Data Breach Policy

Version 1.0

Approval

Pat Vidgen

Electoral Commissioner

27 / 06 / 2025

Version history

Version	Notes	Author	Date of Change
0.1	Initial Draft	Information & Cyber Security Manager	April 2025
0.2	Incorporated relevant procedures and policy	In-house legal counsel, Information & Cyber Security Manager	May 2025
0.3	Incorporated feedback	In-house legal counsel, Information & Cyber Security Manager	June 2025
1.0	Issued for use	Electoral Commissioner	June 2025

Review

This policy will be reviewed **annually**, or as required to ensure compliance with the *Information Privacy Act 2009* (Qld) (IP Act).

Table of Contents

Purpose

This policy outlines the obligations and responsibilities of the Electoral Commission of Queensland (ECQ) concerning the management and notification of data breaches, in accordance with the *Information Privacy Act 2009* (Qld) (IP Act) Chapter 3A: Mandatory Notification of Data Breach (MNDB) scheme. It ensures that the organisation can effectively respond to data breaches, contain the data breach and mitigate potential harm, and comply with the mandatory notification requirements.

Rationale

The Mandatory Notification of Data Breach (MNDB) scheme under the IP Act imposes specific obligations on agencies regarding the handling of personal information and the notification of eligible data breaches. This policy is established to:

- Ensure compliance with the IP Act.
- Protect the privacy of individuals whose personal information is held by ECQ.
- Minimise the impact of data breaches.
- Maintain transparency and accountability in handling data breaches.

Guiding Principles

ECQ is committed to the following principles in managing and responding to data breaches:

- Compliance: Adherence to all relevant requirements of the IP Act.
- Timeliness: Prompt action to contain, assess, and notification of data breaches.
- Accuracy: Ensuring that all assessments and notifications are accurate and complete.
- Confidentiality: Maintaining the confidentiality of information related to data breaches.
- Mitigation: Taking all necessary steps to mitigate harm to affected individuals.

Responsibilities

- **All Employees:**
    - Report any suspected or actual data breaches to the Cyber Security Team immediately via Digital Technologies Service Desk.
    - Cooperate with investigations into data breaches.
- **Executive Director, Digital Technologies:**
    - Assess and manage data breaches in accordance with this policy and the IP Act.
    - Ensure that all necessary notifications are made.
    - Maintain a register of eligible data breaches.

- **Digital Technologies Incident Response Team:**
    - Page 7 of the *Critical Incident Response Plan* sets out which other ECQ officers have roles to play in responding to an incident which disrupts ECQ election systems, including a data breach.
- **Information Management and Security Committee (IMSC):**
    - Ensure that the organisation has the resources to comply with this policy and the IP Act.
    - Oversee the implementation and review of this policy.
    - The Chair of the IMSC to ensure that they, or a delegate, are authorised to be the OIC portal agency administrator, for the purposes of providing notification to the OIC via the OIC portal (https://www.oic.qld.gov.au).

Policy

Under section 73 of the IP Act, this Policy must be published on ECQ's website.

This policy is to be read in conjunction with the **Digital Technologies Critical Incident Response Plan**, and **ECQ – Data Breach Playbook**.

Managing Data Breaches

Containment, Eradication, and Recovery

- The agency's process for the initial evaluation of a suspected data breach, in order to inform containment and mitigation strategies, will be to validate the data breach claim and identify the likely data sources and/or affected systems and the information owners to inform the subsequent risk assessment.
- All data breaches will be recorded in the ECQ Data Breach Register (**See Appendix 3**).
- Where the data breach is suspected to be the result of an active, or prior, system compromise: the ECQ will handle the cyber security incident, following procedures outlined in the **Digital Technologies Critical Incident Response Plan** in parallel to the containment and mitigation activities relating to the data breach.
- Containment, eradication, and recovery steps will follow the **ECQ - Data Breach Playbook** to ***contain*** the data breach to prevent further access, disclosure, or loss of information and to ***mitigate*** any harm caused by the data breach.
- The Executive Director Digital Technologies will undertake an assessment, including a risk assessment, to determine if it is an 'eligible data breach'. An ***eligible data breach*** is a data breach that involves personal information and is likely to result in '*serious harm'* to an affected individual (defined at page 9 and **Appendix 1**).

