**DRAFT**

[INSERT AGENCY LOGO]

**[Insert Agency Name]**

**[Insert Name of Project, e.g. “Proposed use of GovCMS for [Agency] website hosting”]**

Privacy Impact Assessment (PIA)
[Insert Date/ Version]

|  |
| --- |
| **Guidance Notes:** This PIA template has been prepared to assist your agency to complete a privacy impact assessment (**PIA**) in relation to you agency’s use of a website hosted on the GovCMS platform, if you are required to do so (see the requirements in the Memorandum of Understanding (**MOU**) between the Department of Finance (**Finance**) and your agency in respect of the provision of the GovCMS platform). **Note:** Before commencing a PIA you should first consider conducting a **PIA Threshold Assessment** to determine whether a PIA is in fact required:<https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment#overview> **This template has been designed for use only by agencies who are bound by the *Privacy Act 1988* (Cth) (Privacy Act). This template is not suitable for use by entities who are only subject to State and Territory privacy legislation.** **This template is designed to be a base, which will further considered and developed by you to reflect the particular privacy risks associated with how your agency will use its GovCMS website. Agencies may use all, some, or none of this template in preparing their PIA.**To assist you to complete this template, a number of guidance notes like this one have been included. However, we suggest that you seek advice from your privacy officer or legal team when completing your PIA. This template is designed to record outcomes from the following steps that need to be undertaken to conduct a PIA in accordance with Office of the Australian Information Commissioner (OAIC) guidance:**Step 1 – Planning for the PIA**Before starting the PIA process, consider which stakeholders you need to consult in order to ensure that privacy issues are properly identified, addressed and communicated. Consider the timeframe for the PIA, and a broad assessment of the nature and stage of development of the project (generally, a more advanced stage of development with a greater privacy scope, will mean a more detailed PIA). **Step 2 – Project Description & Information Flows**  Describe the project and map the information flows. See **Part B – Project Description** **and Information Flows** of this template for guidance and helpful tips about completing this step. After undertaking this step, complete **Part B** of this template. **Step 3 – APP Compliance** Analyse the project against each of the APPs to determine if the project complies with the APPs, or if there are gaps. See **Part C – Compliance with the APPs** of this template for guidance and helpful tips about completing this step. After reviewing this material, complete **Part C** of this template.**Step 4 – Risks & Recommendations** See **Part A – Executive Summary** of this template for further guidance about completing this step. After undertaking this step, complete **Part A** of this template. **Useful links:*** [Office of the Australian Information Commissioner](https://www.oaic.gov.au/) (OAIC)
* [OAIC - Guide to undertaking privacy impact assessments](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/)
* [OAIC - Australian Privacy Principles guidelines](https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/)
* [Privacy Act 1988 (Cth)](https://www.legislation.gov.au/Series/C2004A03712)
* [Protective Security Policy Framework – Information Security](https://www.protectivesecurity.gov.au/information/Pages/default.aspx)
 |

Contents

[Part A Executive Summary 3](#_Toc54850565)

[1. Introduction 3](#_Toc54850566)

[2. This PIA process 3](#_Toc54850567)

[3. Summary of risks and recommendations 4](#_Toc54850568)

[Part B Project Description and Information Flows 6](#_Toc54850569)

[4. Overview of project 6](#_Toc54850570)

[5. Collection of Personal Information 7](#_Toc54850571)

[6. Use Of Information 10](#_Toc54850572)

[7. Storage and Maintenance of Information 11](#_Toc54850573)

[8. Disclosure of Information 13](#_Toc54850574)

[9. [Diagram of Information Flows/ Tables of Key Information types (Optional)] 13](#_Toc54850575)

[Part C Compliance with the APPs 14](#_Toc54850576)

[Part D Glossary 34](#_Toc54850577)

1. Executive Summary

|  |
| --- |
| **Guidance Note:** This Part A is optional. If you choose to include it, you should summarise the outcomes from the PIA process. It should be the **last** Part of this template completed (i.e. Parts B and C should be completed before writing this section). When completed, this Part A should:* contain a brief description of the project (including key information flows);
* describe the methodology that has been used to undertake this PIA;
* clearly identify any negative privacy impacts and risks (but also any positive impacts); and
* set out recommendations to avoid or mitigate any identified privacy impacts and risks.
 |

1. Introduction

|  |
| --- |
| **Guidance Note:** This section 1 should provide a ‘big picture’ description of your project. You may wish to include/adapt the following paragraphs.  |

* 1. [Agency] is responsible for [insert summary of relevant Agency functions and activities]. In order to effectively communicate with members of the public for these functions and activities, [Agency] requires an effective website which [insert details, e.g. allows members of the public (**Website Visitors**) to submit enquiries to Agency/request to be added to a mailing list operated by Agency etc].
	2. The Department of Finance (**Finance**) is responsible for administering the Whole of Australian Government (arrangements relating to the hosting and management of GovCMS. GovCMS is a Drupal-based web-hosting service that Commonwealth agencies and certain other entities (e.g. state government organisations, universities and local councils) can use to develop and then host their websites.
	3. [Agency] intends to use GovCMS in order to develop and operate its website, and [has entered/intends to enter] into a memorandum of understanding (**MOU**) with Finance to facilitate this.
	4. This Privacy Impact Assessment (**PIA**) considers whether [Agency’s] use of the GovCMS service will comply with the *Privacy Act 1988* (Cth) (**Privacy Act**), and in particular, the Australian Privacy Principles (**APPs**).
1. This PIA process

|  |
| --- |
| **Guidance Note:** This section 2 should provide an overview of how you have undertaken your PIA process. Include details of any stakeholders (internal or external) that have been consulted.  |

1. Summary of risks and recommendations

|  |
| --- |
| **Guidance Note:** Complete this section 3 once you have completed the other parts of the PIA.This section 3 should summarise the findings arising from the PIA process, including:* outcomes of the privacy impact analysis and compliance checks, including positive privacy impacts and privacy risks that have been identified, and strategies already in place to protect privacy;
* recommendations to avoid or mitigate the privacy risks identified, and the agency’s responses to the recommendations; and
* a description of any privacy risks that cannot be mitigated, the likely community response to these risks, and whether these risks are outweighed by the public benefit that will be delivered by the project.

