Office of the Information Commissioner
Queensland

PRIVACY BREACH RESPONSE PLAN

1 Purpose

The purpose of this Privacy Breach Response Plan is to set out the procedure to be followed by Office of the Information Commissioner (**OIC**) staff in the event that OIC experiences a privacy breach, or suspects that a privacy breach has occurred within OIC.

This plan must be followed when assessing and responding to an actual or suspected data breach that involves personal information.

A hard copy of this document is to be maintained by OIC Commissioners in the event that OIC ICT systems are affected by a cyber security incident.

2 Effective Date

Approved by the Information Commissioner on 25 March 2022.

3 Application

The Privacy Breach Response Plan applies to all employees and contractors engaged by OIC.

This document is to be read in conjunction with OIC's Business Continuity Plan, which consists of the:

- Emergency Response Plan
- Disaster Recovery Plan
- Emergency Communication Plan.

4 Key concepts

Information Security Event - A security 'event' is 'an identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant' [ISO/IEC 27000:2018].

Information Security incident - An information security 'incident' is defined as 'a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security' [ISO/IEC 27000:2018].

Personal Information - Personal information is defined in the *Information Privacy Act 2009* (Qld) as information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Privacy breach - A privacy breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.

Privacy breaches can occur for a variety of reasons including:

- human error
- misconduct by an employee
- malicious activity by an external party involving a cyber-attack or physical access to the office and files

As the appropriate responses to each of these activities will be different, examples of these types of activities and appropriate examples of a response are included in this procedure.

4.1 Examples of types of privacy breaches

Example: privacy breaches resulting from human error • *Loss of an employee's laptop, USB or paper records that contain personal information held by OIC (e.g. left on a train or bus)* • *Accidental disclosure of personal information to the wrong recipient (e.g. sending an email to the wrong addressee)*
Example: privacy breaches resulting from malicious activity • *Scams that trick you into releasing personal information* • *Inappropriate or fraudulent use of an OIC database containing personal information*

Example: Common network security threats that may result in a privacy breach
• *Malware Attack - A malware attack is an umbrella term that refers to a range of different types of security breaches. This includes the following:*
  ○ *Trojan or Trojan horses – programs that appear as a typical file but that hid malicious behaviour*
  ○ *Ransomware – malware viruses that block access to data until a 'ransom' is paid*
• *Password Attack – Attacks where a hacker guesses a password to gain access to a computer system*
• *Denial-of-Service (DoS) and Distributed-Denial-of-Service (DDoS) Attacks - A DoS attack attempts to knock a network or service offline by flooding it with traffic to the point the network or service can't cope. A DDoS attack hijacks devices (often using botnets) to send traffic from multiple sources to take down a network*
• *Man-in-the-Middle Attacks – An attack where a hacker compromises a customer's system to launch an attack on your server, either by sneaking through an already established connection, or by stealing a customer's IP address and disguising themselves as the customer*

Example: privacy breaches resulting from unforeseen circumstances • *OIC office premises are broken into and physical files are stolen*

5 Procedure

There is no single way OIC will respond to a privacy breach if one occurs, as privacy breaches can be caused or exacerbated by a number of factors. Each breach will be dealt with by OIC on a case-by-case basis, with OIC undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

In line with the Australian Cyber Security Centre (**ACSC**) 'Data Spill Management Guide', there the OIC has identified five key steps that it will generally follow when responding to a privacy breach or suspected privacy breach; these are:

a. identify that a breach has occurred
b. contain the breach
c. evaluate the risks associated with the breach
d. consider whether notification is appropriate
e. prevent future breaches.

Each of these steps is addressed in further detail below.

5.1 Step 1 - identify the breach

5.1.1 Identifying the privacy breach

If you become aware of an actual or suspected privacy breach, you must:

- report it as soon as possible to your line manager.
- discontinue any process that may be the cause of the privacy breach. If you were the cause of the incident or undertaking a process that has led to the incident, you should not continue with that process until further advised by your manager.

The responsible manager must:

- report the breach to the Director Engagement and Corporate Services (**DECS**)
- undertake preliminary assessment of the actual or suspected breach.

In the event of a privacy breach, the following questions should be addressed when making the preliminary assessment:

- when did the breach occur?
- what type of information is involved?
- what was the cause of the breach?
- what is the extent of the breach?
- how can the breach be contained?

The DECS is responsible for leading the response once reported, in consultation with the relevant area, commissioner, a privacy officer and the Information Commissioner.

*Where the DECS identifies parties may have a conflict of interest, consideration should be given to engaging external advisor and/or the OIC Information and Assistance (**I&A**) Team.*

The DECS will maintain a record of OIC Privacy Breaches and resulting actions. The OIC Privacy Breach Report Template may be useful in capturing a record of the steps taken to contain or control a privacy breach.

