|  |
| --- |
| <Project name>  **Privacy Impact Assessment Report**  <Day> <Month> <Year> |
| **NOTE**  This template is provided by the Queensland Office of the Information Commissioner (**OIC**) as an example of information generally included in a PIA Report. It is a guide only. You may need to adapt the template to meet your agency’s needs or include additional information to address the size and complexity of your project.  Instructions and tips for completing the report are provided in blue italicised text. Please delete it as you complete each section.  This template is intended to be used in conjunction with *Undertaking a Privacy Impact Assessment* and other relevant OIC guidelines. If you are unsure about the need to conduct a Privacy Impact Assessment (PIA), *Threshold privacy assessment at a glance* and the *Threshold privacy assessment form* may be useful. If you answer yes to any questions in the threshold assessment form, the project will benefit from a PIA.  Please send your feedback on suggested improvements and your experience using the template to [enquiries@oic.qld.gov.au](mailto:enquiries@oic.qld.gov.au) or contact the Enquiries Service on 07 3234 7373 for information on the privacy obligations in the Information Privacy Act 2009 (Qld).  Published 16 September 2014 and Last Updated \*\*\*\*\*  Changes to legislation after the update date are not included in this document |

## **Document information**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date PIA completed: |  | | | |
| Status: | New PIA | Update. Date of previous version: | | |
| Prepared by: |  | | | |
| Position: |  | | | |
| Email: |  | | Telephone: |  |

## **Endorsement and approval**

Project manager:

I **recommend** the project proceeds as proposed in this document.

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Name: |  | | |
| 1. Position: |  | | |
| 1. Signature |  | 1. Date: |  |

The following officer/s have **endorsed** this document:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Name: |  | | |
| 1. Position: |  | | |
| 1. Signature |  | 1. Date: |  |

*Add further names as required*

Project Executive/Steering Committee/senior management:

I **agree** to the project proceeding as proposed in this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | | |
| Position: |  | | |
| Signature |  | 1. Date: |  |
| 1. Comments: | | | |

**Table of contents**

[**Document information** 2](#_Toc158987765)

[**Endorsement and approval** 2](#_Toc158987766)

[**Table of contents** 3](#_Toc158987767)

[**1** **Introduction** 4](#_Toc158987768)

[**1.1** **Purpose** 4](#_Toc158987769)

[**1.2** **Applicable legislation** 4](#_Toc158987770)

[**1.3** **Project description** 4](#_Toc158987771)

[**1.4** **Scope of the PIA** 4](#_Toc158987772)

[**1.5** **Review** 4](#_Toc158987773)

[**2** **Personal information flows** 5](#_Toc158987774)

[**3** **Risk analysis** 7](#_Toc158987775)

[**3.1** ***Information Privacy Act 2009* (Qld)** 7](#_Toc158987776)

[**3.2** **Legislative confidentiality and human rights** 16](#_Toc158987777)

[**3.3** **Risk Ratings** 18](#_Toc158987778)

[**4** **Actions to address the identified risks** 19](#_Toc158987779)

[**5** **Stakeholder consultation** 20](#_Toc158987780)

[**6** **PIA outcomes** 21](#_Toc158987781)

[**6.1** **Agreed recommended actions** 21](#_Toc158987782)

[**6.2** **Action plan** 21](#_Toc158987783)

[**6.3** **Contact point for future enquiries** 21](#_Toc158987784)

1. **Introduction**
   1. **Purpose**

This Privacy Impact Assessment (PIA) Report:

* identifies possible impacts on the privacy of individuals' personal information; and
* recommends options for mitigating or minimising any negative impacts.
  1. **Applicable legislation**

This PIA analyses the privacy impacts of collecting, storing, using and disclosing personal information for the purposes of <the project> against the privacy obligations in the *Information Privacy Act 2009* (Qld) (IP Act). It also analyses the project and its information against relevant provisions of the *Human Rights Act 2019* (Qld) and legislative confidentiality obligations.