Incident Response Support

During response to a data breach, Digital Technologies Incident Response Team may seek additional support from various external agencies or service providers, such as;

- Queensland Government Virtual Incident Response Team

- See also ECQ – Data Breach Playbook and Digital Technologies Critical Incident Response Plan
- External legal support through ECQ's General Counsel

Risk Assessment

- The ECQ will undertake a risk assessment (See **ECQ - Data Breach Playbook**) in parallel with the Data Breach Assessment**.**
- The risk assessment will determine whether the breach is, for example, lower risk (smaller scale / minor) or medium to higher risk (more significant / Suspected Eligible Data Breach). It will also inform and support the decision as to whether the Data Breach is an Eligible Data Breach.
- Each risk level requires a different approach, especially in the context of containment and mitigation and notification obligations. For example, the following considerations may inform what containment measures need to be taken:
    - what happened to cause the incident;
    - can interim controls be implemented;
    - how serious is the incident (i.e. what information and individuals are impacted);
    - does the agency need to work with any third parties to investigate and resolve the incident;
    - is internal assistance from other business areas required (e.g. information security);
    - can the personal information be recovered;
    - can the person who has received information incorrectly be contacted;
    - can the system which has been breached be shut down;
    - can the activity that led to the breach be stopped;
    - can access codes or passwords be revoked or changed; and
    - did the data breach occur due to the actions of an external party (i.e. a cyber-attack).
- The following factors will inform the ECQ's risk assessment:

Factor	Details
Nature and sensitivity of information	**Sensitive information** If the data breach involved sensitive information, the higher the risk of harm to the affected individuals. **Publicity of the data** In addition to sensitivity, the level of publicity already given to the information is also important. The agency should confirm whether the information was already (publicly) accessible. **Linked personal data** Data breaches involving health data, identity documents, or financial data, such as credit card information, are damaging in isolation, but combined with publicly available information, can pose additional risks of serious crimes such as identity theft. For that reason, linked personal information poses a greater risk than isolated personal information.
Amount of information and number of affected individuals	Consider the amount of information affected by the data breach and the total number of individuals whose personal information has been affected. The more data and individuals affected, the higher the risks.
Ease of identifying the individuals	Consider how easy it will be for a party with access to personal information to identify an individual (possibly after comparison with additional information available). The risk depends on whether individuals can be identified directly without any other personal information, or whether additional information from other categories of data is needed to identify the individuals.
Seriousness of the harm	The potential harm to the individuals, and the seriousness of the harm must be determined. Data breaches can be extremely damaging, cause physical harm, psychological stress, humiliation or reputational damage in cases such as identity fraud. If the data breach concerns the personal information of vulnerable individuals (e.g. patients, children), a higher risk of damage may be attributed.
Existing mitigating measures	Existing mitigating measures in place during the data breach should be considered in the overall risk assessment, by asking whether, and how, these measures protect the affected individuals.

Data Breach Assessment (ss 46-49 of the IP Act)

Deciding whether a data breach is an Eligible Data Breach:

- It is important to note that the concept of a ‘data breach’ extends to any information held by an agency, regardless of its format. An ‘eligible data breach’, however, only involves personal information that is *held* by an agency (ie. in document form), regardless of whether it is *disclosed* digitally, in hard copy or verbally.

A Data Breach occurs when there is:

- unauthorised access to, or unauthorised disclosure of, information held by ECQ; or
- the loss of information in circumstances where unauthorised access or unauthorised disclosure of the information is likely to occur.

