Blackall-Tambo Regional Council

Data Breach Response Plan

Policy Number: P29	Effective Date: 21.04.2021
Version Number: One	Review Date: 21.04.2025
Policy Compiled by: Information Technology Officer	
Policy Approved by: Chief Executive Officer	

DATA BREACH RESPONSE PLAN

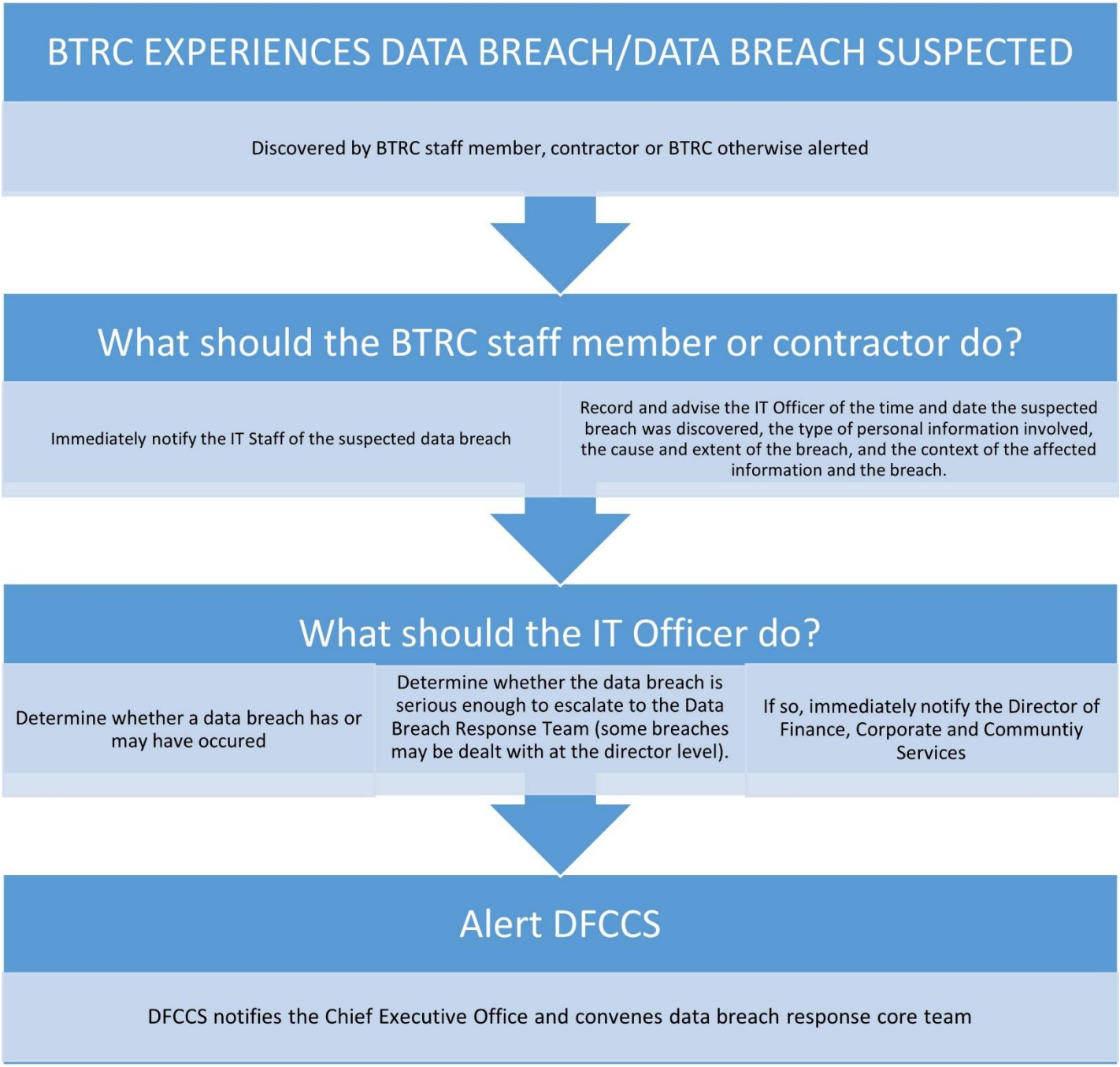
This data breach response plan (response plan) sets out procedures and clear lines of authority for BTRC staff in the event that the BTRC experiences a data breach (or suspects that a data breach has occurred).

A data breach covered by the Information Privacy Act 2009 (QLD) (IP Act) occurs when personal information is lost or subjected to unauthorised access or disclosure. For good privacy practice purposes, this response plan also covers any instances of unauthorised use, modification or interference with personal information held by the BTRC. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information, and give rise to a range of actual or potential harms to individuals and entities.

