| **What to do if you have found a potential information breach.** |
| --- |
| **If there is an immediate risk to a person’s life, health or safety, call 000 now.****This self-assessment tool gives you a process to follow and suggestions for help and advice.**Your agency might have its own form or a version of this tool that you can use. For assistance with dealing with a potential breach and the tool, refer to the people in your agency who handle information security or privacy, read the Office of the Information Commissioner’s online [guidance](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/privacy-breach-management-and-notification) (OIC) or call the OIC’s enquiries service on (07) 3234 7373.  |
|  |  |  |  |  |
| **Are you a government employee or contractor who has discovered a potential breach of your agency’s data?**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | **Yes - continue** |  | **No – Stop; this tool is designed to help government staff deal with a possible breach of government-held information** |  |

 |
| A government agency is a department, a local government, a public authority, a university or a hospital and health service. (‘Your agency’ includes a government agency contracting you to provide services). |
| **If you are acting as an individual, you may have a privacy complaint. Alternatively, you may be concerned about information you have received. In either of these circumstances, start by contacting the relevant government agency.** |
|  |  |  |  |  |
| **Does the breach involve personal information?**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | **Yes - continue** |  | **No – Stop; this tool is about personal information** |  |

See the OIC’s guidelines about [personal information](https://www.oic.qld.gov.au/guidelines/for-government/access-and-amendment/introduction-to-the-acts/what-is-personal-information) and [privacy breaches](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/privacy-breach-management-and-notification) for advice about personal information.**If it involves personal information, it may be a privacy breach. Seek advice from the people dealing with privacy in your agency. You may have to act on any data breach. Seek advice from the people dealing with information security in your agency.** |
|  |  |  |  |  |
| **What type of harm might happen?** (Identifying the type/s of harm will help you assess the risk.) |
| * physical
* identity theft
* loss of benefits
* loss of employment
 | * reputational, agency or person
* loss of access to information
* humiliation or loss of dignity
* financial
 | * emotional
* psychological
* discrimination
* other – please describe
 |
|  |  |  |  |  |
| **Is the breach likely to cause serious harm?** (Each of these characteristics adds to the likelihood of serious harm.)

|  |
| --- |
| **If you have a privacy breach and potential harm is:** |
| **Not serious/ Unlikely**No need to notify OIC | **Serious/ Unlikely**Consider notifying OIC |
| **Not serious/ Likely**No need to notify OIC | **Serious/ Likely****Recommend notifying OIC** |

Seriousness (extent, depth and duration of harm)* the breach may lead to imminent, irreparable physical, psychological or financial harm – **consider immediate action and notification**
* the harm might be costly – physically, personally or financially
* the harm would require sustained remedial action
* the harm is difficult to remedy
* the breach involves a combination of types of information
* the information is sensitive, for example, medical records

Likelihood (amount, dispersal and ease of access, and intent)* harm has already occurred
* there is a risk of further access, for example online or via media
* the breach affects many people (also might increase seriousness)
* the breach occurred on multiple occasions or with other breaches (also might increase seriousness)
* the personal information is easily accessed, for example, was not encrypted or anonymised
* the information went to a person likely to cause harm, for example, if stolen or in a domestic violence situation

**Seek advice from people handling privacy or information security in your agency to help you answer these questions.**  |
|  |  |  |  |  |
| **What steps have you taken to reduce the potential harm?*** **if the breach is from a computer system**, contact your computer / information systems team immediately (they may need to access or lock down the system and collect evidence)
* recover information before the information is accessed, for example, hard copy documents
* fix any non-computer related problems that caused the privacy breach, for example, securing rooms or cupboards
* contact the people who received the information to discuss mitigating harm, if that might help
* contact the people who may be affected to enable them to take immediate steps to minimise harm, for example to avoid or lessen the impact of disclosed financial information or contact details.
 |
|  |  |  |  |  |
| You may need to notify:* **internally** in your agency, for example, your line manager or a designated person or team, like your cybersecurity, privacy, media or communications team – seek advice
* **externally** (for example, information security, the insurer, police, OIC, OAIC)– seek advice fromyour agency

Consider your responsibility to notify individuals whose information has been breached. Prompt notification to individuals can help to avoid or lessen the damage by enabling the individual to take steps to protect themselves. Transparency and clear information about a breach is also important to help build trust. Refer to OIC online [guidance](https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/privacy-breach-management-and-notification). Talk to people in your agency handling privacy or contact OIC’s Enquiries Service on (07) 3234 7373. |
|  |
| **Agency assessment record** |
| **You may wish to expand this assessment record.****For example, you may wish to record details of the breach, details of action taken in response, any contact made for assistance, delegated decision-making authority, notification decisions, reasons for decisions.****As a minimum, include the following details in this record.** |
| Assessor’s name/signature | Assessor’s position | Date of assessment |