An Eligible Data Breach is a Data Breach that:

- involves personal information, and
- is likely to result in *serious harm* to an affected individual.

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 to the IP Act, and includes serous physical, psychological, emotional or financial harm to an individual. It also includes serious harm to a person's reputation.

The relevant factors prescribed under the IP Act for assessing whether a data breach may result in *serious harm* to an individual are:

- the kind of personal information accessed, disclosed or lost
- the sensitivity of the personal information
- whether the personal information is protected by one or more security measures
- if the personal information is protected by one or more security measures – the likelihood that any of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the personal information
- the nature of the harm likely to result from the data breach, and
- any other relevant matter.

Where it is not immediately clear whether the data breach is an eligible data breach, the ECQ has 30 days to form a view about whether it has a reasonable suspicion that the data breach is an eligible data breach. The ECQ may seek an extension of that time under section 49 of the IP Act.

'Other relevant matters' will depend on the nature of the data breach, but the following considerations may also assist in assessing the seriousness of the data breach:

- what is the nature of the breach
- is it likely that a counterparty or third party caused the breach
- what is the seriousness of the breach
- has the breach affected another agency
- are there any vulnerabilities of the affected individuals e.g. involving children or a domestic violence victim-survivor
- the effectiveness of the steps taken to control the breach e.g. has containment and mitigation lessened the risk
- has there been unauthorised access, disclosure or loss of personal information that was collected by the agency, and

- if so, would a reasonable person conclude the breach is likely to result in serious harm to an individual to whom the information relates.

The ECQ will record the assessment, including the reasons for the decision, in writing in the Data Breach Register (**See Record Keeping & Appendix 3**).

Eligible Data Breaches trigger the Mandatory Notification of Data Breach (MNDB) requirements under the IP Act (see: 'Eligible Data Breach – Notification Requirements' below).

Eligible Data Breach – Notification Requirements

Decision about whether the relevant data breach is an eligible data breach

Once an assessment has been made, the Executive Director of Digital Technologies will make a recommendation to the Chair of the ECQ IMSC about the status of the data breach and whether it is an eligible data breach.

Statement to OIC and Notification to individuals affected (ss 50-54 of the IP Act):

Where the ECQ reasonably believes that there has been an eligible data breach and an exemption does not apply, (see below) the Chair of the ECQ IMSC must:

a) *Prepare* and give a ***statement*** to the Office of the Information Commissioner (OIC) via the OIC portal as the person authorised to be the OIC portal agency administrator, which contains the information set out in section 51(2)(Refer to OIC Online Portal for notifying);

b) Where practicable to do so, ***notify*** (with the information set out in paragraph (c) below):
   i. each *individual* whose personal information has been accessed, disclosed, or lost; or
   ii. to each '*affected individual'* for the data breach; or
   iii. where (i) and (ii) are not practicable, publish the relevant information on its website.

c) The ***statement*** to the OIC referred to in paragraph (a) above, must, to the extent it is reasonably practicable to do so, include the following:

   i. the information that must be included in a notification given under paragraph (d) below (except the information referred to at (d)(vi) and (vii));

   ii. a description of the kind of personal information the subject of the data breach, without including any personal information in the description;

   iii. the ECQ's recommendations about the steps individuals should take in response to the data breach;

   iv. whether the agency is reporting on behalf of other agencies affected by the same data breach and, if so, the details of the other agencies;

   v. the total number or, if it is not reasonably practicable to work out the total number, an estimate of the total number of each of the following:
      - all individuals affected or likely to be affected by the data breach;

- affected individuals for the data breach

vi. either:

- the total number of individuals notified of the data breach or, if it is not reasonably practicable to work out the total number, an estimate of the total number; or

- if section 57 is relied on, the total number of individuals who would have been notified if that section had not been relied on or, if it is not reasonably practicable to work out the total number, an estimate of the total number;

vii. whether the individuals notified have been advised about how to make a privacy complaint to the agency under section 166A.

