



Data Breach Response Plan

The Taillem Bend Community Centre (TBCC) is committed to protecting the privacy and personal information that it holds about individuals. TBCC will act appropriately and in a timely manner in the event of a data breach, to contain the possible resulting harm and notify individuals affected as required.

Definitions

Data Breach: When personal information held by an organisation is disclosed accidentally, lost, or accessed without permission. This can be as a result of human error, or through malicious action by an employee or an external party.

Examples include where a secure IT system containing personal information has been hacked, a storage device being lost by an employee, or an employee accidentally releasing personal information to the wrong person.

Personal information: 'Information about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

Personal information includes a person's health information, tax file number, and information about racial or ethnic origin, sexual orientation or criminal record.

Data breach response team

The response team is responsible for assessing, investigating, notifying and reviewing data breaches. Roles and responsibilities are to be established and communicated prior to a data breach occurring. Depending on the size of the organisation, there may be the following roles in a response team:

Procedure

Identify

When staff have reason to believe there has been a data breach, they should inform TBCC CEO immediately.

Chief Executive Officer (CEO) is responsible for leading the response and reporting to senior management/governing body, and reporting lines in consultation with Murray Computers.

At this time, details such as when and how the breach was discovered, and by whom, should be recorded. This will be recorded in a Data Breach Incident Reporting form.

The following security measures are in place supported by Murray Computers. TBCC Dropbox Accounts are protected via Multi Factor authentication. Devices are protected via password. Dropbox Compliance standards and regulations. <https://www.dropbox.com/business/trust/compliance/certifications-compliance>

Patch management and Managed Endpoint Security (antivirus) provided by Murray Computers to ensure computers are scanned, updated and protected.

Multifactor authentication turned on for key Microsoft 365 accounts.
Azure active directory used for PC logins.
WiFi system isolates public internet traffic from business network.

Contain

As soon as a breach or suspected breach has been identified, any steps to contain or limit the potential harm should be taken. This may include shutting down a system that has been breached, or recovering any records.

The TBCC CEO or nominated staff member will complete a preliminary assessment of the breach in consultation with Murray Computers and take any immediate action to contain the breach if possible.

Assess

If the preliminary assessment finds that further investigation and assessment is necessary to understand the nature and extent of the breach, it will be escalated to the data breach response team. The team will work together to gather information, assess risks and the likelihood of serious harm from the breach, and therefore whether it is an 'eligible' (notifiable) breach.

To evaluate whether a known data breach is notifiable, consider the following three questions:

- **Has there been unauthorised access, unauthorised disclosure, accidental loss, or theft of personal information that the organisation holds?**

For example, the organisation's database is hacked, a portable storage device containing personal information is lost, or the organisation accidentally releases personal information to the wrong person.

- **Is it *likely* that this may result in serious harm to individual/s whose data has been breached?**

This can include but is not limited to psychological, financial, emotional, physical or reputational harm. To be able to accurately assess the likelihood and seriousness of harm, it requires looking at the context of the data and how it may have been breached.

For information about the factors to consider when deciding whether harm is likely and/or serious, refer to section 26WG of the [Privacy Amendment \(Notifiable Data Breaches\) Act 2017](#)

- **Does the likelihood of serious harm remain despite taking available remedial action?**

The obligation to notify the OAIC can be avoided if the organisation takes remedial action in a timely manner to prevent the risk of harm occurring, either by making the harm unlikely to occur, or non-serious.

If the answer to the above three questions is yes, then the breach classifies as an eligible data breach and organisations are required to notify the OAIC and any affected individuals.

If there are reasonable grounds to *suspect* that there has been a data breach, the data response team should conduct an assessment of the suspected breach. The assessment of a suspected breach must take place within 30 days of it occurring, and should seek to find out the likelihood of serious harm occurring as a result of the suspected breach. If it is assessed to be likely, this has the same notification obligations as a known data breach under the NDB Scheme.

The TBCC CEO is responsible for four key steps following a data breach:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

TBCC will take remedial action, where possible, to limit the impact of the breach on affected individuals.