You can use the compliance table below, which sets out a ‘traffic light’ system, to help you complete this section. After conducting your PIA and analysing your compliance with the APPs in Part C, you can use this table to indicate your agency’s level of compliance with each APP and the action required (if any) to ensure compliance. You can highlight the second column with the corresponding, green, yellow, or red fill to indicate your agency’s level of compliance. When you have finalised the draft PIA, you should also include, in the column labelled ‘Action Required’, your agency’s response to any recommendations (i.e. whether you agency will implement the relevant recommendation). You can then proceed to finalise the PIA. |

|  |  |  |
| --- | --- | --- |
| **APP** | **Complies/Partially Complies/Does not comply** | **Action(s) Required** |
| **1** | **Complies** | **N/A** |
| **2** | **Partially complies***(e.g. include short description of partial non-compliance and the risk it presents)* | *(e.g. explain your recommendation and how it will fix partial non-compliance – if it will not fix the non-compliance, describe the likely community response to the relevant risk/s, and whether this risk/s is outweighed by the public benefit that will be delivered by the project)* |
| **3** | **Does not comply***(e.g. include a short description of non–compliance and the risk it presents)*  | *(e.g. explain your recommendation and how it will fix partial non-compliance – if it will not fix the non-compliance, describe the likely community response to the relevant risk/s, and whether this risk/s is outweighed by the public benefit that will be delivered by the project)* |
| **4** |  |  |
| **5** |  |  |
| **6** |  |  |
| **7** |  |  |
| **8** |  |  |
| **9** |  |  |
| **10** |  |  |
| **11** |  |  |
| **12** |  |  |
| **13** |  |  |

1. Project Description and Information Flows
2. Overview of project

|  |
| --- |
| **Guidance Note:** In this section, include a thorough description of the project. It should be written so that external stakeholders can understand it (i.e. without overly technical language). Include details about the:* overall aims of the project, and how it fits with your agency’s broader objectives;
* scope and extent of the project; and
* stage of development of the project.

You may wish to include/adapt the following paragraphs. |

* 1. In order to fulfil its functions and activities, [Agency] needs to effectively communicate with members of the public. In particular, [Agency] needs to have an effective website to allow:
		1. [insert general summary of what your website will do, e.g. allow members of the public (**Website Visitors**) to submit enquiries to Agency/request to be added to a mailing list operated by Agency etc
	2. [Agency] wishes to use the whole of government arrangements relating to the hosting and management of websites, known as GovCMS, to establish and then host its website.
	3. GovCMS is a Drupal-based web-hosting service that Commonwealth agencies and certain other entities can use to develop and then host their websites. GovCMS is administered by the Department of Finance (**Finance**).
	4. [Agency] will use its website to:

[insert as applicable, for example]

* + 1. collect information from and about natural persons who visit their website (**Website Visitors**). This information will include:
			1. personal information which is actively inputted by the Website Visitor into Agency’s online forms;
			2. other information which is actively inputted by the Website Visitor into Agency’s online forms;
			3. other information about the Website Visitor or their ICT equipment where the Website Visitor does not actively input that information (e.g. through the use of cookies or other analytics tools); and
		2. display other information, which may include personal information, in material that [Agency] places on its website hosted on GovCMS (e.g. contact information about its personnel) (**Website Information**).
	1. GovCMS is provided by Finance (through its third party contractors) on a cloud platform which is hosted by Amazon Web Services (**AWS**) in multiple available zones in the Asia Pacific (Sydney) region. Finance has entered into a Head Agreement with Salsa Digital (**Salsa**) for the provision of GovCMS, noting that Drupal enables Finance to customise the platform and streamline processes, administration and logging functionality[[1]](#footnote-1). Salsa has subcontracted some of the services under the Head Agreement to amazee.io (**Amazee**) and VHSN (**Vision**). Amazee is responsible for the management of the GovCMS Lagoon (a bespoke collection of tools including the GovCMS Dashboard, Lagoon UI for website management and the GitLab code repository) and the OpenShift (Kubernetes) Platform. Vision assists Amazee to manage the infrastructure layers.
	2. GovCMS is accredited to UNCLASS=DLM / Official: Sensitive.
	3. [Agency] has decided to use GovCMS as a [insert as applicable Software as a Service (**SaaS**), or Platform as a Service (**PaaS**) solution]. In accordance with the GovCMS arrangements, [insert as applicable, depending on the relevant solution: the PaaS solution will allow [Agency] to run and customise its own Drupal codebase and manage its relevant governance arrangements through GovCMS Lagoon. / the SaaS solution means [Agency’s] website will have infrastructure and application support provided by Salsa, while [Agency] will maintain the content, look and feel of its website].
	4. GovCMS is structured so that [Agency] will have a separate database for storage of information in connection with its website hosted on GovCMS (if [Agency] has more than one website, it will have separate databases in the GovCMS infrastructure). The website will have multiple non-production environments that may contain clones of the production database. [Agency’s] authorised users and developers will be able to download backups of databases, including production databases.
	5. [Agency] has, or will, enter into a Memorandum of Understanding for the provision of GovCMS Services (**MOU**) with Finance.
1. Collection of Personal Information