d) The ***notification*** to individuals, affected individuals, or the public, referred to in paragraph (b) above must, to the extent it is reasonably practicable to do so, include the following information:

i. the name of the agency and, if more than 1 agency was affected by the data breach, the name of each other agency;

ii. the contact details of the agency or a person nominated by the agency for the individual to contact in relation to the data breach;

iii. the date the data breach occurred;

iv. a description of the data breach, including the type of eligible data breach under section 47;

v. information about how the data breach occurred;

vi. for a notification under subsection 53 (1)(a) or (b)—
- a description of the personal information the subject of the data breach; and
- the agency's recommendations about the steps the individual should take in response to the data breach;

vii. for a notification under subsection 53 (1)(c):
- a description of the kind of personal information the subject of the data breach, without including any personal information in the description; and
- the agency's recommendations about the steps individuals should take in response to the data breach;

viii. 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;

ix. the steps the agency has taken or will take to contain the data breach and mitigate the harm caused to individuals by the data breach;

x. information about how an individual may make a privacy complaint to the agency under section 166A.

*How to notify particular individuals (See also **Appendix 2** for sample letter)*

How affected individuals/organisations affected by the data breach are notified will depend on the type and scale of the breach, as well as the immediate practical issues such as having contact details for the affected individuals/ organisations.

Option 1: Notify each individual

If it is reasonably practicable to notify each individual whose personal information was accessed, disclosed or lost, the agency must take reasonable steps to notify each individual of the required information directly. This may include by telephone, letter, email or in person.

Option 2: Notify each affected individual

If Option 1 does not apply, agencies must take reasonable steps to notify each affected individual of the required information for the data breach, if doing so is reasonably practicable.

Under sections 47(1)(a)(ii) and (b)(ii) of the IP Act, an 'affected individual' is someone to whom the personal information relates, and who is likely to suffer serious harm as a result of the data breach.

Option 3: Publish Information

If the agency cannot directly notify each individual (Option 1) or each affected individual (Option 2), it must publish the required information on its website for a period of at least 12 months, in accordance with section 53(1)(c) of the IP Act. An agency is not required to include information in its notice if it would prejudice its functions. An agency must advise the Information Commissioner how to access the notice and the Commissioner is required to publish the notice on the Commissioner's website for at least 12 months.

Communications Strategy

- All public and internal communications will be developed and produced in consultation with the ECQ Communications Team.

- ECQ has other reporting obligations, which could include:
    - Queensland Police Service
    - Queensland Government Cyber Security Unit
    - Australian Cyber Security Centre
    - Commonwealth Notifiable Data Breach Scheme
    - Crime and Corruption Commission
    - Queensland Government Insurance Fund
    - Queensland Government State Archives

Record Keeping

- The ECQ will maintain a Data Breach Register of all data breaches, including details of the breach, the assessment, and actions taken. (**See Appendix 3)**.

- The ECQ is to ensure that all records are accurate and up-to-date.
- The Register will include the following information in relation to data breaches:
    - a description of the eligible data breach, including the type of data breach under section 47
    - the date the agency gave a statement to the Information Commissioner about the eligible data breach and the date any additional information was provided to the Commissioner
    - if individuals were directly notified about the eligible data breach,[6] the register must include the individuals who were notified and the date and method by which they were notified
    - if the agency relied on an exemption[7] exempting notification to either the Information Commissioner or individuals, details of the exemption
    - details of the steps taken by the agency to contain the eligible data breach[8] and mitigate its harm;
    - if an eligible data breach is also a breach of another Act, details of that Act; or if the agency was required by contract, another law, or circumstances to notify an external party, details of that party and the date of notification; and

Exemptions

- Notification is not required if an exemption under sections 55-60 of the IP Act applies. The exemptions are:
    - Notification could prejudice an Investigation or legal proceedings;
    - The data breach relates to more than one agency and one of the other agencies is providing the notification
    - The ECQ has taken remedial action so that the data breach is no longer likely to result in serious harm to any individual
    - Notification would be inconsistency with a confidentiality provision in an Act, whether in Queensland or a Commonwealth law
    - Notification would create serious risk of harm to health or safety to an individual (see section 59, as there are still some alternative notification requirements in such cases)
    - Notification would compromise ECQ's cybersecurity or lead to further data breaches for the ECQ (certain notice requirements still apply in such cases – see section 60(3) and (4)).

