Policy document

Data breach

This policy applies in cases where the Independent Planning Commission must respond to a breach of data that is held by the Commission.

1. POLICY OUTLINE

The Commission collects data, including personal information provided by submitters, in the course of its public consultation on specific development applications. The Commission has agency-level cybersecurity controls in place and treats personal information confidentially and sensitively. Please see the Commission's Privacy Statement and Public Submission Guidelines for more information on the Commission's practices and associated guidance to the public.

However, if the information held by the Commission is breached, this policy sets out the Commission's procedures for managing the data breach, including the considerations required regarding the notification of persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists the Commission in avoiding or reducing possible harm to both the affected individuals/organisations and the Commission, and may prevent future breaches.

2. SCOPE

This policy applies to all staff and contractors of the Commission. This includes temporary and casual staff, private contractors and consultants engaged by the Commission to perform the role of a public official.

3. PURPOSE

The purpose of this policy is to provide guidance to staff in responding to a breach of Commission-held data, especially personal information. It sets out procedures for managing a data breach, including the considerations around notifying persons whose privacy may be affected by the breach, including:

- providing examples of situations considered to constitute a data breach
- the steps involved in responding to a data breach
- the considerations around notifying persons whose privacy may be affected by the breach
- template correspondence for notifying persons whose privacy may be affected by the breach.

Effective breach management, including notification where warranted, assists the Commission in avoiding or reducing possible harm to both the affected individuals/organisations and the Commission, and may prevent future breaches.

4. WHAT IS A DATA BREACH?

A data breach occurs if there is a failure that has caused or has the potential to cause unauthorised access to Commission-held data, such as:

- accidental loss or theft of classified material data or equipment on which data is stored (e.g., paper record, laptop, tablet or mobile phone, or USB stick)
- unauthorised use, access to or modification of data or information systems (e.g., sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems)

- unauthorised disclosure of classified material or personal information (e.g., email sent to an incorrect recipient or document posted to an incorrect address or addressee), or personal information posted to the Commission's website without consent
- compromised user account (e.g., accidental disclosure of user login details through phishing)
- failed or successful attempts to gain unauthorised access to Commission information or information systems
- equipment failure
- malware infection
- disruption to or denial of IT services.

A data breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

A data breach does not include circumstances in which the Commission has not maintained confidentiality in any information provided to it that the Commission has not expressly committed to keep confidential under law or the Commission's polices (particularly the Commission's *Privacy Statement*).

For example, a data breach has not occurred when a person inadvertently discloses personal information in a submission to the Commission that the Commission then publishes on its website in accordance with its policies.

5. RESPONDING TO A DATA BREACH

The Office of the Independent Planning Commission's Executive Director and/or Director, Legal must be informed of any data breach to ensure the application of this policy and to ensure the Chair of the Commission is sufficiently advised so that appropriate responses can be provided to enquiries made by the public, and for the management of any complaints that may be received resulting from the breach.

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

1. Contain the breach
2. Evaluate the associated risks
3. Consider notifying affected individuals
4. Prevent a repeat.

Each step is set out in further detail below. The first three steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

The Department of Planning and Environment (DPE) and/or its service providers support the Commission in the supply and maintenance of its IT systems. The Executive Director or delegate will coordinate with the DPE and/or its service providers to address and respond to identified data breaches related to its IT systems.

5.1 STEP ONE: CONTAIN THE BREACH

Containing the breach is the priority. All necessary steps possible must be taken to contain the breach and minimise any resulting damage. For example: recover the personal information; shut down the system that has been breached; suspend the activity that led to the breach; revoke or change access codes or passwords.

If a third party is in possession of data and declines to return it, it may be necessary for the Commission to seek legal or other advice on what action can be taken to recover the data. When recovering data, the Commission will make sure that copies have not been made by a third party or, if they have, that all copies are recovered.

5.2 STEP TWO: EVALUATE ASSOCIATED RISKS

To determine what other steps are needed, an assessment of the type of data involved in the breach and the risks associated with the breach will be undertaken.

Some types of data are more likely to cause harm if compromised. For example: personal information; health information; and security classified information will be more significant than names and email addresses on a newsletter subscription list.

Given the Commission's regulatory responsibilities, release of case-related market sensitive information will be treated very seriously.

A combination of data will typically create a greater potential for harm than a single piece of data (for example, an address, date of birth and bank account details, if combined, could be used for identity theft).

Factors to consider include:

- Who is affected by the breach? This includes review of whether individuals and organisations have been affected by the breach, how many individuals and organisations have been affected and whether any of the individuals have personal circumstances which may put them at particular risk of harm.

- What was the cause of the breach? This includes review of whether the breach occurred as part of a targeted attack or through inadvertent oversight. Was it a one-off incident, has it occurred previously, or does it expose a more systemic vulnerability? What steps have been taken to contain the breach? Has the data or personal information been recovered? Is the data or personal information encrypted or otherwise not readily accessible?
- what is the foreseeable harm to the affected individuals/organisations? This includes review of what possible use there is for the data or personal information. This involves considering the type of data in issue (such as health information personal information subject to special restrictions under s.19(1) of the Privacy and Personal Information Protection Act 1998 (PPIP Act) if could it be used for identity theft, or lead to threats to physical safety, financial loss, or damage to reputation. Who is in receipt of the data? What is the risk of further access, use or disclosure, including via media or online? If case-related, does it risk embarrassment or harm to a client and/or damage the Commission's reputation?