5.2 Step 2 - contain the privacy breach

If appropriate, and in consultation with relevant stakeholders (see list in part 7 of this procedure), steps should be immediately commenced to initiate a process of containment. For example:

- stop the unauthorised process
- recover any records
- shut down the system that was breached. If it is not practical to shut down the system, account privileges should be revoked or changed.

Below are examples of containment / remedial steps that may be appropriate:

Example: if breach involves electronic records held on an ICT system:
• *Isolate the causes of the breach in the relevant system, software or database*
• *Shut down the compromised system, software or database*
• *Reset log-in details and passwords for compromised devices, systems or databases*
• *Quarantine any compromised devices*
Example: if the breach involves the loss of a device or physical files
• *Arrange to have the lost device remotely disabled*

- *Arrange a search of the site where the loss occurred by contacting any relevant authorities (e.g., public transport authorities, airlines)*

Example: if the breach involves the unauthorised disclosure of personal information to a third party

- *By email – recall the email from the recipient and ask the recipient not to read the email, delete the email and request a confirmation by email when these steps have been completed*
- *By post – contact the recipient and ask them not to open or read the posted materials, and arrange for collection/return of the posted materials*
- *By publication online – deactivate the link to the publication*

5.3 Step 3 - evaluate the risks

Once the breach is contained, the following factors should be considered to asses the risk:

- What system has been compromised [redacted]
- What vendor is involved [redacted]
- Who is affected?
- What information is involved (contact details, email addresses, financial information)?
- What is the source of compromise, and the timeframe involved?
- What parties have gained unauthorised access to the information?
- What are the harms (to affected persons) that could potentially be caused by the breach (financial, reputational, embarassment)?
- How could the information be used – is there a foreseeable harm to the affected individual (identity theft, financial loss, humiliation)?
- Does the breach indicate a systemic problem with OIC's practices and procedures?
- What is the reputational damage to OIC?
- What is OIC's legal liability?

The Risk Assessment Tool in Appendix 1 may assist in assessing the impact of a privacy breach. Consideration should then be given to whether the residual risk is consistent the OIC's risk appetite.

The OIC Privacy Breach Self-Assessment tool may also provide guidance on assessing the risk of *"serious harm to an individual"* caused by a privacy breach.

5.4 Step 4 - notify stakeholders

Some types of privacy breaches are required by law to be reported to regulatory or oversight bodies. Othertimes it is good practice to report the breach to an oversight body to alert them to the risks and issue guidance to assist in resolving the issue and minimise the risk to other agencies, particularly where the breach is the result of a malicious attack from a third party.

5.4.1 Notify the Office of the Australian Information Commissioner (OAIC)

The *Privacy Act 1988* (Cth) established a Notifiable Data Breaches (**NDB**) scheme in Australia.

This scheme applies to all entities that are subject to the Australian Privacy Principles under the *Privacy Act* (e.g. many Australian Government agencies and private sector organisations with an annual turnover of more than $3 million). It also applies to certain credit providers, credit reporting bodies, and holders of tax file number information. Therefore, it will apply to OIC should the privacy breach involve a tax file number.

Data breaches that are 'eligible data breaches' and are required to be reported to the Office of the Australian Information Commissioner (**OAIC**) can be reported using the Notifiable Data Breach Form.

5.4.2 Mandatory reporting obligations under Information security policy IS18:2018

While all Queensland Government departments must apply the policy requirements in IS18:2018 to all information, applications and technology assets, statutory bodies such as OIC should also consider the Information Security Incident Reporting requirements when a data breach occurs as a result of an information security event or incident as defined in the QGEA Information security incident reporting standard.

5.4.3 Notification of a criminal offence, corrupt conduct or misconduct

A breach of privacy may also be a criminal offence, corrupt conduct or misconduct.

If the breach of privacy may involve a criminal offence, consideration should be given to reporting the matter to the Queensland Police Service.

If the breach of privacy involves suspected corrupt conduct the matter must be reported to the Crime and Corruption Commission (**CCC**). This can be done online by completing an online report. In these circumstances there are restrictions on dealing with the allegation until advised by the CCC. Urgent matters can be resolved by seeking verbal approval from the CCC on 07 3360 6285.

Any allegations of misconduct will be dealt with in accordance with OIC's Complaint Management Procedure.

5.4.4 Notifying Individuals

The *Information Privacy Act 2009* (Qld) does not obligate an agency to notify individuals who have been affected by a privacy breach. However, a failure to notify may compound the damage for the individuals affected by the breach and reflect negatively on an agency's reputation. In general, if a risk of serious harm is likely to occur to an individual, they should be notified. It may not always be possible to know the extent of the risk, for example of contact information being released to others, where OIC is not aware that individuals are victims of family and domestic violence. OIC will take a cautious approach to enable individuals to assess risk of harm in such circumstances and take appropriate precautions.