**What Information Will Be Collected?**

|  |
| --- |
| **Guidance Note:** In this section, set out exactly what types of information you will collect through the GovCMS website. Consider whether each type of information is:***Personal information***, which is defined in the Privacy Act as:*“personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:**(a) whether the information or opinion is true or not; and**(b) whether the information or opinion is recorded in a material form or not.”****Sensitive information***, which is defined in the Privacy Act as:*“sensitive information means:**(a) information or an opinion about an individual’s:**(i) racial or ethnic origin; or**(ii) political opinions; or**(iii) membership of a political association; or**(iv) religious beliefs or affiliations; or**(v) philosophical beliefs; or*(vi) *membership of a professional or trade association; or**(vii) membership of a trade union; or**(viii) sexual orientation or practices; or**(ix) criminal record;**that is also personal information; or**(b) health information about an individual; or**(c) genetic information about an individual that is not otherwise health information; or**(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or**(e) biometric templates.”****Health information***, which is defined in the Privacy Act as:*“(a) information or an opinion about:**(i) the health, including an illness, disability or injury, (at any time) of an individual; or**(ii) an individual’s expressed wishes about the future provision of health services to the individual; or**(iii) a health service provided, or to be provided, to an individual;**that is also personal information;**(b) other personal information collected to provide, or in providing, a health service to an individual;**(c) other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances;**(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.”*Record whether individuals can choose not to provide some or all of the information, and whether the information can be provided in an anonymous fashion, and any consequences for the individual if they do so.Record whether all information collected is solicited by your agency, or whether any unsolicited information may be collected. **Tips**This PIA only needs to consider personal information (including any personal information which is also sensitive information or health information). Carefully check each type of information against the definitions in the Privacy Act.Information that has been properly de-identified will not, by itself, be personal information. However, even if information does not contain a person’s name or has had ‘direct identifiers’ such as name and address removed, this does not necessarily mean that the information is de-identified and therefore not personal information. This is because in certain circumstances de-identified information might still fall within the definition of personal information because the individual can still be reasonably identified (e.g. through combining that information with other available information, including where a process of re-identification is possible and reasonably likely).You may like to use/adapt the following paragraphs. |

* 1. Information will be collected from Website Visitors when they visit [Agency’s] website hosted on GovCMS. Some information will be collected through an action by the Website Visitor, including if they fill in a form on the website, whilst other information may be collected passively, such as the Google Analytics information mentioned above.
	2. Some, but not all, of this information will be ‘personal information’ as defined in the Privacy Act, being information about an individual whose identity is apparent or can reasonably be ascertained from that information.
	3. [Agency] intends that the following information will be collected through its website:
		1. [insert details, consider including at the end of each item whether it is ‘(personal information, but not sensitive information’) (‘personal information which is sensitive information’), ‘(not personal information)’.]
	4. [insert if applicable: Some personal information may be collected from Website Visitors about individuals other than themselves (e.g. a Website Visitor may complete a form on behalf of another individual (including as a parent, guardian, trustee or other legal representative), or as a result of a reporting or other requirement to provide information about other individuals).]
	5. [insert if applicable: [Agency] also intends that the following additional personal information will be displayed on its website, noting that this personal information will have been previous collected from the relevant individuals:
		1. [insert details, e.g. contact names and details of staff members]

### **Why Will the Information Be Collected?**

|  |
| --- |
| **Guidance Note:** In thissection, describe:* The primary purpose of the collection, and why the collection is necessary for the purposes of the project. Check that the collection relates to your agency’s functions or activities.
* Who collects the information.
* Who the information has been or will be collected from.

**Tips** Consider and record whether your agency or the project actually collects the information from the individual, or whether collection will be undertaken by a third party (e.g. a contracted service provider, or another Commonwealth agency). * Consider and record whether there are multiple methods of collection (e.g. submission of a form, automated collection, collection by phone, collection through a app etc).
* Consider and record whether the information is always collected from the individual concerned, or from another source.
* Consider whether the identity of the individual providing the information is confirmed at any stage.
* Consider and record whether any individuals from whom information is collected might need additional support to understand how and why their information has been collected and will be used.
 |

### **What will individuals be told at the point of collection?**

|  |
| --- |
| **Guidance Note:** In thissection, describe what individuals will be told at the time of collection about the collection, use and disclosure of their personal information (e.g. does your Agency have a proposed form of words that will be included on your website)? |

* 1.
1. Use Of Information

### **How Will The Information Be Used?**

|  |
| --- |
| **Guidance Note:** In thissection, describe all current or planned uses by your agency of the information which is or will be collected, and how these relate to the purposes of collection.**Tips** It does not matter if your agency only uses, or intends to use, the information on an infrequent or ad hoc basis – these uses still need to be considered in the PIA.* If your agency will use the information collected for the purposes of data linking or matching (i.e. aggregating different datasets together), you will need to identify and describe exactly how this will be done, and the protections and safeguards that will be in place.
 |

* 1. Visitor Information collected through the website will used by [Agency] as follows :
		1. [insert details]
1. Storage and Maintenance of Information

### **How Will The Information Be Stored?**

|  |
| --- |
| **Guidance Notes:** In thissection, describe how and where the information will be stored and protected. Describe how this meets your agency’s ICT and physical security measures. Please see Part C in relation to APP 11 for an overview of the security measures that have been implemented in respect of the GovCMS platform. You should include an overview of these measures here. **Tips** Particularly consider the arrangements with any third party providers involved in storage of, or support services for, the information. * Particularly investigate the arrangements for any cloud-based storage (e.g. is there a contractual obligation requiring on-shore storage? Is access to the information by off-shore personnel restricted?)
* Consider all access to the stored information, and how that access will be authorised or restricted.