*If your agency’s enabling legislation or other legislation explicitly requires, permits or limits the collection, use or disclosure of personal information involved in this project, you should also cite the legislation and relevant sections within that Act. The IP Act does not override the provisions of other Acts which relate to or prohibit the collection, use or disclosure of information.*

* 1. **Project description**

*Explain the project and what it intends to achieve by addressing the following key points:*

* *what the project will deliver*
* *why the project is needed*
* *the benefits to the agency or the community; and*
* *whether the project is part of a program of related projects.*

*The term ‘project’ is used broadly in this context. It is intended to cover the full range of activities and initiatives that may have privacy implications, such as new systems, processes or practices for handling personal information, new legislation or policies, or an information sharing initiative.*

* 1. **Scope of the PIA**

*If applicable, explain what part or stage of the project the PIA covers and, if necessary, what it does not cover.*

* 1. **Review**

*In the case of a large or complex project, the PIA may need to be reviewed a number of times throughout the project’s lifecycle to ensure that its findings continue to be relevant. If applicable, outline any dates or milestones that will be used as a checkpoint to review whether anything significant has changed since this PIA was completed.*

1. **Personal information flows**

This section explains how personal information will flow through the agency’s systems and processes as a result of the output or deliverable to be produced by the project. It describes:

* what personal information will be collected for what purposes
* who it will be collected from
* how it will be used and disclosed
* who will have access to it; and
* how it will be stored and protected.

*Describe what personal information is involved and document how this information will flow through the proposed new system or process. For example:*

* *What kind of information being collected and who is it collected from?*
* *Will the project collect sensitive information? Will the agency have consent to collect it?*
* *How will the information be collected?*
* *Why is the personal information necessary for the project?*
* *How will it be stored and what safeguards will be put in place to protect it?*
* *Who will have access to the information?*
* *What will the personal information be used for and by whom?*
* *Will the personal information be routinely disclosed and if so, to whom will it be given and for what purpose?*
* *How can individuals seek access or amendment to their personal information?*
* *How long will the information need to be retained?*

*Keep in mind that personal information includes any information or opinion about a living individual who is or can reasonably be identified. Whether information is about a reasonably identifiable individual requires case-by-case consideration of factors such as: the nature and amount of information, who will have access to the information, and what other readily available information could reasonably be used to cross match or link the information to the individual. See Key privacy concepts – personal and sensitive information for more information.*

*There is no ‘one size fits all’ approach to documenting the flow of information. The following table is one example of how you could describe the information flows. You may prefer to use a diagram or business process map. The approach will depend on the complexity of the project’s information flows.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business process/activity**  *(For example, an individual applies for permit or licence)* | **Components of personal information**  *(For example, name, date of birth, address, whether it is sensitive information)* | **Collection**   * *From?* * *By whom?* * *How?* * *Lawful authority (if any)?* | **Storage**   * *How?* * *Where?* * *By whom?* * *For how long?* | **Use**   * *By whom?* * *Why?* * *When?* * *How?* * *Lawful authority (if any)?* | **Disclosure**   * *By whom?* * *To?* * *Why?* * *When?* * *How?* * *Lawful authority (if any)?* * *Overseas?* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Risk analysis**
   1. ***Information Privacy Act 2009* (Qld)**

*The following table provides an overview of the Queensland Privacy Principles (QPPs) and other IP Act obligations. It includes key questions to help you to identify potential privacy risks and examples of common potential risks. These are not exhaustive, but provide an indication of the types of questions you could consider.*

