Crime and Corruption Commission
QUEENSLAND

Data Breach Policy

July 2025

Objective

Chapter 3A of the Information Privacy Act 2009 (Qld) (**IP Act**) creates Queensland's Mandatory Notification of Data Breach (**MNDB**) scheme.

The MNDB scheme requires the Crime and Corruption Commission (**CCC**) to notify the Queensland Information Commissioner of the Office of the Information Commission (**OIC**) and, in certain cases, affected individuals of eligible data breaches.

Under the MNDB scheme, the CCC is required to:

- publish a data breach policy (DBP) which outlines the CCC's overall strategy for managing data breaches; and
- maintain an internal register of eligible data breaches.

This DBP outlines the approach of the CCC to comply with the MNDB scheme, including the roles and responsibilities for reporting data breaches and strategies for containing, assessing and managing eligible data breaches.

Relevant legislation

Information Privacy Act 2009

Crime and Corruption Act 2001

Public Records Act 2023

Right to Information Act 2009

Definitions

Affected individual	An ***affected individual*** is an individual specified in subsection 47(1)(a)(ii) or 47(1)(b)(ii) of the IP Act, that is, an individual to whom serious harm is likely to result and to whom the personal information involved in an eligible data breach relates.
Approved form	The ***approved form*** is the form approved by the Information Commission under section 200 of the IP Act.
Assessment	The ***assessment*** under section 48(2)(b) of the IP Act, being an assessment by the CCC as to whether the data breach is, or there are reasonable grounds to believe the data breach is, an eligible data breach of the CCC.

Assessor	The ***assessor*** is the person appointed by the CEO to investigate the data breach in accordance with the MNDB scheme.
Data breach	A ***data breach*** of an agency is defined in Schedule 5 of the IP Act and means either of the following in relation to information held by the CCC – (a) unauthorised access to, or unauthorised disclosure of, the information; or (b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.
Eligible data breach	An ***eligible data breach*** is defined in section 47 of the IP Act and means a data breach of the CCC that occurs in relation to personal information held by the CCC if – (a) both of the following apply – (i) the data breach involves unauthorised access to, or unauthorised disclosure of, the personal information; and (ii) the access or disclosure is likely to result in serious harm to an individual (an ***affected individual***) to whom the personal information relates, having regard to the matters set out in section 47(2) IP Act; or (b) the data breach involves the personal information being lost in circumstances where – (i) unauthorised access to, or unauthorised disclosure of, the personal information is likely to occur; and if the unauthorised access to or unauthorised disclosure of the personal information were to occur, it would be likely to result in serious harm to an individual (also an ***affected individual***) to whom the personal information relates, having regard to the matters stated in section 47(2) IP Act.
Held or **holds**	***Held*** or ***holds*** in relation to personal information is defined by section 13 of the IP Act. Personal information is ***held*** by the CCC, or the CCC ***holds*** personal information, if the personal information is contained in a document in the possession, or under the control, of the CCC.
Personal information	***Personal information*** is defined by section 12 of the IP Act and means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion – (a) whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.
Relevant matters (in assessing serious harm)	The ***relevant matters*** in assessing if the data breach is likely to result in serious harm in section 47(2) of the IP Act are: (a) the kind of personal information accessed, disclosed or lost; and

	(b) the sensitivity of the personal information; and (c) whether the personal information is protected by 1 or more security measures; and (d) if the personal information is protected by 1 or more security measures – the likelihood that any of those security measures could be overcome; and (e) the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and (f) the nature of the harm likely to result from the data breach; and (g) any other relevant matter.
Serious harm	***Serious harm*** to an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information is defined in Schedule 5 of the IP Act and includes, for example – (a) serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure; or serious harm to the individual's reputation because of the access or disclosure.

Application

This DBP applies to all staff and contractors of the CCC, including seconded officers, contractors and consultants who have access to CCC systems, networks and/or information.