In summary TBCC will:

- take each data breach or suspected data breach seriously and move immediately to contain, assess and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed
- undertake steps 1 (Contain), 2 (Assess), and 3 (Notify) either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs
- determine how to respond on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, an entity may take additional steps that are specific to the nature of the breach

Take remedial action

Remedial action can be taken at any point throughout the data breach response process – the sooner the better. However, it may be that the full extent and nature of the breach, and therefore the actions that could be taken, are not known until after assessing and investigating the breach.

Examples of remedial action include remotely deleting sensitive information from a laptop which has been lost, or emailing affected individuals with advice to change their password details for an online account for which login information may have been hacked.

The data breach response team should document the process of any remedial action, making sure to document rationale and reasoning as to why a certain conclusion has been made.

If, after the remedial action has been taken, the risk of harm is reduced so that it is unlikely to occur, or non-serious, then there is no requirement to notify.

Even if there is no requirement, however, the data response team should consider whether to contact affected individuals with advice for further protecting their information as a customer service measure.

Notify

Once a breach has been assessed as eligible, relevant individuals and bodies should be notified as soon as practicable. Notification must include the following information as a minimum:

- The organisation's name and contact details
- Description of the data breach
- Type of information involved in the breach
- Advice and recommendations for individuals to take in response

1. The OAIC

TBCC CEO is responsible for notifying and liaising with the OAIC for data breaches which have been assessed as eligible for the purposes of the Notifiable Data Breaches Scheme, using the OAIC's Notifiable Data Breach form.

2. Notification of individuals who are at likely risk of serious harm due to the data breach

The way notification occurs will depend on the context and nature of the breach, and the relationship of the individuals affected to the organisation. It should occur as soon as practicable after completing the notification statement for the OAIC.

TBCC CEO is responsible for notifying affected individuals, including when they are to be notified, and the method of communication – whether they will be individually notified or through a public notification.

Notification to affected individuals may contain an explanation of what happened to their personal information, an apology, description of what measures have been put in place as a result of the breach, and advice on what they can do to further protect their information.

Record and review

Data breach log


A data breach log will record all instances of data breaches or suspected breaches, as well as document assessments of the breach and any changes made as a result of a breach.

All staff should be made aware of the log, and TBCC CEO will be responsible for ensuring that all breaches or suspected breaches are recorded accurately in the log. The Data Breach Log is located **Confidential – TBCC Risk Hazard Incident Register Data Breach log** found in C:\Users\CEO-TBCC\Dropbox (Tailem Bend Community)\BOM\Policies Procedures reviewed 2020-2022.

Review

Whether or not the breach or suspected breach was notifiable, a review should be conducted into processes relating to the breach to strengthen protections in the future. Depending on the type and seriousness of the breach, this may include:

- A full investigation into how the breach occurred
- Implement measures to ensure it does not reoccur, documented in a prevention plan
- Reviews of security, cybersecurity and ICT policies and procedures
- Audit of implementation of relevant policies and procedures
- Additional staff training about privacy and data breach responses

Date first formulated	Feb 2022	
Dates approved by Board	V1	Feb 2022
Next Review Date	Feb 2024	
Related Documents	Office of the Australian Information Commissioner Australian Cyber Security Essential Eight Protective Security Policy Framework Australian Government Information Security Manual Privacy (Tax File Number) Rule 2015 AS/NZS 4360:2004 Australian, New Zealand Risk Management Standard Aust. Taxation Office – Enterprise Risk Management Framework Australian Institute of Company Directors Board of Management Kit - Volunteer Pack Volunteering Australia Business Continuity Policy Delegation of Authority Feedback and Complaints Policy Finance Policy Human Resources Management Policy Privacy and Confidentiality Policy Risk Assessment Matrix Risk Management Procedures Work Health and Safety Policy Viral Outbreak JASI Global BNG DHS	
Legislation	Privacy Amendment Act 2017 Privacy Act 1998 Public Governance, Performance and Accountability Act 2013 My Health Record Act 2012 Healthcare Identifiers Act 2010 National Cancer Screening Register Act 2016 Work Health and Safety Act Work Health and Safety Regulations 2012 Codes of Practice Safework SA Return to Work SA Aged Care Quality and Safety Commission Act 2018 Aged Care Act 1997 Competition and Consumer Act 2010 Associations Incorporation Act 2009	
Signed on behalf of TBCC Board of Management by: Name: Jack Hunt Position held: Chairperson <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 10px;">  <div style="text-align: right;">Signature: 2 February 2022</div> </div>		