|  |  |  |
| --- | --- | --- |
| **Privacy principles** | **Proposed information handling practices** | **Identified risks** |
| **Make individuals aware (QPP 5)**  Notify individuals or make them aware of the matters (QPP 5 matters) listed in QPP 5.2 which are relevant to the collection.  The QPP 5.2 matters include:   * Agency identity and contact details. * Details of any law or court order that require or authorise collection. * Why the information is being collected (this is the primary purpose). * Any consequences for not providing the information. * Anyone to whom the agency will regularly disclose the information. * If the information will be disclosed overseas and where it will be disclosed. * If information was collected from someone else and the individual may not be aware of the collection: the individual must be informed of the collection and its details. | *Are there any laws that require or authorise the agency to collect this information? If so, include details of the legislation and the relevant section and a description of the information to be collected. Include only those laws that create an explicit authority or obligation for your agency to collect personal information, rather than legislation that broadly details the nature and extent of the agency’s responsibilities and powers.*  *Are there any consequences if the individual doesn't provide the information? What are they? Can they be mitigated or reduced or are they absolute?*  *Will information be disclosed to someone else and/or overseas? To whom and where?*  *What reasonable steps will be taken to ensure individuals are informed or aware of the QPP 5 matters:*   * *when information is collected directly form the individual?* * *when it's collected from someone else?* | * *QPP 5 matters are not consistently provided, for example, across all communication channels.* * *QPP 5 matter failures may inhibit future use or disclosure if the agency cannot establish the primary purpose of collection or individual were told the wrong primary purpose.* * *Individuals are not aware of how their personal information will be used, or to whom it will be routinely disclosed, which can lead to a lack of trust.* * *Individuals do not know the agency collected their personal information.* |
| **Anonymity or pseudonymity (QPP 2)**  Where lawful and practicable, individuals must have the option of not identifying themselves | *Can individuals choose to not identify themselves when interacting with the agency? If not:*   * *Why is it impracticable or unlawful to allow the individual to remain anonymous or to use a pseudonym?* * *Will individuals be required to verify their identity? If so, do their identification documents need to be recorded or just sighted?* * *How will individuals be advised that they can or cannot remain anonymous or use a pseudonym?* | * *Collecting personal information and/or identifiers that are not required.* * *Assuming individuals must always provide their name.* * *Allowing anonymity where a law requires identities.* |
| **Collection of personal information (QPP 3)**  QPP 3 only applies to personal information solicited by the agency.  Only collect personal information reasonably necessary for or directly related to an agency's function or activities.  Only collect personal information from the individual it's about, unless:   * they consent * a law or court order allow you get it from someone else; or * it is not reasonable or practical to do so.   Obtain personal information lawfully and fairly.  Take steps to ensure the information is accurate, complete and up-to date. (QPP 10) | *Will personal information be collected directly from the individual it is about? If not:*   * *have they consented?* * *is there a relevant law or court order?* * *why it is not reasonable or practical to do so?*   *If the information isn't collected from the individual, how will you ensure it's accurate, complete and up to date?*  *Will the information be sourced from an internal system? If yes, will the personal information be used or disclosed for the primary purpose of collection? If not, does QPP 6 allow it to be used or disclosed for a secondary purpose?*  *Is the personal information being collected for more than one purpose (e.g. demographic information that is collected that will be used to improve customer engagement)? If so, how will an individual know what information will be used for which purpose?*  *Is the individual likely to be upset by the way in which their personal information will be collected? If so, is the collection unlawful or unfair?*  *What business process or function is enabled by collecting this information? How is the collection of each piece of personal information necessary for this purpose?* | * *Personal information is collected without a clear purpose, which could increase the risk of scope creep or unauthorised use/disclosure.* * *Information collected is either unnecessary or excessive.* * *Information is collected unfairly because the individual provides information that they would not have, had they known they had a choice not to provide it.* * *Personal information collected from a third party may be of poor quality, as the affected person does not have the opportunity to check the data for accuracy.* |
| **Collection of sensitive information (QPP 3.3 and 3.4)**  Sensitive information can only be collected with the individual's consent, unless QPP 3.4 applies.  Schedule 5 sets out what kinds of personal information are sensitive information, including health, religion, and sexuality. See *Key privacy concepts – personal and sensitive information* for full details.  QPP 3.4 only allows it to be collected without consent if:   * Collection is required by a law or court order. * A permitted general situation listed in schedule 4, part 1 exists. * You are a law enforcement agency collecting it because it's reasonably necessary or directly related to a function or activity. * You are a health agency dealing with health information and a permitted health situation listed in schedule 4, part 2 exists. | *Is sensitive information being collected? If so:*   * *Is it necessary?* * *Are individuals likely to consent, eg because they receive a clear benefit?* * *How will you establish that they consent, particularly if collecting it from someone else?*   *If individuals don't or are not likely to consent does one of the exceptions apply? Will it always apply or will its application be time limited or apply only in certain situations?* | * *Collection of sensitive information without the authority to do so.* * *Collection of sensitive information when it was not required.* * *Can also lead to sensitive information being inappropriately considered when making a decision.* * *Reliance on invalid or outdated consent.* * *An individual’s refusal of consent, or conditional consent, is not respected.* |