Notification can also demonstrate a commitment to OIC's privacy obligations and an open and transparent governance.

Prompt notification to individuals in these cases can help to avoid or lessen the damage by enabling the individual to take steps to protect themselves.

Factors to consider when deciding whether notification is appropriate include:

- What is the risk of harm to the individual?
- If the individual was a vulnerable member of the community, for example a victim of family or domestic violence, would the risk of harm change?
- What is the ability of the individual to take further steps to avoid or remedy harm?
- Is the information that has been compromised sensitive, or likely to cause humiliation or embarrassment for the individual?
- Are there any applicable legislative provisions or contractual obligations that requires your agency to notify affected individuals?

There are occasions where notification to an affected individual can be counterproductive. For example, 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 - for example, where OIC has confirmed the breach has been contained without risk to others.

Once all factors have been considered, the DECS, in consultation with a privacy officer and Commissioners, will assess whether an affected individual should be notified. If affected individuals are to be notified, the Information and Assistance Team should be advised what information can be provided or who they should refer calls to in response to telephone inquiries.

5.4.5 Notifying the Queensland Parliamentary Legal Affairs and Safety Committee

The Parliamentary Committee's functions include monitoring and reporting on the performance of the OIC, and reporting to the Legislative Assembly about any matter that it considers should be drawn to the Assembly's attention.

In the event of a privacy breach, the Information Commissioner will action reporting requirements appropriate to the nature of the breach and investigation, on advice from DECS and Commissioners.

5.4.6 Media management

All media releases, requests and alerts should be directed to the Training and Stakeholder Relations Team. All media requests will be assessed by the Manager Training and Stakeholder Relations to recommend an appropriate course of action to the IC or delegate and respond accordingly.

5.5 Step 5 - prevent future breaches

Once the breach has been contained, if appropriate, further investigations will be carried out by the involved business areas to determine all relevant causes of the breach and consider what short or long-term measures could be taken to prevent any reoccurrence.

Below are some examples of further actions that could be considered in particular situations:

Example: if breach was caused by employee conduct, could OIC: • *Provide any staff training, reminders or additional oversight or supervision of staff to prevent a re-occurrence* • *Increase auditing or monitoring of staff* • *Change any staff policies or procedures* • *Introduce new controls or restrictions on staff access*
Example: if the breach involved a security breach by a third party, could OIC: • *Improve its IT or building security* • *Apply any additional security protections (e.g. encryption, use of pseudonyms)* • *Give any directions to staff or contractors* • *Introduce new access restrictions*

The Information Commissioner must be briefed on the outcome of any investigation into a privacy breach, including any recommendations.

The DECS will report to the Governance Committee monthly on risks arising from breaches, and actions taken, including any trends and systemic issues. Specific breach investigation outcomes may also result in monthly or quarterly monitoring and review by the Governance Committee, in accordance with the Risk Assessment Tool at Appendix 1.

6 OIC Roles and Responsibilities

6.1 General roles and responsibilities of staff

All OIC Staff	Record and advise your manager/commissioner of - the time and date the suspected breach was discovered - the type of information involved - cause and extent of the breach if known - context of the affected information and the breach

Managers/Directors/Assistant Commissioners **Privacy & RTI Commissioners**	Assess and determine whether a likely privacy breach has occurred. If confirmed, notify DECS of breach. Ensure that staff cease actions/process until breach is contained.

DECS	The DECS is responsible for leading the OIC assessment and response once reported, carrying out the investigation and finalising a report about the breach to the Information Commissioner.
	
	Insignificant or Minor breach:
	
	- record details of breach, remedial action taken by OIC and the outcome of that action
	- work with manager/Commissioner to ensure breach does not reoccur and communicate lessons for OIC/other teams
	- report on breaches to Governance Committee monthly, including trends and systemic issues, recommended action
	
	Moderate, Major or Critical breach:
	
	- notify Information Commissioner of breach
	- coordinate response
	- identify and engage/notify relevant stakeholders of breach.
	It is not necessary that all stakeholders be included in all privacy breach responses unless the stakeholder is affected or involved or can assist in mitigating the harm caused by a breach
	- investigate breach and prepare a report for the Information Commissioner, including recommendations to:
	  - make appropriate changes to policies and procedures
	  - revise staff training practices if necessary, and
	  - update this response plan if necessary.
	- record details of breach and action taken by OIC to address the breach. DECs will manage the folder in [redacted] with appropriate permissions and access.
	
	Where the DECS identifies parties may have a conflict of interest, consideration should be given to engaging external advisor and/or the OIC Information and Assistance (I&A) Team.
	
	Manage communications and escalations in relation to ICT/data breaches [redacted] to relevant vendors.