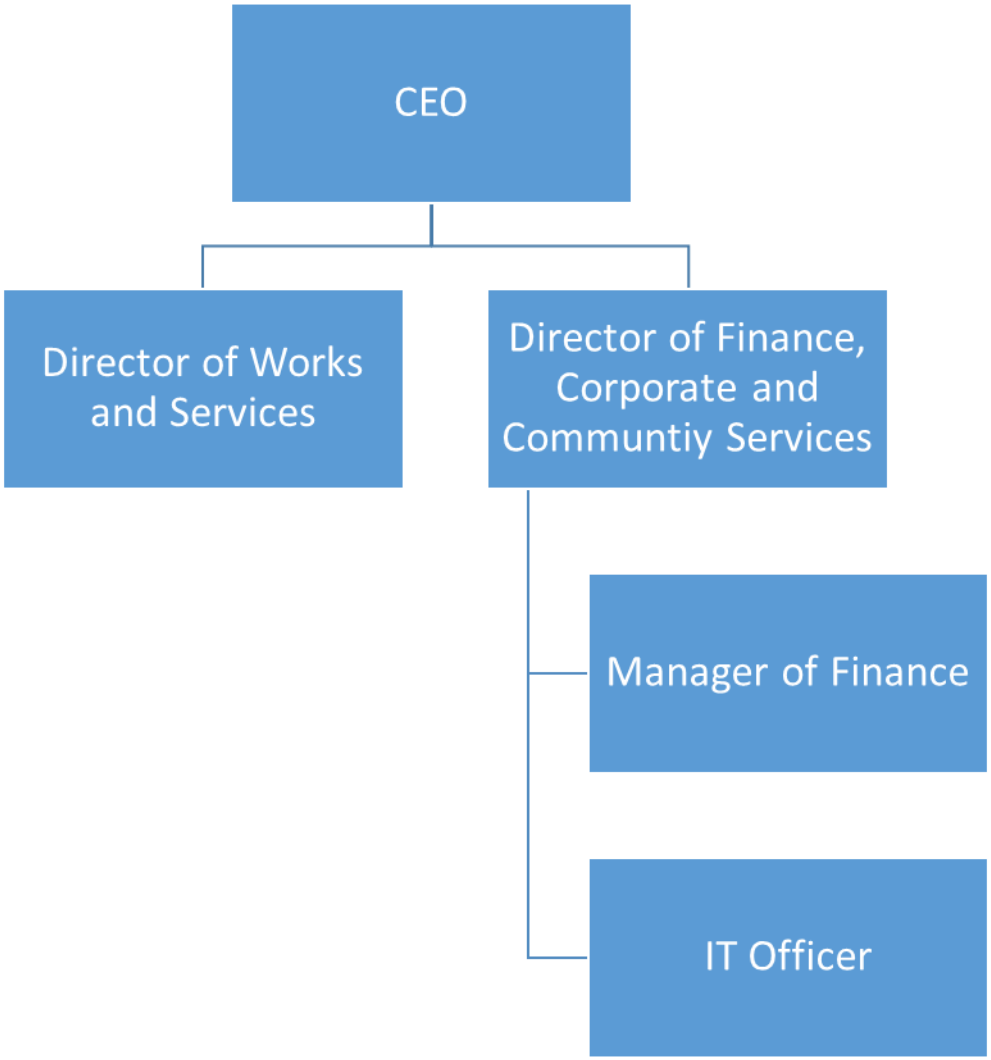
This response plan is intended to enable the BTRC to contain, assess and respond to data breaches quickly, to help mitigate potential harm to affected individuals and to comply with the IP Act scheme. Our actions in the first 24 hours after discovering a data breach are crucial to the success of our response.

The plan sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist the BTRC to respond to a data breach.

DATA BREACH RESPONSE PROCESS



DATA BREACH RESPONSE TEAM – MEMBERS



WHEN SHOULD A DATA BREACH BE ESCALATED TO THE DATA BREACH RESPONSE TEAM

Some data breaches may be comparatively minor, and able to be dealt with easily without action from the Data Breach Response Team (response team).

For example, a council employee may, as a result of human error, send an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be successfully recalled (only relates to internal emails), or if the council employee can contact the

recipient and obtain an assurance that the recipient has deleted the email, it may be that there is no value in escalating the issue to the response team.

IT Officer should use their discretion in determining whether a data breach or suspected data breach requires escalation to the response team. In making that determination, IT Officer should consider the following questions,

- Are multiple individuals affected by the breach or suspected breach?
- Is there (or may there be) a real risk of serious harm to any of the affected individual(s)?
- Does the breach or suspected breach indicate a systemic problem in BTRC processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then the Reporting Employee should attempt immediate verbal contact with the IT Officer, or if this is not possible, another primary response team member.

