Office of the Information Commissioner
Queensland

Data breach response plan

The final report of the Coaldrake review (https://www.coaldrakereview.qld.gov.au) recommended *'a mandatory data breach notification (MDBN) scheme be established in Queensland, forthwith.'*

This echoes the recommendation from the CCC's Operation Impala in 2020 that '*a mandatory data breach notification scheme be implemented in Queensland and the OIC be responsible for developing the scheme, and receiving and managing the notifications*.'

On 28 June 2022, the Premier indicated that the Queensland Government will accept all the recommendations from the Coaldrake review and will implement them.

The Office of the Information Commissioner (OIC) is conducting this survey under section 135 of the *Information Privacy Act 2009* (Qld). It asks a series of questions about **your agency's data breach response plan**. Most questions are binary yes/no questions.

This survey will establish baseline data on government agencies' level of preparedness to respond to a data breach. Government agencies include Queensland Government departments, statutory authorities, local governments, hospital and health services, government-owned corporations and universities and TAFE.

We will collate the results of this survey and present them in an aggregated format in a report to Parliament.

* Required

Office of the Information Commissioner
Queensland

Instructions and contact

The questions in this survey are based on the guide "*Data breach preparation and response*" published by the Office of the Australian Information Commissioner (OAIC) available www.oaic.gov.au
Please refer to the guide (parts 2 and 3) for further information on how to prepare a data breach response plan.

Before you start answering the survey, see all the questions here (link to a page on our website?). This will help you identify the information you need to complete the survey.

THERE IS NO 'SAVE and RESUME' FUNCTION - the survey needs to be completed in one go

Instructions

- The survey takes about 15 minutes to complete
- Complete only 1 survey for each government agency
- Complete the survey by 6pm **Friday 12 May 2023**
- Do **NOT** provide personal information in the survey

If you have any question about this survey, please email us at audit@oic.qld.gov.au

Agency details

1

Name of the agency *

2

Type of agency *

- Queensland Government Department
- Local Government
- Hospital and Health Service
- Statutory authority
- University and TAFE
- Government Owned Corporation
- Other

Contact details

3

Name of the person completing this survey on behalf of the agency *

4

Position *

5

Business email address *

Data breach response plan

6

Does the agency have a **documented** data breach response plan? *

- Yes
- No

7

When was the plan approved? *

8

Has the agency reviewed the plan since it was approved? *

- Yes
- No

9

Date of the most recent review *

10

Date of the next scheduled review

11

Has the agency tested the plan? *

- Yes
- No

12

Date of the most recent test *

13

What did the test involve? *

14

Date of the next scheduled test

15

Has the agency made its staff aware of the data breach response plan? *

- ◯ Yes
- ◯ No

16

How has the agency made its staff aware of the plan? *

17

Has the agency published its data breach response plan, or a version of it, on its website? *

- ◯ Yes
- ◯ No

Definitions

18

Does the plan clearly explain what is a data breach?
(*A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure, or is lost* - page 7 Data breach preparation and response, OAIC) *

- ◯ Yes
- ◯ No

19

Does the plan give examples of data breaches? *

- ◯ Yes
- ◯ No

20

How many examples of data breaches are in the plan? *

The value must be a number

21

Does the plan outline possible consequences of a data breach? *

- Yes
- No

22

Does the plan identify risk of serious harm to affected individuals as a possible consequence of a data breach? *

- Yes
- No

Roles and responsibilities

23

Does the plan outline roles and responsibilities in case of a data breach? *

- ◯ Yes
- ◯ No

24

Does the plan explicitly state who staff should inform if they suspect a data breach? *

- ◯ Yes
- ◯ No

25

Does the plan outline the circumstances in which a line manager can handle a data breach? *

- ◯ Yes
- ◯ No

26

Has the agency established a data breach response team? *

- ◯ Yes
- ◯ No

27

Does the plan explain when a data breach must be escalated to the response team? *

- ◯ Yes
- ◯ No

28

Does the plan identify who is responsible for deciding whether to escalate to the response team? *

- ◯ Yes
- ◯ No

29

Does the plan specify the factors to consider when deciding whether to escalate to the response team? *

- ◯ Yes
- ◯ No

30

According to the plan, what factors should be considered when deciding to escalate to the response team? *

- ☐ the number of people affected by the breach or suspected breach
- ☐ the risk of serious harm to affected individuals now or in the future
- ☐ whether the data breach or suspected data breach may indicate a systemic problem in the agency
- ☐ the value of the data to the agency
- ☐ the reputational risk to the agency
- ☐ Other

Response team

31

Does the plan clearly identify each member of the response team? *

- Yes
- No

32

Does the plan describe the roles and responsibilities of each member of the response team? *

- Yes
- No

33

Does the response team include a senior member of staff with overall accountability and expertise about privacy? *