You may wish to include/adapt the paragraphs below. |

* 1. [Insert as applicable: [Agency] will not store Visitor Information on its GovCMS database in any enduring form. Instead it will be transferred via email to [Agency] and then automatically deleted from [Agency’s] database. / [Agency] intends to store Visitor Information on its GovCMS database.
	2. An IRAP assessment has been undertaken in respect of GovCMS, and as a result GovCMS is now certified to UNCLASS=DLM / Official: Sensitive. As part of this extensive assessment, penetration testing of GovCMS occurred in 2019.
	3. In addition, Finance’s GovCMS System Security Plan (SSP) sets out the operational security controls relevant to GovCMS, noting that the SSP assesses GovCMS against the Information Security Manual (ISM). This assessment represents a minimum best practice security baseline for all WoAG systems managed by Finance’s Online Services Branch (OSB).
	4. A number of key security features have been implemented in respect of GovCMS, including:
		1. the application of whitelisting;
		2. administrator access to GovCMS being restricted to Finance and Salsa personnel;
		3. active patching testing of all modules in the GovCMS distribution;
		4. testing of the integrity of [Agency’s] website, including:
			1. onboarding all production websites; and
			2. undertaking continuous audit checks of such websites, in particular to identify any escalated account privileges;
		5. data being encrypted at rest (at AES-256 bits);
		6. SHA256 bit SSL certificates for [Agency’s] website;
		7. the application of ISM-compliant passphrase policies, to enforce complexity rules and system assurance; and
		8. regular threat monitoring and perimeter monitoring.
	5. All data storage for GovCMS is located in Australia, but some support services provided by Salsa may be provided by overseas parties.

### **How Will the Information Be Accessed and Maintained?**

|  |
| --- |
| **Guidance Notes:** In thissection, describe:Whether individuals can or will be able to access and/or correct their information (or have annotations made to it?)The processes that ensure, or will ensure, the information is relevant, up-to-date and complete.When and how the information is or will be de-identified or destroyed (including any information retention policies or destruction schedules in place).What action will be taken if a data breach was to occur?Whether the Agency’s ICT service providers (e.g. Finance and Salsa) will be able to access personal information when providing Services and to what extent they will be able to access it (noting that although Finance and Salsa personnel will technically be able to access all information in GovCMS, such personnel are only permitted to access the information in the specific circumstances set out in the MoU (being circumstances in which an ICT service needs to provide services)). You may wish to include/adapt the paragraphs below. |

* 1. [Agency] will be responsible for the management of user accounts for its personnel and contractors requiring access to GovCMS or its personnel.
	2. [Agency] personnel with access to GovCMS [insert as applicable: have a minimum baseline security clearance / are bound by internal terms of use that require them to act in a responsible, accountable and security conscious manner].
	3. While Finance (and Salsa) personnel will technically have access to GovCMS for the purposes of providing services to [Agency] in connection with GovCMS, that access will be governed by the strict requirements in the MOU (and in the case of Salsa, by the Head Agreement) which are designed to ensure that [Agency] has effective control over its information in GovCMS at all times.
1. Disclosure of Information

### **How Will The Information Be Disclosed?**

|  |
| --- |
| **Guidance Notes:** In this section, describe all current or planned disclosure of the information collected. Explain:To whom the information is or will be disclosed?Why the information is or will be disclosed?What information is or will be disclosed? How the information is or will be disclosed (e.g. in a de-identified form)?Whether the individual was or will be told about (or consented to) the disclosure, and whether they were or will be given any choices about the disclosure.Confirm that personal information will not be disclosed to Finance or any of its subcontractors and outline the ways in which Finance is taking appropriate steps to ensure that Salsa and its subcontractors are meeting their privacy and security obligations.**Tips** * Consider whether your agency may disclose the information to an overseas recipient (remember that service providers, include cloud service or ICT support service providers, or their platforms, may be located overseas).
* In some circumstances, storage in a cloud service may be considered “use” of the information by your agency, rather than a “disclosure” to the cloud services provider.
 |

* 1. [Agency] will be disclose Visitor Information to the following entities, for the following reasons:
		1. [insert details]
	2. [Agency] may disclose Visitor Information to its contracted service providers, if they need to access [Agency’s] database in GovCMS in order to fulfil their contractual obligations, including:
		1. [insert details]
	3. [Agency] will disclose Website Information to anyone accessing [Agency]’s website.
	4. Finance may, in its role as a service provider of GovCMS, collect and use Google Analytics data from Website Visitors, noting that this data is not Visitor Information (i.e. it is not personal information).
1. [Diagram of Information Flows/ Tables of Key Information types (Optional)]

|  |
| --- |
| **Guidance Notes:** This is an optional section. Sometimes it is useful to include a diagrammatical depiction of the flow of information, showing how information flows into your agency, how it is used, and to whom it is disclosed. Sometimes it can also be useful to include tables which set out the key information for different types of personal information involved in the project. If desired, include appropriate diagrams or tables here. Otherwise simply delete this section. |

1. Compliance with the APPs

The table below sets out an analysis of the key elements of the APPs that are relevant to the project. The analysis does not address those elements of the APPs that reflect [Agency’s] broader compliance obligations, but only considers those elements that specifically relate to the project.

|  |
| --- |
| **Guidance Note:** The table in this section is designed to help you assess whether your project complies with each of the APPs. Some guidance questions (and some suggested paragraphs that you could include/adapt if desired) are provided within the table. You should document and provide specific details about either, how your use of the GovCMS website will comply with the APP or, why you are not required to comply with a specific APP, and any considerations you took into account to come to that conclusion. The questions are not exhaustive and are provided as a guide only. You should think about potential privacy risks even when not explicitly prompted in the table and note any identified risks and potential mitigation strategies. You should also refer to the OAIC’s [APP Guidelines](https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/), which provide a comprehensive guide to interpreting and applying the APPs. You may need to consider other issues, including other legislation and rules that apply to your entity (such as secrecy provisions) or, considering the nature of your project. It is also important to note that, even if the project appears to be compliant with privacy legislation, there may still be other privacy risks that need to be addressed, such as community expectations. As you go through your compliance check, you should consider the privacy risks and, where possible, come up with alternatives to avoid or mitigate those risks. This will help to inform any recommendations you make to address the risks and ensure that they have been identified in the PIA process. |

| APP | Overview of APP | Compliance with APP | Gap Analysis & Recommendations  |
| --- | --- | --- | --- |
| 1  | APP 1 provides that APP entities must have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. |

|  |
| --- |
| ***Guidance Note:****Om this section, consider whether your agency has taken reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code for the purposes of the project.**See the OAIC’s* [*Privacy Management Framework*](https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice/) *for the steps the OAIC expects you to take to meet your obligations under APP 1.2. Agencies should also consider their obligations under the Privacy (Australian Government Agencies – Governance) APP Code 2017. Consider whether any adjustments or additions need to be made to your practices, procedures and systems for the purposes of this project.* |