Policy statement

The purpose of this DBP is to provide publicly accessible information about how the CCC will respond to data breaches of CCC information in accordance with the IP Act. The CCC acknowledges that not all data breaches will be eligible data breaches under the MNDB scheme. Notwithstanding, the CCC takes all data breaches seriously. This DBP details:

- what constitutes an eligible data breach under the IP Act.
- the roles and responsibilities for reporting, reviewing and managing eligible data breaches.
- the steps involved in responding to an eligible data breach, including the communication strategy as well as review processes to prevent future data breaches.

Human rights

The CCC recognises that data breaches, and actions taken to respond to data breaches, may engage individual's human rights including the right to privacy and the right to freedom of expression as set out in the *Human Rights Act 2019* (**HR Act**). When taking actions and making decisions pursuant to this DBP, decision-makers will give proper consideration to relevant human rights in accordance with the HR Act.

Roles and responsibilities

Everyone to whom this DBP applies is responsible for:

- ensuring they have read this policy and the *Mandatory Notification of Data Breach Procedure* (internal CCC document) and that they understand what is expected of them;
- complying with the IP Act and the CC Act including by protecting personal information held by the CCC from unauthorised access, disclosure or loss; and
- immediately reporting a data breach, suspected data breach or possible data breach to the CEO (and their manager, as appropriate).

The **CEO**[1] is responsible for:

- receiving notifications of data breaches;
- assessing whether data breaches are eligible data breaches under the MNDB scheme;
- where required, notifying the Information Commissioner and affected persons about the eligible data breach;
- reviewing eligible data breaches in order to identify remedial actions to prevent the further incidence of data breaches involving CCC information;
- maintaining the internal register of eligible data breaches of the CCC;[2] and
- reviewing and updating this DBP and ensuring its continued publication on the CCC's website.[3]

The **Business Continuity Committee** (the Committee) is a multi-disciplinary group of senior commission officers who are responsible for the Business Continuity Management System of the CCC. The Chair of the Committee is the CEO. The Chair has responsibility for deciding when to engage the Committee and activate the Business Continuity Plan. The Chair will decide whether, in responding to and dealing with a data breach, it is necessary to engage the Committee.

How the CCC has prepared for a data breach

The CCC has established a range of systems and processes for preventing and managing data breaches, including the following:

- initial and ongoing training for commission officers in identifying, managing and reporting data breaches, and the introduction of an online learning module about the MNDB scheme to be completed by commission officers annually.
- other training and awareness activities around the protection of personal information.
- implementation of an internal procedure for identifying and reporting data breaches to the CCC CEO.
- review of service provider contracts and inclusion of data breach management and notification obligations in service provider contracts and agreements as necessary.
- creation of a schedule for reviewing, testing and updating this DBP annually.

[1] By way of sub-delegated statutory authority under section 269(5) of the *Crime and Corruption Act 2001*.

[2] As required by IP Act s 72.

[3] As required by IP Act s 73.

Eligible data breaches

An eligible data breach is defined in section 47 of the IP Act (per Definitions above).

A data breach can be caused in various ways from both deliberate and accidental actions, including as a result of malicious action, systems failure or human error.

Examples of data breaches include:

- when a letter or email is sent to the wrong recipient.
- when systems access is incorrectly granted to someone without appropriate authorisation.
- when a physical asset such as a paper record, laptop, USB or mobile telephone containing personal information is lost, misplaced or stolen.
- cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to, or theft of, personal information.
- employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.

The data breach will become an eligible data breach when the MNDB scheme applies to the information and the harm from the data breach has resulted, or may result, in a real and substantial detrimental effect to the individual (serious harm).

Serious harm (per Definitions above) to an individual includes physical, economic, financial or material harm, emotional or psychological harm, reputational harm, and other forms of serious harm that a reasonable person would identify as a possible outcome of the data breach.

Reporting and responding to a data breach

The CEO must be informed of all data breaches to ensure the application of this DBP, including making notifications to the Information Commissioner for eligible data breaches and, where relevant, affected individuals.

There are five key steps required in responding to a data breach:

1. Identification and report
2. Contain and mitigate
3. Assess and mitigate
4. Notify
5. Review

Each step is set out in further detail below. The first four steps may be carried out concurrently, depending on the circumstances and nature of the data breach. Step five involves recommendations for longer-term solutions and prevention strategies and occurs as a post incident review.