5.3 STEP THREE: CONSIDER NOTIFYING AFFECTED INDIVIDUALS & ORGANISATIONS

Notification to individuals or organisations affected by a data breach can assist in mitigating any damage for those affected individuals/organisations. Notification demonstrates a commitment to open and transparent governance, which is consistent with the Commission's policies.

Accordingly, the Commission adopts a relatively lower threshold in considering whether to notify individuals of the release or risk to the security of their personal information and will generally make such a notification. The Commission will also have regard to the impact upon individuals in recognition of the need to balance the harm and distress caused through notification against the potential harm that may result from the breach.

There are occasions where notification can be counterproductive. For example, information collected may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitise individuals to a significant privacy breach.

Factors to consider when deciding whether notification is appropriate include:

- Are there any applicable legislative provisions or contractual obligations that require the Commission to notify affected individuals?
- What type of information is involved?
- What is the risk of harm to the individual/organisation?
- Is this a repeated and/or systemic issue?
- What risks are presented by the mode of the breach e.g., is it encrypted information or contained in a less secure platform e.g., email?
- Does the breach relate to casework functions and include case-related material flowing from the exercise of our regulatory functions?
- What steps has the Commission taken to date to avoid or remedy any actual or potential harm?
- What is the ability of the individual/organisation to take further steps to avoid or remedy harm?
- Even if the individual/organisation would not be able to take steps to rectify the situation, is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual/organisation?

Notification will be done promptly to help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves

The method of notifying affected individuals/organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals/organisations.

Considerations include the following:

5.3.1 WHEN TO NOTIFY

In general, individuals or organisations affected by the breach who the Commission considers should be notified, should be notified as soon as is practicable. Circumstances where it may be appropriate to delay notification include where notification would compromise an investigation into the cause of the breach or reveal a software vulnerability.

5.3.2 HOW TO NOTIFY

Affected individuals or organisations should be notified directly – by telephone, letter, email or in person. Indirect notification – such as information posted on the Commission's website, a public notice in a newspaper, or a media release – should generally only occur where the contact information of affected individuals/organisations are unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained).

5.3.3 WHAT TO SAY

The notification advice will be tailored to the circumstances of the breach. Content of a notification could include:

- information about the breach, including when it happened
- a description of what data or personal information has been disclosed
- assurances (as appropriate) about what data has not been disclosed
- what the Commission is doing to control or reduce the harm
- what steps the person/organisation can take to further protect themselves and what the Commission will do to assist people with this
- contact details for the Commission for questions or requests for information
- the right to lodge a privacy complaint with the Privacy Commissioner. The template is at Appendix A.

5.4 STEP FOUR: PREVENT A REPEAT

The Commission's investigation will determine the relevant causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Preventative actions could include a:

- security audit of both physical and technical security controls
- review of policies and procedures
- review of staff/contractor training practices
- review of contractual obligations with contracted service providers.

5.5 REPORTING BREACHES

The template at Appendix B is to be used for reporting on the investigation of the breach and authorising actions in response. The Officer delegated by the Executive Director will prepare a report using the template and provide the report to the Director, Legal.

The Director, Legal will review the proposed actions and recommendations of the report and provide to the Executive Director and Chair of the Commission for approval.

The Executive Director will be responsible for delegating responsibility for the implementation of proposed actions and recommendations.

5.3.4 NOTIFYING THE PRIVACY COMMISSIONER

The Chair of the Commission may notify the NSW Privacy Commissioner of a data breach where personal information has been disclosed and there are risks to the privacy of individuals. In doing so the Commission will ensure relevant evidence is contained securely for access by the Privacy Commissioner should regulatory action be considered appropriate. Such notification will:

- demonstrate to the affected individuals and broader public that the Commission views the protection of personal information as an important and serious matter and may therefore maintain public confidence in the Commission
- facilitate full, timely and effective handling of any complaints made to the Privacy Commissioner regarding the breach and thus assist those whose privacy has been breached.

Notification should contain similar content to that provided to individuals/organisations. The personal information about the affected individuals is not required. It may be appropriate to include:

- a description of the breach
- the type of personal information involved in the breach
- what response the Commission has made to the breach
- what assistance has been offered to affected individuals
- the name and contact details of the appropriate contact person
- whether the breach has been notified to other external contact(s).

DOCUMENT GOVERNANCE

Document ID	Data Breach Policy
Owner	Executive Director, OIPC
Custodian	Director, Legal
Approved	23 August 2023

For more information

Office of the Independent Planning Commission NSW

Suite 15.02, Level 15, 135 King Street

SYDNEY NSW 2000

Phone: (02) 9383 2100

Email: ipcn@ipcn.nsw.gov.au