Post Data Breach review

- A decision about who or which entity will conduct a post data breach review and remediation will be made based on the nature and scale of the breach.

- Conducting a post data breach review will be undertaken utilising the Digital Technologies Post Incident Review (PIR) process.

- What is required to remediate will be determined by the nature and scale of the data breach. This is particularly relevant to building an agency's corporate knowledge around data breach responses, and will assist in mitigating future risks of reoccurrence or similar breaches, and improving personal information handling processes in line with community and regulator expectations

- It will include a review of any key learnings from the data breach and potential changes that should be made to prevent or reduce a risk of reoccurrence, and a prompt to consider revising and updating systems, processes and procedures relevant to data breaches

Appendix 1 — Definitions

Term	Definition
Data Breach	Either unauthorised access to, or unauthorised disclosure of, information held by the ECQ, or the loss of information in circumstances where unauthorized access or unauthorized disclosure is likely to occur.
Eligible Data Breach	A data breach involving personal information that is likely to result in serious harm to an affected individual.
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable from the information or opinion.
Serious Harm	Includes serious physical, psychological, emotional, or financial harm, or serious harm to an individual's reputation.
Affected Individual	An individual to whom the personal information relates, and who is likely to suffer serious harm as a result of the data breach.

Appendix 2 – Sample Letter – Individuals and Affected Individuals

Who should use this template?

This template will assist Queensland government agencies to complete a notification to affected individuals under the mandatory notification of data breach scheme.

Why should I utilise this template?

The template is provided as a guide for agencies when they are required to notify affected individuals about an eligible data breach. Under the MNDB scheme an agency has an obligation to notify affected individuals, the template provides a framework and overview of information that may be relevant when an agency is required to notify an affected individual. The agency should also refer to the *Information Privacy Act 2009* s 53(2) to ensure relevant information regarding the data breach is included in the notification letter.

How to use this template

Text in ***bold and italics*** are provided as a guide and should be reviewed to **update or delete.** Your letter should reflect information specific of the data breach and consider the affected individual you are notifying to ensure the reader can understand what has occurred. Keep the language plain and free from jargon.

[Date]

Dear ***[name of affected individual],***

We are writing to notify you of a recent data breach that involves ***a/an access, disclosure, loss*** of your personal information. Our agency, ***add name of your agency,*** is making contact to provide you information regarding the breach, including information about the actions taken by our agency to contain the breach and options you may want to consider, or further actions you can take.

Incident Information

Date***: 'on or 'between dates'***

Time: ***'at' or 'between times'***

****The summary of the incident is to be provided here.***

****Include a description of the data breach, including the type of eligible data breach (s 47) so the affected person understands why the incident is considered a data breach.***

****Advise how the data breach occurred.***

Affected personal information

Whilst responding to the breach our agency identified the personal information that has been affected due to the incident. The personal information involved includes:

Provide a full list and description of the personal information subject of the data breach.

This aim of providing the full information subject of the breach is to enable the affected person to take proactive steps and make their decisions regarding other actions steps they may need to take to protect themselves.

What has our agency done to contain the breach?

List the steps your agency has taken to contain and mitigate - s 48 (2) E.g. restricted access to affected system, isolated affected device, reset passwords etc.

You can also provide information on the actions taken to reduce the likelihood of a future breach occurring. E.g. introduction of multi-factor authentication, encryption of sensitive data.