Step 1: Initial identification and reporting of data breaches

Commission officers are to notify the CEO as soon as possible and, in any event, within one business day of becoming aware that a data breach or suspected data breach has occurred and provide information about the type of data breach. The CCC's MNDB Procedure sets out reporting processes commission officers should follow.

A contractor or third-party provider with access to CCC information is to notify the senior CCC manager to whom they report of a data breach in the same timeframe. The manager will notify the CEO of the data breach immediately.

All data breaches (per Definitions above) must be reported to the CEO. It is the CEO's responsibility to assess whether the data breach is an eligible data breach (per Definitions above).

Members of the public may report any data breaches to the CCC in writing using the contact options available on the CCC website (www.ccc.qld.gov.au).

Step 2: Containing and mitigating a data breach

The CCC will prioritise containing the breach.

All reasonable steps must immediately be taken to contain the data breach and mitigate the harm caused by the data breach as soon as the CCC knows or reasonably suspects that a data breach is an eligible data breach. The CEO will determine the containment and mitigation measures that need to be taken having regard to the scale, seriousness and significance of the data breach. For example, the CCC might:

- make efforts to recover the personal information.
- make efforts to contact the person who has received the information incorrectly.
- secure, restrict access to and/or shut down the breached systems.
- suspend the activity that led to the data breach.
- revoke or change access codes or passwords.

If a third party is in possession of the data and declines to return it, it may be necessary for the CCC to seek legal or other advice on what action can be taken to recover the data. When recovering data, the CCC will take steps to ascertain whether the data has been shared or disseminated to a third party, and if it has, to ensure that all copies are recovered. This can include receiving written confirmation from a third party that the copy of the data that they received in error has been permanently deleted.

The CCC will ensure that while containing a data breach, information is not destroyed that may be required as part of an internal or external investigation into the breach.

Step 3: Assessing the data breach

To determine what steps are needed, the CCC will undertake an assessment of the type of information involved in the breach, whether the breach is an eligible data breach under the MNDB scheme, and the risks and potential for serious harm associated with the breach.

While all data breaches will turn on their own set of circumstances and varying on a case-by-case basis having regard to the seriousness, scale and type of data breach, generally, an assessment will involve the following steps:

- gathering information about and evidence of the data breach;
- analysing gathered information having regard to the factors which influence the likelihood of serious harm; and

- making a decision as to whether the gathered information and analysis supports knowledge, reasonable belief or reasonable suspicion that the data breach is eligible.

Firstly, the CEO will consider whether the MNDB scheme applies to the information involved in the data breach. The MNDB scheme does not apply to personal information contained in a document to which the privacy principle requirements do not apply.[4] Relevantly for the CCC, the privacy principle requirements do not apply to personal information arising out of covert activity, witness protection information, and a complaint or investigation of corruption under the CC Act.

If the MNDB scheme does apply, the CEO will then address the section 47(2) IP Act matters (*factors an agency must have regard to when considering if a breach is likely to result in serious harm*) and any other relevant factors when making the assessment.

Some types of data breaches are more likely to cause serious harm. Factors to consider in assessing the potential for harm include:

- the type of information accessed, disclosed or lost (e.g. security classified information or information relating to confidential and sensitive matters will be more significant than, for example, names and email addresses on a newsletter subscription list) and whether a combination of types of personal information might lead to increased risk (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).
- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the breach being discovered.
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (for example, whether any individuals are at a heightened risk of harm or have decreased capacity to protect themselves from harm).
- the circumstances in which the breach occurred, including whether the breach occurred as part of a targeted attack or through inadvertent oversight, and whether the incident was a one-off or exposes a more systemic vulnerability.
- the foreseeable harm to affected individuals/organisations, including consideration as to who is in receipt of the data and whether a risk of physical safety, financial loss, damage to reputation or other harm is at stake.