| **Unsolicited information (QPP 4)**  Unsolicited personal information must be assessed and either retained as personal information or destroyed/de-identified (subject to public records obligations) | *Will the project allow people to provide unsolicited information? If so, how will it be identified, managed and assessed?*  *Can the provision of unsolicited personal information be limited or restricted?*  *Do systems allow a distinction to be made between solicited and unsolicited information?*  *What steps will be taken to identify any public records requirements?*  *How will it be destroyed or de-identified?* |  |
| **Limits on use and disclosure (QPP 6)**  Personal information can only be used and disclosed for the primary purpose of collection, ie the reason it was collected.  Use and disclosure for a **secondary** purpose is only permitted where the use or disclosure falls within QPP 6, which includes:   * the permitted general situations in schedule 4, part 1; and * for health agencies, the permitted health situations in schedule 4, part 2.   Use and disclosure are defined in section 23, but essentially:   * Use is anything an agency does with information while it controls it. * Disclosure is giving information to someone who doesn't know it and the agency will cease to control it. | *Will the personal information be routinely disclosed outside the agency? If yes, how and why is this information being disclosed?*  *What reasonable steps will be taken when collecting personal information to make the individual aware of this disclosure (as required under QPP 5)?*  *What process will be followed when a request is made to use or disclose personal information for a secondary purpose? How will you ensure that QPP 6 applies? For example:*   * *by or for a law enforcement agency* * *where authorised or required by law or court order* * *where the individual has expressly or impliedly consented* * *for public interest research* * *for ADR or court proceedings.*   *Will consent be relied on to use or disclose the information? If yes, will you be relying on implied or express consent?*   * *If you are relying on implied consent, what are the facts and circumstances of the particular situation that support an assumption of the individual’s consent?* * *If you will be seeking express consent, how will you ensure their consent is valid, i.e. that it is voluntary, informed, specific and current? What mechanisms will be in place to accommodate an objection to the proposed use or disclosure? Will individuals be permitted to opt out if they change their mind and if so, how?* | * *Function creep – information collected for one purpose is used/disclosed for another purpose.* * *Information is used/disclosed in circumstances not permitted under the IP Act. If found to be in breach of the IP Act, there is capacity for an individual to be awarded up to a maximum of $100,000 in compensatory damages.* * *Individuals are surprised or upset by a secondary use or disclosure, which can lead to a privacy complaint, a lack of trust or negative publicity.* * *An individual’s refusal of consent, or conditional consent, is not respected.* |
| **Disclosure out of Australia**  An agency can only disclose personal information out of Australia if it complies with section 33. This means:   * the individual must agree * there must be a legal authority to do so * it must necessary to prevent or lessen a serious threat; or * two of the four criteria in section 33(d) can be satisfied. | *Will personal information be disclosed outside Australia? Disclosure requires the agency to cease having control of the information, so using overseas based tools will not automatically be a disclosure overseas. If so, what provision in section 33 of the IP Act will be relied upon to permit this disclosure?*  *If relying on agreement, how will you ensure their agreement is valid, i.e. that it is voluntary, informed, specific and current? What mechanisms will be in place to accommodate an objection to the overseas disclosure? Will individuals be permitted to opt out if they change their mind and if so, how?*  *If section 33(d) will be relied on, what evidence can be provided to show that its requirements have been satisfied?* | * *Personal information disclosed outside Australia is not afforded the same of privacy protections as are in Queensland’s IP Act.* * *Individual does not wish for their information to be disclosed outside Australia.* * *An individual’s refusal of consent, or conditional consent, is not respected.* |
| **Data quality (QPP 10)**  Take reasonable steps to:   * ensure personal information being collected is accurate, up to date and complete; and * ensure personal information being used and disclosed is accurate, up to date, complete and relevant to whatever is being done with it. | *For example:*  *What reasonable steps will be taken to ensure the information is accurate, complete and up to date at the time it is collected?*  *Has the information been supplied by the individual directly? If not, can it be checked with the individual who it is about? How will you ensure its accuracy etc?*  *What reasonable steps will be taken to ensure the information is accurate, complete and up to date before it is used or disclosed?*  *What reasonable steps will be taken to ensure only relevant personal information is being used or disclosed?*  *How will you know when the personal information was last updated?*  *Is it information that is likely to change over time (such as an address) or information that is static (such as a date of birth)?*  *How damaging will it be to the individual if inaccurate etc information is used/disclosed? (The more damaging it will be, the more rigorous the required steps.)*  *Is there any opportunity for individuals to routinely correct or update their personal information or to verify its accuracy?* | *Common risks may include:*   * *Incomplete, inaccurate or out-dated information lead to incorrectly informed decisions, which in turn may have a negative impact on the individual concerned.* * *Inadvertent disclosure of personal information if the agency sends correspondence using incorrect or out of date contact information.* |