 [Insert description of your agency’s compliance with APP 1]***APP 1.4 – Privacy Policy***

|  |
| --- |
| The MOU with Finance requires [Agency] to include on their GovCMS hosted website a link to a privacy policy that is compliant with APP 1. ***Guidance Note:****Does your agency have a privacy policy which:** *is clearly expressed, understandable and up-to-date;*
* *covers the matters listed in APP 1.4; and*
* *is freely available at no cost (for example, on your website.*

*Identify the document(s) and provide a link where available or include as an attachment to this PIA. See the OAICs* [*Guide to developing an APP privacy policy*](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-developing-an-app-privacy-policy/) *for more information.**Will the APP privacy policy need to be updated to reflect a new collection, use or disclosure of personal information for the purposes of this project?* |

The website will display the [Agency] has a privacy policy which is available at [insert link]. This privacy policy [does/does not] contain all information required by APP 1.4 in relation to the Visitor Information which will be collected through the website.. The privacy policy specifically references ICT contractors who may access Visitor Information for the purposes of providing services to [Agency]. The [privacy policy/other information on the website] will also reference Finance, in its role as a service provider of GovCMS, collecting and using Google Analytics data. |

|  |
| --- |
| ***Guidance Note:****In this column you should describe any gaps in your agency’s compliance with the relevant APP and also include any recommendations that may, if implemented, mitigate the risk.**If there is no recommendation that can fix the non-compliance, describe the likely community response to the relevant risk/s, and whether this risk/s is outweighed by the public benefit that will be delivered by the project.*  |

 |
| 2 | APP 2 provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter, subject to particular exceptions.  |

|  |
| --- |
| ***Guidance Note:****In this section, describe:****APP 2.1**** *how individuals will be provided with the option of not identifying themselves or of using a pseudonym.*

***APP 2.2**** *Alternatively, explain why it is impracticable for you to deal with individuals who have not identified themselves (for example, if you need to deliver purchased goods to an individual, you may need to know their name if the individual needs to sign for delivery). See Chapter 2 of the APP Guidelines for more information about when it may be impracticable to deal with an individual who is not identified.*
* *Otherwise, consider whether you are otherwise required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves.*
 |

[Insert description of your agency’s compliance with APP 2] |  |
| 3 | APP 3 provides that any personal information collected (other than sensitive information) must be reasonably necessary for (or if your entity is an agency, reasonably necessary for, or directly related to) one or more of the entity’s functions or activities.An APP entity must not collect sensitive information about an individual unless one of the exceptions listed in APP 3.3 or APP 3.4 applies.Personal information can only be collected by lawful and fair means.Personal information about an individual must only be collected from the individual unless one of the exceptions in APP 3.6 applies. |

|  |
| --- |
| ***Guidance Note:****In considering your agency’s compliance with APP 3, you will need to describe:* ***APP 3.1*** * *the information being collected necessary for, or directly related to, one or more of your functions or activities?*
* *and list each item of personal information that will be collected (e.g. name, date of birth, address) and explain why each item is necessary for one or more of your functions or activities. This should be a very granular assessment. You should clearly and specifically describe the relevant function or activity and why each item of personal information is directly related to that specific function or activity. You should only collect the minimum amount of personal information that is necessary for the relevant function or activity (‘data minimisation’).*

*Data minimisation is an important concept that can help reduce the privacy impacts for individuals that may be associated with your project. Minimising the amount of data that you collect can also help to mitigate security risks. For example, collecting more personal information than is necessary may increase the risk of harm to an individual in the event of a data breach, which could also trigger your notification obligations under the Notifiable Data Breach scheme. Holding large amounts of personal information may also increase the risk of unauthorised access by internal or external sources. Security issues are considered further below under APP 11.* *Also consider whether your APP privacy policy will need to be updated if the project will involve a new collection of personal information and record this under APP 1 above.* ***Privacy risk:*** *If some personal information is not reasonably necessary for the project, there may be a risk of over collection. For example, it may be not be necessary to collect all personal information on an individual’s driver licence when the purpose of collection is to verify the individual’s age.****APP 3.2*** *For the collection of sensitive information, can you rely on any of the exceptions in APP 3.3 or APP 3.4?**Explain which exception you are relying on for the collection of any sensitive information. For example, has the individual consented or is the collection required or authorised by or under an Australian law or a court/tribunal order?* ***APP 3.5*** *Will the information be collected by lawful and fair means?**Describe the means by which personal information will be collected.* ***Privacy risk****: Your method of collection may be ‘unfair’ if it involves intimidation, deception or is unreasonably intrusive. For example, it would usually be unfair to collect personal information covertly without the knowledge of the individual (however, this will depend on the circumstances).* |

|  |
| --- |
| ***APP 3.6*** *Will the personal information be collected from the individual concerned? If not, do any of the exceptions in APP 3.6 apply*?*Describe how, and from which other sources, the personal information will be collected. Also, explain which exception you are relying on to collect personal information about the individual from another source.****Privacy risk****: There may be a risk of the information being inaccurate, out-of-date or incomplete if collected from another source.**If the collection of personal information will be outsourced, will measures be in place to ensure compliance with APP 3and prevent over collection of information?**Describe how you will ensure that any third party that collects personal information on your behalf complies with APP 3 (for example, by entering an enforceable contractual arrangement).* |

[Insert description of your agency’s compliance with APP 3] |  |
| 4 | APP 4 provides that where an APP entity receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information. If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the APP entity must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so. |

|  |
| --- |
| ***Guidance Note:****If your website will not allow collection of any unsolicited personal information (all information collected through the website will be provided in response to a particular field requested or required by your agency), APP 4 is unlikely to be relevant.*  |