The CEO must carry out the assessment in an expeditious way and in any event, within 30 days of the CCC becoming aware of the data breach. If the CEO is satisfied that the assessment cannot reasonably be completed within 30 days, the timeframe can be extended under section 49 IP Act. The CEO may only extend the assessment period by a further period that is reasonably required to complete the assessment.

Before the initial 30-day assessment period expires, the CEO must:

- start the assessment; and
- give the Information Commissioner written notice that the CCC has extended the time for the assessment to take place, and the day the extended period ends.

[4] See IP Act s 46(1) and sch 1.

Step 4: Notifying the eligible data breach

If an eligible data breach has occurred, the notification process under Part 3 of the MNDB scheme will be triggered unless an exemption applies.

Exemptions from notification obligations

Chapter 3A, part 3, division 3 of the IP Act sets out the circumstances in which an agency is not required to comply with the notification obligations, including where:

- complying with the obligation would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal (section 55).
- the eligible data breach involves more than one agency, and the other agency (other than the CCC) is undertaking the notification obligations (section 56).
- the CCC has taken remedial action (section 57).
- complying with the obligation would be inconsistent with a provision of an Act (section 58).
- compliance would create a serious risk of harm to an individual's health and safety (section 59).
- compliance is likely to compromise or worsen the CCC's cybersecurity or lead to further data breaches (section 60).

If the CEO is satisfied that an exemption does not apply, the CEO will commence the notification process. The notification process involves the CEO:

1. Notifying the Information Commissioner of the eligible data breach.
2. Notifying individuals affected by the breach by providing them the information stated in section 53(2) IP Act (see ***Appendix 1***).

Notifying the Information Commissioner

The CCC will, as soon as practicable after forming the belief that a data breach is an eligible data breach, notify the Information Commissioner.

The CCC will notify the Information Commissioner in writing either via the OIC's online portal or by email. The CCC will include the information that is required to be given to the Information Commissioner under section 51(2) IP Act.

If it is not reasonably practicable to include any of the information to the Information Commissioner at the time of notification, the CCC will take all reasonable steps to provide the information to the Information Commissioner as soon as practicable after the written notification is given as required by section 52(2) IP Act.

The CEO is responsible for notifying the Information Commissioner.

Notifying particular individuals

The CCC will, as soon as practicable after forming a reasonable belief that a data breach is an eligible data breach, take the steps set out in section 53 IP Act to notify particular individuals and provide them with the required information (section 53(2) IP Act).

The CCC will consider the three options for notifying individuals and elect the option that is reasonably practicable depending on the particular circumstances of the matter, which includes considering:

- the time, cost and effort required to notify affected individuals; and
- the currency and accuracy of their contact details, which will affect the ability of the CCC to notify the affected individuals.

The CEO is responsible for determining the method of notifying individuals and for approving the correspondence provided to individuals.

Option 1: Notify each individual

Where it is reasonably practicable to notify each individual whose personal information was accessed, disclosed or lost, the CCC will take reasonable steps to notify each individual of the required information.

Individuals will be notified directly, either by telephone, letter, email or in person, depending on the circumstances of the matter.

Option 2: Notify each affected individual

If Option 1 does not apply, the CCC will take reasonable steps to notify each *affected* individual (per Definitions above) in relation to the data breach of the required information, if doing so is reasonably practicable. An individual will be an affected individual if the information involved in an eligible data breach is about them, regardless of whether it was originally collected from the individual or a third party.

Affected individuals will be notified directly, either by telephone, letter, email or in person, depending on the circumstances of the matter.

Option 3: Publish information

If options 1 and 2 do not apply, the CCC will publish the required information on an accessible agency website (ordinarily, the CCC website) for a period of at least 12 months. However, the CCC will not publish the information if it would prejudice the CCC functions.

The CCC will advise the Information Commissioner how to access the published notice. The Information Commission is also required to publish the notice on the Office of the Information Commissioners website for at least 12 months.