| **Data security (QPP 11)**   * Take reasonable steps to protect personal information from misuse, loss and unauthorised access, modification or disclosure. * If the personal information is no longer needed, take reasonable steps to de-identify the information. | *For example:*  *What steps will be taken to protect the personal information from misuse, loss and unauthorised access, modification or disclosure – while in transit and at rest? Has the project considered operational (e.g. policies or training), technical (e.g. access controls or encryption) and physical controls (e.g. doors or locks)? Are these safeguards adequate to provide the level of protection that can reasonably be expected to be provided? Can you reference any standards or documents that support the chosen controls?*  *How will access be controlled? Who will authorise access? What process will be used to grant access? How will access be changed or revoked when the user leaves or their role changes? Will access be audited regularly?*  *What measures will be in place to prevent and detect misuse or unauthorised access? For example – will audit logs enable actions to be linked to individuals and will these logs be reviewed on an ongoing basis?*  *What training and awareness is necessary to ensure that staff are aware of their privacy and confidentiality obligations, as well as the agency’s security policies and practices?*  *Can the personal information be accessed remotely? Can users access or save the personal information to their personal device? If yes, what controls will be in place?*  *Is there a testing or training environment? If yes, is real or dummy data used?*  *What steps will be taken to ensure that the information will be identified where it is no longer required? What steps will be taken to ensure any deidentification complies with public records requirements?* | *Common risks may include:*   * *Access is not limited to the ‘need-to-know’ requirement.* * *System users with administrative privileges is not limited to staff requiring those privileges.* * *Access is not revoked promptly when no longer required.* * *The system does not log who has accessed a file, making it difficult to detect or investigate unauthorised access or misuse.* * *Staff are unaware of their privacy, confidentiality and security obligations.* * *Information is saved onto privately-owned storage devices, increasing the risk of loss, unauthorised access or disclosure.* * *Personal information is kept for longer than required under approved retention and disposal schedule/s.* * *Information is not deidentified, increasing the risk of a privacy breach.* * *Information is deidentified in breach of public records requirements.* |
| **Openness, access and amendment of documents containing personal information (QPP 1, 12, 13)**   * Agencies must have a QPP Privacy Policy that complies with QPP 1.4. * Individuals can access their personal information under QPP 12. * Individuals can correct their personal information under QPP 13. | *Will requests from individuals for access to, or amendment of, documents containing their personal information be handled as a formal application under the Right to Information Act 2009 (Qld) or can the request be handled administratively?*  *Will the project allow information to be amended if it is inaccurate, irrelevant, incomplete, out of date or misleading? If information cannot be altered, what mechanism will be in place for a notation to be attached?*  *Can information be extracted from the project systems in generic format, eg a text file or PDF?*  *If information is held by a contracted service provider, how can your agency get it back when you need it?*  *Will your agency’s QPP privacy policy need to be updated in light of this project? If yes who is responsible for doing so?* | *Common risks may include:*   * *Individuals are not able to easily access or amend their personal information.* * *An individual’s access to their personal information may be hampered if the data is held by a contracted service provider.* * *An individual’s lack of access to their personal information increases the risk of inaccurate or outdated information.* * *The QPP Privacy Policy does not accurately reflect the types of personal information held by the agency or its information handling practices. This reduces its effectiveness in terms of helping an individual to find out what information is held about them or how their personal information is managed and protected.* |
| **Use of contracted service providers (chapter 2, part 3)**  Take reasonable steps to bind a contracted service provider to the IP Act if the agreement satisfies section 34(2) and 35. Generally when:   * the contract involves personal information; and/or * the contractor will be providing a service on behalf of the agency. | *Will the project involve contracting an external service provider to provide a service for the purpose of performing a function of the agency? And is this service provided directly to the agency, or to a third party of behalf of the agency? If so, will the provision of services under the contract or arrangement involve the exchange or handling of personal information in any way?*  *If yes: what steps will your agency take to ensure that the service provider is bound to comply with the IP Act? Note – even if the service provider is subject to the Commonwealth Privacy Act 1988 you must still take all reasonable steps to bind them to Queensland’s IP Act as the obligations in the Commonwealth legislation do not apply to a contracted service provider for any acts or practices it undertakes in relation to a State Government contract.*  *Have you considered additional contractual provisions, such as limiting secondary use, placing conditions on the use of sub-contractors or mandatory reporting of any breaches?*  *It is recommended that you contact your procurement unit and/or legal services unit to ensure the contract includes clauses/provisions to bind the service provider appropriately.* | *Common risks may include:*   * *Reliance on the contractor being covered by the Commonwealth Privacy Act* * *Existing government Information Technology Contracting (GITC) framework contracts may not adequately address the privacy risks of this particular project.* * *The standardised contracts in the Queensland Information Technology Contracting (QITC) framework may not adequately address the privacy risks of this particular project.* * *If the contractor has not been appropriately bound to comply with the IP Act, the contracting agency will be liable for any breaches arising from the actions of the service provider.* |
| **Mandatory data breach notification (chapter 3A)**  Chapter 3A of the IP Act places robust obligations on agencies to manage and respond to eligible data breaches, including mandatory data breach notification (MDBN). | *How will eligible data breaches be identified?*  *What systems or policies will be used to inform internal stakeholders of data breaches and undertake mandatory data breach notification?*  *How will the information required by section 47 be identified and complied?*  *What steps will be taken to include the data breach in the agency's data breach register?* | * *A failure to comply with chapter 3A could result in OIC intervention.* * *A failure to identify data breaches increases the potential damage from the breach.* * *Loss of public trust and confidence.* |

