potential data breach, the Manager must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its possible severity.
- Advice on how to manage the data breach should be sought from appropriate managerial team member.

- Criteria for determining whether a privacy data breach has occurred:
    - Is personal information involved?
    - Is the personal information of a sensitive nature?
    - Has there been either - unauthorised access to personal information or unauthorised disclosure of personal information or loss of personal information in circumstances where access to the information is likely to occur?
- Criteria for determining the severity of the breach:
    - type and extent of personal information involved
    - the number of individuals that have been affected
    - if the information is protected by any security measures (password protection or encryption)
    - type of person/s who now have access
    - whether there is (or could be) a real risk of serious harm to the affected individuals
    - if there could be media or stakeholder attention due to the breach/suspected breach.
- Concerning the above, serious harm could include physical, physiological, emotional, economic/financial or harm to reputation and is defined in *Section 26WG* of the *National Data Breach Act.*

The Director and relevant team member will take a preliminary view as to whether the breach (or suspected breach) may constitute a Notifiable Data Breach. Accordingly, the Director will issue pre-emptive instructions as to whether the data breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team); this will depend on the nature and severity of the breach.

Stage 2. Select appropriate data breach management option

Option 1 - Data breach managed at a local level by managerial team member

1. The Director will ensure implementation of immediate corrective action if this has not already occurred. Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
2. A Data Breach Process Report is to be completed within 48 hours of receiving instructions. The report will contain a:
    - description of the breach or suspected breach
    - summary of action taken
    - summary of outcomes from the action taken

w. TassieCare.com
a. Suite 2 Level 1 35 Oldaker Street Devonport TAS 7310
p. (03)6421 6066
Registered NDIS Provider
405 007 0192
ABN 30 647 885 809

- outline of processes implemented to prevent a repeat situation
- recommendation that outlines why no further action is necessary.

3. The Director will sign-off, confirming that no further action is required.

Option 2 - Data breach managed by the Data Breach Response Team

1. When the Director instructs that the data breach be escalated to the Response Team, the Manager will convene the Response Team and notify any relevant managerial team members.
2. The Response Team will consist of:
   - Director
   - Human Resource nominee
   - Information Technology nominee
   - Marketing and external relations nominee
   - Other people nominated by the Director.

Primary role of the Data Breach Response Team

There is no single method of responding to a data breach. On a case by case basis, each incident must be dealt with by assessing the circumstances and associated risks to inform the appropriate course of action. The following steps may be undertaken by the Response Team, as appropriate:

1. Immediately contain the breach if this has not already occurred. Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.
2. Evaluate the risks associated with the breach, including collecting and documenting all available evidence regarding the information outlined above.
3. Call upon the expertise of, or consult with, relevant staff members in specific circumstances.
4. Engage independent cybersecurity or a forensic expert, as appropriate.
5. Assess whether serious harm is likely (with reference above and Section 26WG of the National Data Breach Act).
6. Make a recommendation to the Manager whether this breach constitutes an NDB for mandatory reporting to the OAIC and the practicality of notifying affected individuals.
7. Consider developing a communication or media strategy including the timing, content and method of any announcements to participants, staff members or the media.
8. The Response Team must undertake its assessment within 48 hours of being convened.

Secondary role of the Data Breach Response Team

Once the data breach has been dealt with appropriately, the Response Team should turn its attention to the following steps:

1. Identify lessons learnt and remedial action that can be taken to reduce the likelihood of a recurrence; this may involve a review of policies, processes, and refresher training.
2. Prepare a report for submission to senior management.
3. Consider conducting an audit to ensure that the necessary outcomes are affected and effective.

Notify the Office of the Australian Information Commissioner

- Taking into consideration the Response Team's recommendation, the Director will determine whether there are reasonable grounds to suspect that a Notifiable Data Breach has occurred.
- If there are reasonable grounds, the Director must prepare a prescribed statement and provide a copy to the OAIC as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach).

Related documents

- Team Member Training Record
- Team Member Training Plan
- Data Breach Process Form

References

- NDIS Practice Standards and Quality Indicators 2021
- Privacy Act 1988 (Commonwealth)
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Commonwealth)