Training & Stakeholder Relations (TSR)	Contract management: Privacy or ICT/data breaches [redacted]

	Media management: Assess and respond to requests from media, prepare releases
Information & Assistance (I&A)	Respond to enquiries about OIC privacy breaches Provide guidance and assistance to ELT and Privacy team
Governance Committee	Review and monitor reports on breaches from DECS

7 Key contacts/stakeholders

Contact	When to contact
[redacted]	[redacted]
[redacted]	[redacted]
Crime and Corruption Commission	If the breach involves corrupt conduct within the meaning of the *Crime and Corruption Act 2001* Phone: 07 3360 6285 (Executive Direction, Integrity Services) https://www.ccc.qld.gov.au/public-sector/assessing-and-notifying
Office of the Australian Information Commissioner	If the breach involves Tax File Numbers (TFN) or if any obligations under the *Privacy Act 1988* (Cth) apply https://www.oaic.gov.au/privacy/notifiable-data-breaches/report-a-data-breach/
Parliamentary Committee	Legal Affairs and Safety Committee Parliament House George Street BRISBANE QLD 4000 Phone: 07 3553 6641 | Fax: 07 3553 6699 Email: lasc@parliament.qld.gov.au
Queensland Government Information Security Virtual Response Team (QGISVRT)	Privacy breaches involving cyber security incidents, ICT systems or with broader implications for OIC Phone: 07 3215 3951 Email: qgisvrt@qld.gov.au
Queensland Government Insurance Fund (QGIF)	Privacy breaches involving a cyber incident that results in a loss and OIC is considering making a claim https://qgif.qld.gov.au/
Queensland Police	Privacy breaches that appear to involve theft or other criminal activity. QPS has links and assistance to report cybercrime.

8 References

- *Information Privacy Act 2009* (Qld)
- Mobile ICT Devices Policy
- Privacy breach management and notification guideline
- QGEA Information security incident reporting standard
- Risk Management Framework
- Use of ICT services, facilities and devices Policy
- Use of Portable storage devices Policy
- Information Standard 18
- Australian Cyber Security Centre (**ACSC**) 'Data Spill Management Guide'

9 Resources

- OIC Work From Home Tip Sheet
- [redacted]
- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (nist.gov)
- ICT risk matrix | Queensland Government Enterprise Architecture (qgcio.qld.gov.au)

10 Amendment Log

Date	Version No.	Officer	Change
10/06/2021	Draft v1.0	[redacted]	
06/07/2021	Draft v1.1	[redacted]	[redacted]
04/08/2021	Draft v1.2	[redacted]	[redacted]
18/08/2021	Draft v1.3	[redacted]	[redacted]
11/10/2021	Draft v1.4	[redacted]	[redacted]
	Draft v1.5	[redacted]	[redacted]

Appendix 1

The following tool may assist in assessing the impact of a privacy breach by 'risk scoring'. Risk scoring is achieved when you multiply the *probability* against the *impact.*

Impact Criteria

When assessing impact look at what the actual impact and damage to the individual concerned.

	Impact Criteria			
	Harm to individual(s)	**Reputational harm to OIC**	**Cost**	**#**
Insignificant	No harm to individuals.	Nil or minor impact on reputation. Unlikely to be reported in the media.	Trivial impact on budget <$1,000	1
Minor	No or little harm to individuals, which could include minor inconvenience or disruption to their activities.	Small impact on reputation, may be some local news reports for 1- 2 days.	Minor impact on budget <$10k	2
Moderate	Likely harm to individuals that would require them to take some action or ensure their welfare is not impacted.	Moderate impact on reputation sustained regional and/or national negative perception.	Moderate impact on budget <$100k	3
Major	Harm to individuals which has impacted on their safety and will need to action to protect their interests	Sustained regional and/or national negative perception.	Significant cost impact on budget <$500k Remediation is likely to be time consuming and complex	4
Critical	Individuals suffer harm which requires them to take action to protect their safety or financial security.	Sustained negative national perception.	Large cost impact on budget >$500k Remediation is likely to be time consuming and complex	5

Likelihood Criteria

When assessing likelihood, assess what is the probability of this breach happening again.

Likelihood Criteria		
Rare	One off incident - will not be repeated	1
Unlikely	May happen again, but remedial actions make this unlikely	2
Possible	Could happen again but remedial action has reduced this likelihood	3
Likely	Is likely to happen again within 1-7 days unless action is taken	4
Almost certain	Is likely to happen again almost immediately unless action is taken ASAP	5

The Matrix

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Critical
Rare	LOW Accept the risk Routine management	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Unlikely	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
Possible	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quartely senior management review	HIGH Quarterly senior management review
Likely	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review	EXTREME Monthly senior management review
Almost certain	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	EXTREME Monthly senior management review	EXTREME Monthly senior management review