* 1. **Legislative confidentiality and human rights**

*The IP Act governs the collection and handling of personal information by agencies, but it is not the only limitation on how agencies deal with information. The Human Rights Act 2019 (Qld) (HR Act) contains a right to privacy and a right to access government information. Agencies may also be subject to confidentiality and secrecy provisions in their governing legislation and the IP Act does not override or displace these provisions. The OIC cannot assist with non-IP Act obligations, but it is important that they are considered as part of the PIA.*

|  |  |  |
| --- | --- | --- |
| **Act** | **Proposed information handling practices** | **Identified risks** |
| **The HR Act**  Agencies must act compatibility with human rights in the *Human Rights Act 2019* (Qld) (**HR Act**), including:   * the human right to privacy (section 25) * the human right to access government information (section 21) | Is the project generally compatible with these (and any other relevant) rights?  Can people access their information and information about the project? Will the agency proactively publish information about the project or provide it administratively on request?  Will the project impact individual's privacy generally, eg bodily privacy or territorial privacy? Are individuals informed about how the project will impact on their privacy?  If the project limits these rights, is the limitation reasonable and justifiable? How is it reasonable and justifiable? If it's not reasonable and justifiable, is the limitation required by, or a result of compliance with, another law?  Does the project strike an appropriate balance between any competing rights? | * *Decisions or actions incompatible with Human Rights may be a breach of the HR Act.* * *Could result in a complaint to the Queensland Human Rights Commission.* * *Breaching human rights impacts public trust and confidence and can harm the affected individuals.* |
| *Are there any confidentiality or secrecy obligations in your governing legislation or other laws which apply to the project or its information? If so, list them here.*  *If there are none, write Nil in all three boxes. This demonstrates that you considered this issue.*  *Examples of confidentiality/secrecy obligations are sections 186-188 of the Child Protection Act 1999 (Qld) and sections 142-142A of the Hospital and Health Boards Act 2011 (Qld).* | *Do they apply to the project or its information? For example, because of the type of information involved, the individuals involved, or how or why the agency acquired the information?*  *Are there any exceptions? Do they apply to the project? Do you need approval, eg from the chief executive, to rely on the exceptions?* | * *There may be offences for using or disclosing confidential information* * *If confidential information is used or disclosed in contravention of these provisions, it could result in disciplinary action or monetary penalties.* * *A breach of confidentiality or secrecy provisions may also be a breach of the IP Act, which can result in a privacy complaint.* |