[Insert description of your agency’s compliance with APP 4] |  |
| 5 | APP 5 provides that an APP entity that collects personal information about an individual must take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of the matters listed in APP 5.2.An APP entity must provide notification before, or at the time it collects personal information. If this is not practicable, notification should be provided as soon as practicable after collection. |

|  |
| --- |
| ***Guidance Note:****In considering your agency’s compliance with APP 5, you will need to describe:****APP 5.2**** *each of the matters listed in APP 5.2. Will steps be taken to notify the individual of each matter? If steps are not being taken in relation to a matter, is it reasonable not to notify the individual?*
* *the steps taken to notify the individual OR explain why steps are not being taken. Include a link or attach collection notices where appropriate.*
* *If personal information is collected from another source, will the individual be notified? What steps will be taken to notify of each of the APP 5.2 matters?*
* *the steps taken to notify the individual OR explain why steps are not being taken. Include a link or attach collection notices where appropriate.*

 ***Privacy risk****: If you are collecting personal information from another source, there may be a risk that an individual is not aware that you have collected their personal information. Ensure that any third-party notifies, or makes an individual aware, of the relevant APP 5 matters on your behalf (such as through an enforceable contractual arrangement).* |

The MOU with Finance expressly requires [Agency] to provide Website Visitors with information (including in the form of a collection notice that meets APP 5 requirements if applicable) that: contains all matters required by APP 5.2; and which clearly states that Finance (and its contracted service providers, which will include Salsa) may access Visitor Information for the purposes of providing services to [Agency], and that Finance may collect Google Analytics information. [Agency’s] website [will/will not] contain such a notice.[Insert other description of your agency’s compliance with APP 5] |  |
| 6 | APP 6 provides that an APP entity can only use or disclose personal information for the particular purpose for which it was collected (known as the ‘primary purpose’), or for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure of the information.Note that APP 6 does not apply to organisations using or disclosing personal information for the purpose of direct marketing (refer to APP 7), or government related identifiers (refer to APP 9). |

|  |
| --- |
| ***Guidance Note:****In considering your agency’s compliance with APP 6, you will need to describe whether:****APP 6.1*** * *your agency will only use and disclose personal information collected through, or displayed on, its website for the primary purpose of its collection?*
* *your agency will use or disclose that personal information (including sensitive information) for any secondary or additional purpose?*

***APP 6.2**** *the secondary purpose and explain how it is authorised, by either asking the individual to consent, or by applying one of the exceptions to the requirement for consent in APP 6.2. Also consider whether your APP privacy policy will need to be updated if the project will involve a new use or disclosure of personal information and record this above under APP 1.*

*If you are an agency, is it possible that personal information may be used or disclosed because it is reasonably necessary for an enforcement related activity? If so, are procedures in place to ensure a written note of the use or disclosure is made in compliance with APP 6.5?**Will the individual be notified of any additional use(s) or disclosure of their personal information?**Explain how the individual will be given notice of the secondary use(s) or disclosure of their information, or why notice is not required (e.g. additional notice may not be required if the proposed use or disclosure is consistent with the notice originally provided at the point of collection).* ***Privacy risk****: If relying on APP 6.2(a) to use or disclose personal information for a secondary purpose, but your project involves a new way of handling personal information, there may be a risk that individuals would not reasonably expect their personal information to be used for the new purpose. Carefully consider whether additional notification is required.**If you’re disclosing personal information to another entity (e.g. if you are outsourcing some of your functions, or as part of an ongoing data sharing arrangement), will measures be put in place to protect the information and will compliance with APP 6 be monitored?**Describe the measures (such as an enforceable contractual arrangement or other information sharing agreement) that will be put in place to ensure compliance with APP 6 and protect the personal information that is being disclosed/shared. If no measures will be put in place, explain why (for example, the disclosure is a once-off and permitted by one of the exceptions under APP 6).* |

[Insert description of your agency’s compliance with APP 6]Finance has ensured that Salsa (and its subcontractors, including Amazee and Vision) are bound by contractual arrangements that include appropriate privacy and security protections, which require use only for the performance of the required contractual obligations. Additionally, Finance will ensure that compliance with those arrangements is monitored, with appropriate further steps taken if required. |  |
| 7 | APP 7 provides that an organisation must not use or disclose personal information for the purpose of direct marketing unless an exception applies, such as where the individual has consented. APP 7 may also apply to an agency in the circumstances set out in s 7A of the Privacy Act. |

|  |
| --- |
| **Guidance Note:** *The majority of agencies will not be bound by APP 7. However, if your agency is one that can be considered an ‘organisation’ for the purposes of the Privacy Act, you should seek advice.*  |

 |  |
| 8 | APP 8 provides that before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information, unless an exception applies, such as the individual has given informed consent.An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (see s 16C of the Privacy Act). |

|  |
| --- |
| ***Guidance Note:****In considering your agency’s compliance with APP 8, you will need to describe:** *what information will be transferred, to whom the information will be transferred, in which jurisdiction the information will be stored, and how the information will be transferred.*

***APP 8.1*** * *whether reasonable steps have been taken under APP 8.1 to ensure the overseas recipient does not breach the APPs (other than APP 1) in relation to the information?*
* *the arrangements in place with overseas recipients to ensure that personal information is handled in accordance with the APPs. For example, provide details of any enforceable contractual arrangement.*

***APP 8.2*** * *Alternatively, whether an exception under APP 8.2 will apply?*
* *How one of the exceptions in APP 8.2 apply to the transfer. For example, is the disclosure required or authorised by or under an Australian law or a court/tribunal order?*
 |