The checklist below sets out the steps that the response team will take in the event of a serious data breach.

If it is decided not to escalate a minor data breach or suspected data breach to the response team for further action, then an email should be sent to the Chief Executive Officer that contains the following information:

  - Description of the breach or suspected breach
  - Action taken to address the breach or suspected breach
  - The outcome of the action, and
  - The reasons for their view that no further action is required
- Save a copy of that email in the following MAGIQ Documents Folder:
  - Data Breach Response – reports and investigation of data breaches

DATA BREACH RESPONSE PROCESS

There is no single method of responding to a data breach. Data breaches must be dealt with on a case-by case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action. Depending on the nature of the breach, the response team may need to include additional staff or external experts, for example an IT specialist/data forensics expert.

There are four key steps to consider when responding to a breach or suspected breach.

STEP 1: Contain the breach

STEP 2: Assess the risks associated with the breach

STEP 3: Consider breach notification

STEP 4: Review the incident and take action to prevent future breaches

The response team should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. At all times, the response team should consider whether remedial action can be taken to reduce any potential harm to individuals.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

Following serious data breaches, the response team should conduct a post-breach review to assess the Council's response to the breach and the effectiveness of this plan and report the results of the review to the CEO. The post-breach review report should identify any weaknesses in this response plan and include recommendations for revisions or staff training as needed.

The response team should also consider the following documents where applicable:

BTRC Disaster Recovery & Business Continuity Plan

BTRC Incident Response Plan

TESTING THIS PLAN

Members of the response team should test plan with a hypothetical data breach annually to ensure that it is effective. As with the post-breach review following an actual data breach, the response team must report to the CEO on the outcome of the test and make any recommendations for improving the plan.

RECORDS MANAGEMENT

Documents created by the response team, including post-breach and testing reviews, should be saved in MAGIQ Documents Folder:

- Data Breach Response – reports and investigation of data breaches

BLACKALL-TAMBO REGIONAL COUNCIL'S DATA BREACH RESPONSE CHECKLIST

Step 1: Contain the breach

- Notify the Director of Finance, Corporate and Community Services, who may convene the data response team.
- Immediately contain the breach:
  - IT to implement the Incident Response Plan if necessary.
  - Contact Security Operations Centre (SOC) – PinnacleIT
- Consider whether team needs other expertise
- Inform the CEO, and Queensland Government Chief Information Office (QGCIO), as soon as possible; provide ongoing updates on key developments.
- Ensure evidence is preserved that may be valuable in determining the cause of the breach or allowing the Council to take appropriate corrective action.
- Consider a communications or media strategy to manage public expectations.

Step 2: Assess the risks for individual associated with the breach

- Conduct initial investigation, and collect information about the breach promptly, including:
  - the date, time, duration, and location of the breach
  - the type of personal 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 possible affected individuals
  - the risk of serious harm to affected individuals
  - the risk of other harms.
- Determine whether the context of the information is important.
- Establish the cause and extent of the breach.
- Assess priorities and risks based on what is known.

- Keep appropriate records of the suspected breach and actions of the response team, including the steps taken to rectify the situation and the decisions made.

Step 3: Consider breach notification

- Determine who needs to be made aware of the breach (internally, and potentially externally) at this preliminary stage.
- Determine whether and how to notify affected individuals. Does the breach trigger the requirements of the IP Act – is the breach likely to result in serious harm to any of the individuals to whom the information relates and the Council has not been able to prevent the likely risk of serious harm, the affected individuals should be notified. Prompt notification to individuals in these cases can help avoid or lessen the damage by enabling the individual to take steps to protect themselves.
- Consider whether others should be notified, including Office of the Information Commissioner QLD (OIC), Queensland Government Chief Information Office (QGCIO), law enforcement or other agencies or organisations affected by the breach or can assist in containing the breach or assisting individuals affected by the breach.

Step 4: Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach.
- Implement a strategy to identify and address any weaknesses in data handling that contributed to the breach.
- Conduct a post-breach review and report to the CEO on outcomes and recommendations:
    - Update security (physical and technical) and response plan if necessary.
    - Make appropriate changes to policies and procedures if necessary.
    - Revise staff training practices if necessary.
    - Consider the option of an audit to ensure necessary outcomes are accomplished.

POLICY REVIEW

This policy will be reviewed when any of the following occur:

a) As required by legislation

b) Other circumstances as determined by the Chief Executive Officer

Notwithstanding the above, this policy is to be reviewed at intervals of no more than four (4) years.

VERSION CONTROL

Version 1	New Document 21-04-2021

RECORDS

When completed and approved, the original signed hard copy of the policy is filed in the Master File.

Electronic copies are saved in the appropriately labelled folder in Magiq.