Next steps

Please take the time to review the information in this letter and the type of personal information affected by the data breach. You should consider if the personal information involved in the data breach is likely to cause harm. This may include, financial loss, concern for physical safety or damage to reputation or relationships. Depending on the circumstances, some of the actions you may wish to consider to protect yourself include:

Remember to delete text that is not applicable to the data breach incident. You can add further recommendations that are relevant to the data breach scenario to advise the affected individual what they should consider in response to the data breach

Risk of harm is identity fraud including contact information

The below are suggestions** only **– agencies will need to determine appropriate advice:

Change your related account password as soon as possible.

You may wish to contact IDCare on 1300 432 273 or visit www.idcare.org . IDCare can provide specific guidance on the steps you can take to protect yourself from identity fraud.

Keep an eye out for emails and telephone calls where they are requesting your personal details. This may include a request for information for your home address, an email address, your date of birth, account usernames, passwords or personal identification numbers.

Should you start to receive unwanted telemarketing calls, consider registering your number with the Australian Communications and Media Authority's 'Do Not Call register' by visiting www.donotcall.gov.au/consumers/register-your-numbers. You can also contact your service provider and request to change your number.

Risk of harm involves financial information

The below are suggestions** only **– agencies will need to determine appropriate advice:

Contact your financial institution as soon as possible, to enable additional monitoring and security actions to your account.

Enable multi-factor authentication (if able), change your online banking password (if applicable), cancel affected debit or credit card, change your personal identification number (PIN).

Continue to review your bank statements and online banking transactions for unauthorised purchases. Report any discrepancies to your bank as soon as possible.

You may consider contacting Australia's three credit reporting agencies (Equifax, Illion and Experian) to understand if your identity has been used to obtain credit without your knowledge. You may consider making a request for a credit ban to be put in place.

If the affected personal information relates to your tax file number of superannuation, contact the Australian Tax Office on 1800 467 033 and your superannuation fund to discuss if additional monitoring needs to be placed on your account.

Risk of harm involves Health Information

• ***The below are suggestions** only **– agencies will need to determine appropriate advice:***

Contact your health service provider using their contact details, either located on their website or via hard copy information you may hold.

It is also important to consider your physical safety. If you are at risk of domestic violence and in immediate danger, contact police on triple zero (000) immediately, or if you are not in immediate danger you may wish to contact DVConnect on 1800 737 732, Womensline on 1800 811 811 or Mens Helpline on 1800 600 636. If you are feeling distressed due to this incident, you may want to consider contacting your doctor, a support service or family or friends.

Further information is also available at the Office of the Information Commissioner website What to do if you're affected by a privacy breach.

Seeking more information and making a complaint

If you have any questions or concerns about what has happened or would like further information, you can contact:

[individual or department's name within your organisation]

[phone number] or [email].

If you would like to make a privacy complaint because you are not satisfied with how our agency has managed this incident, or you have suffered harm as a result, you can do so by contacting us at this email address: ***@XXXXXX***

Our agency is committed to resolving your complaint and we would value an opportunity to understand how you were affected by the incident, and what you would like done to resolve the complaint.

Whilst we will endeavour to resolve your complaint, you are able to make a complaint to the Office of the Information Commissioner when:

- you do not consider our response to your complaint to be adequate, or
- we have not responded to you by the end of the response period, which is 45 days unless you have agreed to an extension of this time.

Please find website link for further information Make a privacy complaint | Office of the Information Commissioner Queensland.

Yours sincerely,

[Name]

[Position/Title]

[Organisation name]

Appendix 3 – Eligible Data Breach Register

(As required by section 72 *Information Privacy Act 2009*)

Date of Breach	Description of EDB / type of data breach	Date statement provided to OIC	Date additional information supplied to OIC or N/A	Individuals notified, including date and method	Details of any exemption (s) relied on, or N/A	Steps taken to contain and mitigate	Actions taken to prevent similar breaches