Insert description of your agency’s compliance with APP 8]All information collected through GovCMS is stored on infrastructure located in Australia.[Agency] notes the contractual protections in the agreements between Salsa and Finance in which Salsa agrees ‘not to use or disclose Personal Information, or engage in an act or practice that would breach an Australian Privacy Principle or an APP Code, unless….it carries out and discharge [sic] the obligations contained in the Australian Privacy Principles as if it were an Agency (including Finance) under the Privacy Act’. Additionally, clause 17.4 of the Head Agreement provides: ‘[Salsa] must ensure that all Subcontracts entered into for the purposes of fulfilling its obligations under a Contract contain provisions to ensure that each Subcontractor has the same awareness and obligations as the Contract has under this clause 17, including the requirement in relation to Subcontracts.’The Head Agreement requires Salsa’s contractual arrangements with overseas recipients (e.g. its support service providers) to include appropriate contractual mechanisms that require adherence to the APPs.  |  |
| 9 | APP 9 provides that an organisation must not adopt, use or disclose a government related identifier of an individual as its own identifier of the individual unless an exception applies. APP 9 does not apply to the handling of government related identifiers by agencies. However, agencies should still give careful consideration to any proposed creation, adoption, use or disclosure of government related identifiers and the potential privacy impacts this may have, including community expectations around how government should handle these identifiers. |

|  |
| --- |
| ***Guidance Note:****Most agencies will not be bound by APP 9. However, if your agency is one that can be considered an ‘organisation’ for the purposes of the Privacy Act, you should seek advice.* |

[Insert description of your agency’s compliance with APP 9] |  |
| 10 | APP 10 provides that an APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.An APP entity must take reasonable steps to ensure that the personal information it uses and discloses is, having regard to the purpose of the use or disclosure, accurate, up to date and complete. |

|  |
| --- |
| ***Guidance Note:****In considering your agency’s compliance with APP 10, you will need to describe:** *What steps will you take to ensure the personal information collected is accurate, up to date and complete? Will guidance or processes be in place to ensure these steps are followed?*
* *What steps will be taken to ensure that any personal information being used or disclosed is accurate, current, complete and relevant, having regard to the purpose of the use or disclosure? Will guidance or processes be in place to ensure these steps are followed?*

 ***Privacy risk****: Carefully consider the consequences for individuals if the personal information is not accurate or up‑to-date, including the kinds of decisions made using the information and the risks of using or disclosing inaccurate information.* |

[Insert description of your agency’s compliance with APP 10] |  |
| 11 | APP 11 provides that an APP entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.  |

|  |
| --- |
| ***Guidance Note:****In considering your agency’s compliance with APP 11, you will need to describe:** *the processes your agency has put in place to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure;*
* *whether, in your opinion, these steps are reasonable in the circumstances; and*
* *the technical controls (such as software security, encryption, whitelisting and blacklisting, backing up, email security etc) that have been, or will be, implemented for the project, including any relevant policies and procedures. Include links or attachments where appropriate.*

 ***Privacy risk:*** *If there are inadequate technical security measures in place, consider whether there is a risk that the information will not be properly protected, leading to misuse, interference, loss, unauthorised access, modification or disclosure. Consider the nature of the personal information collected and how valuable it would be to unauthorised users? Include a recommendation to address any such risks, as appropriate.* ***Physical security measures*** *You should describe the physical security measures that have been, or will be implemented, for the project, including any relevant policies and procedures. Include links or attachments where appropriate.**For example, are there access security and monitoring controls in place to protect against internal and external risks and ensure that personal information is only accessed by authorised persons?**You should describe the access security controls (such as identity management and authentication, password practices, audit logs/trails and access monitoring) that have been, or will be, implemented for the project, including any policies and procedures. Consider who will have access to the data and ensure access is limited to those staff (or other third parties) necessary to enable your entity to carry out its functions and activities (i.e. access should be strictly on a ‘need-to-know’ basis). Include links or attachments where appropriate.*  ***Privacy risk:*** *Inadequate access security and monitoring controls may lead to the ‘trusted insider risk’, which can occur when staff mishandle personal information while carrying out their normal duties.**If you have completed a security assessment, you should refer to the assessment or attach a copy to the PIA. .**Do you have a data breach response plan in place? If so, describe at a high level the steps that you will take in the event of a data breach or attach your response plan.**See the OAIC’s* [*Notifiable data breaches*](https://www.oaic.gov.au/privacy/notifiable-data-breaches/) *page which sets out information to help APP entities prepare for and respond to data breaches. You should consider whether changes to your existing data breach response plan need to be made as a result of this project.**If you have outsourced personal information handling as part of this project, have you considered your obligations under the Notifiable Data Breaches (NDB) scheme and how you will manage your relationship with the third party?**Describe how you will ensure you comply with the NDB scheme in the event a third-party provider experiences a data breach (such as including contractual terms to allocate responsibility for identifying, assessing and notifying as required).**How long will you retain the personal information collected, used and/or disclosed as part of this project?**Describe any relevant retention and disposal schedules or policies.**Will personal information be destroyed or de-identified once it is no longer needed for any authorised purpose? Do any of the exceptions apply (for example, the information is part of a Commonwealth record or the APP entity is required by law or a court/tribunal order to retain the information)?**Explain whether an exception applies that requires you to retain the information.**If applicable, how will personal information be destroyed once it is no longer required?**Describe the method of destruction and explain how that method is secure.* ***Privacy risk:*** *There is a risk of unauthorised disclosure if personal information is not securely and irretrievably destroyed.**If applicable, how will personal information be de-identified once it is no longer required?**Describe the method of de-identification that will be used and whether the de-identified information will be used for any other purpose. See the OAIC’s* [*De-identification and the Privacy Act*](https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/) *for further information.* ***Privacy risk:*** *If de-identifying personal information once it is no longer required, consider whether there is a risk that the information can be re-identified.**If you have outsourced personal information handling as part of this project, what will happen to information held by third party providers?**Describe any arrangements (for example, any contractual provisions) in relation to third parties’ obligations to retain and dispose of personal information.* ***Privacy risk:*** *If there are no arrangements in place relating to third parties’ retention and disposal of personal information, there is a risk that personal information could be used by the third party for unsauthorised purposes at the conclusion of the contract.* |