Required information

The information that must be notified to the affected individual or published, to the extent it is reasonably practicable, must include the information set out in section 53(2), which includes:

- identifying the CCC as the relevant agency, and, if more than one agency was affected by the data breach, the name of each other agency;
- the contact details of the CCC and/or the relevant CCC officer nominated by the CCC for individuals to contact in relation to the data breach;

- the date the data breach occurred;
- a description of the breach including the type of eligible data breach under section 47 IP Act;
- information about how the data breach occurred;
- if the notification is being made via option 1 or option 2 above:
    - a description of the personal information the subject of the data breach; and
    - the CCC's recommendations about steps the individual should take in response to the data breach; OR
- if the notification is being made via option 3 above:
    - a description of the kind of personal information the subject of the data breach without including any personal information in the description; and
    - the CCC's recommendations about the steps individuals should take in response to the data breach.
- if the data breach involved unauthorised access to or disclosure of personal information, the period during which the access or disclosure was available or made;
- the steps the CCC has taken or will take to contain the data breach and mitigate the harm caused to individuals by the data breach; and
- information about how to make a complaint to the CCC under section 166A IP Act.

While there is no requirement for the CCC to notify individuals whose personal information is not involved in a data breach, if the CCC identifies an individual who is likely to suffer harm for reasons other than their personal information being involved, the CCC will consider notifying these individuals. The CCC will consider doing so where this may assist in mitigating any risk of harm to that individual, though this will only occur in circumstances where it is possible to do so without the risk of further breaches occurring.

Where a data breach involves the personal information of a child, notification should generally be made to the child's parent or legal guardian. For minors aged 16 years or older, the CCC will consider if it is more appropriate to make the notification directly to the child.

Other obligations including external engagement or reporting

The CCC will consider whether it is necessary or appropriate to notify other entities of a data breach depending on the circumstances of the breach and the categories of data involved. It may be appropriate to engage with or report to other agencies, for example, if the breach involves or may involve:

- cyber and information security incidents – the Queensland Government Information Security Virtual Response Team.
- theft or other criminal activity – the Queensland Police Service.
- the loss or unauthorised destruction of a public record – the Queensland State Archivist.

Step 5: Post data breach review and remediation

The CEO will review the circumstances of the breach and conduct further investigations as considered appropriate to determine all relevant causes and consider what short- or long-term measures could be taken to prevent reoccurrence. This step also involves reviewing how the process of managing the data breach occurred, and whether any improvements were identified. Depending

on the nature and scale of the breach, this step may be completed as part of the assessment and mitigation stages.

Preventative actions might include:

- a review of the CCC's IT systems and remedial actions to prevent future data breaches.
- a security audit of both physical and technical security controls.
- review of relevant policies and procedures.
- review of staff/contractor training practices.
- review of contractual obligations and contracted service providers.
- review of processes which involve handling personal information.

Any recommendations to implement preventative actions are to be approved by the CEO, though may be implemented and actioned by various officers across the CCC. The CEO will report annually about eligible data breaches to the CCC Commission and the CCC's Audit and Risk Management Committee.

Communication strategy

The CEO is responsible for the communication strategy in relation to each data breach.

The CCC aims to notify affected individuals, and external reporting agencies, within five business days of a data breach of CCC held information being reported to the Information Commissioner (unless an exemption applies). Notifications to individuals will have regard to this DBP, the MNDB Procedure, and the CCC's Privacy Policy.

The CEO is also responsible for monitoring and reviewing the currency of public notifications of data breaches published on the CCC's website in accordance with section 53(1)(c) of the IP Act.

Record-keeping

The CCC maintains records documenting data breaches and suspected data breaches in its electronic document management system. Breaches that do not meet the threshold of eligible data breach under the MNDB scheme are nonetheless documented and evidence is recorded of the action taken by the CCC in assessing and otherwise dealing with the suspected data breach.

The CEO is responsible for maintaining the register of eligible data breaches of the CCC required under section 72 of the IP Act. The register includes the information set out in subsection 72(2).

Review and evaluation procedures

This DBP will be reviewed and updated at least annually. Where improvements are identified in response to a particular data breach, or changes in legislation or government policy affect the operation of the MNDB scheme, this DBP will be updated as soon as possible to give effect to those improvements and changes.

This policy will remain in effect until updated, superseded or declared obsolete.

Related documents

- *Privacy Policy*