* 1. **Risk Ratings**

*Rating each risk can help you to prioritise your responses according to how likely it is that the risk will materialise and the severity of its consequences. You should refer to your agency’s risk management framework for guidance on the descriptors for risk likelihood and consequences and definitions of the overall ratings. You should also record all privacy and confidentiality risks in the project’s risk register/log.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Identified privacy risk** | **Consequences for the individual or agency** | **Likelihood** | **Risk rating** |
| 1 | *Copy your list of identified risks from section 3.1 and 3.2* | *E.g. Minor, Moderate, Significant* | *E.g. Unlikely, Possible, Likely* | *E.g. Low, Medium, High* |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |

1. **Actions to address the identified risks**

*Describe the strategies or actions that will mitigate or minimise the identified risks. Note: While a PIA does not set out to eliminate every possible privacy or confidentiality risk; risk management does not provide an alternative to compliance with the privacy principles, HR Act, or legislative confidentiality or secrecy provisions. Privacy and confidentiality need to be incorporated with other project goals, not balanced against them.*

*Adapt this table to suit the nature of the project and the needs of your agency, particularly as large or complex projects may require a more complex risk analysis. For example, an assessment of any residual risk, or a more detailed analysis of the costs, strengths and weaknesses of all potential actions that could address the risks.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Identified privacy risk** | **Existing controls that contribute to managing the identified risk** | **Recommended actions** | **Comments** |
| 1 | *Copy your list of identified risks from sections 3.1 and 3.2* | *What current safeguards help mitigate or minimise the identified risks?* | *What additional measures can be implemented to mitigate or minimise the risk?* | *If there are other strategies that could address the risk, provide comments about why the recommended action is the preferred option.* |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
|  |  |  |  |  |

1. **Stakeholder consultation**

*Consultation with key stakeholders is essential to the PIA process. It helps to ensure that key privacy issues are identified, addressed and communicated. Provide details of who you consulted with, how you engaged with them, what you asked them and what information was gathered.*

The following stakeholders were consulted in undertaking this PIA:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stakeholder** | **Internal/External** | **Scope of consultation** | **Method** | **Results** |
| *Name of stakeholders or group of stakeholders* | *Are the stakeholders internal to the agency or external?* | *What did you ask the stakeholder?* | *How did you engage with the stakeholders? For example, meeting, email, etc.* | *What input did the stakeholder provide?* |
|  |  |  |  |  |
|  |  |  |  |  |

1. **PIA outcomes**

*Complete this section after the Project Executive/Steering Committee/Senior Management has reviewed the proposed actions and strategies set out in section 5.*

*Agreed recommendations should also be integrated into a revised project plan to ensure that the activities necessary to implement the recommendations are managed.*

* 1. **Agreed recommended actions**

|  |  |  |
| --- | --- | --- |
| **#** | **Recommendation** | **Agreed Y/N** |
| 1 | *Copy the list of recommended actions from the table in section 4.* | *Document whether the recommendation was approved by the Project Executive/Steering Committee or senior management. If the recommended actions will not be implemented, record the rationale for this decision.* |

* 1. **Action plan**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Actions to be taken** | **Responsibility for action** | **Date for completion** |
| 1 | *List the agreed additional actions.* | *Record who will be responsible for implementing the agreed actions.* | *Record the planned date for completion.* |

* 1. **Contact point for future enquiries**

|  |  |  |  |
| --- | --- | --- | --- |
| Name: |  | | |
| Position: |  | | |
| Business unit: |  | | |
| Email: |  | Telephone: |  |
| File name/reference: |  | | |