[Insert description of your agency’s compliance with APP 11]The GovCMS solution has the security features and protections as outlined in Part B of this PIA.In addition, the contractual arrangements with Salsa provide that it must:* + comply with Agency’s security requirements, including ensure that all personnel hold the necessary level of security or access clearance; and having and maintaining security checks, clearances or accreditations as required by Agency;
	+ comply with all relevant security procedures or requirements, including as applicable, the PSPF, the Protective Security Manual, the ISM and the Defence Security Manual, and any other security requirements notified by Finance or Agency from time to time;
	+ remove any personnel who have failed to obtain, or ceased to hold, the required level of security or access clearance;
	+ not, unless prior consent has been given by Agency remove Agency data or allow Agency data to be removed from Agency or its contractor’s premises, or taken or transmitted by any means outside of Australia;
	+ notify Agency immediately of any contravention of the Agency’s data security requirements, and to comply with all directions given by Finance and Agency in respect of the contravention
	+ comply with all requirements specified in Agency’s contract in relation to the protection of data or materials, including any anti-virus and firewall requirements (their installation, operation and maintenance) and data back-up obligations;
	+ not, and not permit its personnel or any third party under its direction or control to, negligently or wilfully introduce any ‘Harmful Code’ (noting that there are particular actions that Salsa must take if any Harmful Code is introduced, regardless of where the fault lies)
	+ protect all material and information in respect of which Salsa has custody or control, or which is accessed, transmitted or stored using, or on, Salsa’s information systems or equipment under a Contract, noting that Salsa must ensure that:
	+ the material and information is protected at all times from unauthorised access or use by a third party, and from misuse, damage or destruction; and
	+ there are appropriate protective measures in place, including but not limited to administrative, physical and technical safeguards that are no less rigorous than accepted industry standards and commensurate with the consequences of, and probability of unauthorised access to, or use, misuse or loss of, such information;
	+ ensure that Finance and Agency are advised of any unauthorised remote access to Finance’s or Agency systems and ensure that remote access is strictly limited to access:
	+ approved by Finance or the Agency; and
	+ in accordance with the Head Agreement, and the Agency contract;
	+ ensure that Finance and Agency are advised of any unauthorised remote access to Finance's or Agency systems and ensure that remote access is strictly limited to access:
	+ approved by Finance or Agency; and
	+ in accordance with the Head Agreement, and Agency’s contract;
	+ ensure that if data is stored in, or transferred to, any location outside of Australia (including through the remote access or control of any server or other hardware or software), access is restricted to those personnel with the appropriate authorisations who have a need for such access, and that access is limited to the minimum access necessary to enable Salsa to comply with its obligation under any contract; and
	+ notify Agency, and when required, Finance, by telephone as soon as possible if it becomes aware of any security incident, noting that Salsa and its subcontractors must comply with all directions of Agency to resolve the incident.
 |  |
| 12 | APP 12 provides that an APP entity that holds personal information about an individual must give the individual access to that information on request unless an exception applies. |

|  |
| --- |
| ***Guidance Note:****In considering your agency’s compliance with APP 12, you will need to describe whether:** *there are any elements of the Project that could impede your agency’s ability to provide information to an individual upon request; and*
* *your agency otherwise has procedures in place to comply with APP 12.*

*If there is no element of the Project that will impede upon your agency’s ability to comply with APP 12, you should note this.**If there is an element of the Project that will impede upon your agency’s ability to comply with APP 12, you should consider whether:** *you can recommend changes to your Project to allow for compliance with APP 12; or*
* *whether any of the exceptions under APP 13 apply*
 |

|  |
| --- |
| ***Guidance Note:****If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow correction of personal information held by third parties.**Importantly, Finance and its contractors will not collect personal information collected via your agency’s website.*  |

[Insert description of your agency’s compliance with APP 12] |  |
| 13 | APP 13 requires an entity holding personal information to permit correction of that information, except in limited circumstances.  |

|  |
| --- |
| ***Guidance Note:****In considering your agency’s compliance with APP 13, you will need to describe whether:** *there are any elements of the Project that could impede your agency’s ability to correct an individual’s information upon request; and*
* *your agency otherwise has procedures in place to comply with APP 13.*

*If there is no element of the Project that will impede upon your agency’s ability to comply with APP 13, you should note this.**If there is an element of the Project that will impede upon your agency’s ability to comply with APP 13, you should consider whether:** *you can recommend changes to your Project to allow for compliance with APP 13; or*
* *whether any of the exceptions under APP 13 apply.*
 |

|  |
| --- |
| ***Guidance Note:****If engaging third parties such as contracted service providers, consider whether there are arrangements in place to allow correction of personal information held by third parties.**Importantly, Finance and its contractors will not collect personal information collected via your agency’s website.* |

[Insert description of your agency’s compliance with APP 13] |  |

1. Glossary

|  |
| --- |
| ***Guidance Note:****Complete the below glossary to assist the reader understand terms used in your PIA.* |

|  |
| --- |
| Definitions |
| APP, or Australian Privacy Principle | has the meaning given to it in the Privacy Act. |
| APP Code | means the *Privacy (Australian Government Agencies – Governance) APP Code 2017*.  |
| Eligible Data Breach | has the meaning given to that term in the Privacy Act.  |
| OAIC | means the Office of the Australian Information Commissioner.  |
| personal information | has the meaning given in section 6 of the Privacy Act.  |
| PIA | means this privacy impact assessment.  |
| Privacy Act | means the *Privacy Act 1988* (Cth). |
| sensitive information | has the meaning given in section 6 of the Privacy Act.  |

1. For completeness, there is no interaction between GovCMS and Finance’s other ICT infrastructure in connection with the hosting and management of GovCMS. [↑](#footnote-ref-1)