- Yes
- No

34

Does the plan describe the authority or delegations of each member of the response team? *

- ◯ Yes
- ◯ No

35

Does the plan include **current** contact details for each member of the response team? *

- ◯ Yes
- ◯ No

36

Does the plan outline the circumstances (for instance the nature of the breach) in which the agency may need to include external experts in its response team, for example legal advice, data forensics, or media management? *

- ◯ Yes
- ◯ No

Strategy for containing, assessing and managing data breaches

37

Does the plan include the actions the agency will take in the event of a data breach or a suspected data breach? *

- ◯ Yes
- ◯ No

38

Does the plan include potential strategies for containing and remediating data breaches? *

- ◯ Yes
- ◯ No

39

Does the plan explain how the containment and remediation strategies will apply to various types of data breaches and varying risk profiles? *

- ◯ Yes
- ◯ No

40

Does the plan include legislative or contractual requirements applicable to the agency (such as the requirements of the NDB scheme or an insurance contract)? *

- Yes
- No

Communication strategy

41

Does the plan include a clear communication strategy? *

- ◯ Yes
- ◯ No

42

Does the communication strategy allow for the prompt notification of ? *

- ◯ Affected individuals
- ◯ External stakeholders (for example law enforcement and cyber security agencies at state and federal levels, regulators such as OIC and OAIC, insurance, etc)
- ◯ Agency executives
- ◯ Other

43

Does the plan specify who is responsible for implementing the communication strategy? *

- ◯ Yes
- ◯ No

44

Does the plan explain how to determine whether to notify affected individuals? *

- ◯ Yes
- ◯ No

45

According to the plan, what factors should be considered when determining whether to notify affected individuals? *

- ☐ the type or types of personal information involved in the data breach
- ☐ the circumstances of the data breach, including its cause and extent
- ☐ the nature of the harm to affected individuals, and if this harm can be removed through remedial action.
- ☐ Other

46

Does the plan identify who is responsible for determining whether to notify affected individuals? *

- Yes
- No

47

Does the plan outline **how** affected individuals will be contacted and managed? *

- Yes
- No

48

Does the plan outline **when** affected individuals will be contacted? *

- Yes
- No

49

Does the plan include criteria for determining which external stakeholders should be contacted (for example, law enforcement and cyber security agencies, regulators such as the OAIC, and the media)? *

- Yes
- No

50

Is OIC mentioned in the list of external stakeholders to be contacted under the current voluntary data breach notification scheme? *

- Yes
- No

51

Does the plan identify who is responsible for liaising with external stakeholders? *

- Yes
- No

52

Does the plan explain how to determine whether to notify the agency's executive? *

- Yes
- No

53

Does the plan identify who is responsible for determining whether to notify the agency's executive? *

- Yes
- No

Documentation and review

54

Does the plan outline the agency's policy about recording and documenting data breaches? *

- ◯ Yes
- ◯ No

55

Does the policy include recording data breaches that are not escalated to the response team? *

- ◯ Yes
- ◯ No

56

Does the plan or the policy identify who is responsible for documenting and recording data breaches? *

- ◯ Yes
- ◯ No

57

Does the plan outline the agency's policy about assessing a data breach? *

- ◯ Yes
- ◯ No

58

According to the plan or the policy, what factors should be considered when assessing a data breach? *

- ☐ the type(s) of personal information involved in the breach
- ☐ the individuals whose personal information is involved in the data breach (for example individuals known to be vulnerable)
- ☐ the cause of the breach
- ☐ the extent of the breach - systems, volume of information
- ☐ the extent of the breach - potential number of affected individuals
- ☐ the nature of the harm to affected individuals
- ☐ the likelihood of harm to affected individuals
- ☐ the effectiveness of possible remediation actions to remove the harm
- ☐ the length of time the information has been accessible
- ☐ Other

59

Does the plan outline the agency's policy about documenting and recording the assessment of a data breach? *

- Yes
- No

60

Does the plan or the policy identify who is responsible for documenting and recording the assessment? *

- Yes
- No

61

Does the plan outline the agency's policy about reviewing the response to a data breach? *

- Yes
- No

62

Does the plan or the policy identify who is responsible for reviewing the agency's response to a data breach? *

- Yes
- No

63

Does the review include amending the agency's data breach response plan where applicable, as a result of reviewing the response to a breach? *

- Yes
- No

Resources and guidance

If your agency does not have a data breach response plan, we recommend developing and implementing such plan **as a priority**.

A data breach response plan can help your agency meets its legislative and regulatory obligations, limit the consequences of a data breach and preserve public trust.

The following resources may help:

- https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/privacy-breach-management-and-notification
- https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/responding-to-a-privacy-breach
- https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response
- https://www.forgov.qld.gov.au/information-and-communication-technology/cyber-security