|  |
| --- |
|  |
| BUSINESS APPLICATION INFormATION MANAGemenT ASSESSMENT |

|  |
| --- |
| Introduction |
| **Purpose**: This tool is designed to identify whether a systems holds information that relate to high risk business processes, and/or are the official record of business.  Where this is identified to be the case the system must comply with the (PRACT 1973, Privacy and Data Protection Act 2014) requirements and will need to be approved as a digital information management system.  **Responsibility**: The system/business process owner needs to assess the system to identify whether there are information management requirements. If so, a further assessment of compliance will be required. Systems may need to be re-assessed on a regular basis to cater for changes in business processes and/or system use and functionality overtime. |

|  |
| --- |
| Instructions |
| **Step 1**: Complete this coversheet.  **Step 2**: Respond to the questions in the following sections. Users must accurately reflect the system’s use and records created and held within it.  **Step 3**: Review the results against the table in section 3 of this document. Section 3 will detail the required action based on your overall response to the questions in this assessment.  **Step 4:** A copy of the completed assessment is to be emailed ***XXXXXX***  Note: In completing and lodging this document, the system owner acknowledges that it is an accurate reflection of the system, and the business processes and records the system supports. |

|  |  |  |  |
| --- | --- | --- | --- |
| Summary of the System | | | |
| **NAME OF SYSTEM BEING ASSESSED** |  | Date: |
| **VERSION NUMBER OF SYSTEM** |  | |
| **SUMMARISE THE BUSINESS FUNCTION THE SYSTEM UNDERTAKES/SUPPORTS.** |  | |
| **BUSINESS PROCESS OWNER**  (I.E. WHO OWNS THE DATA?) | Contact: | Phone: |
| Position: | |
| Business Unit: | |
| **SYSTEM ADMINISTRATOR**  (I.E. WHO MANAGES THE SYSTEM) | Contact: | Phone ext. |
| Position: | |
| Business Unit : | |
| **DETAILS OF PERSON COMPLETING THE IDENTIFICATION TOOL** | Name: | Phone ext. |
| Position | |
| Business Unit: | |
| Date of assessment: | |

**CONTENTS**

[1 Identifying Business Applications Supporting High Risk Business Processes. 3](#_Toc458182884)

[2 Identifying Recordkeeping Considerations 5](#_Toc458182885)

[3. Identify Privacy Considerations 10](#_Toc458182886)

[4. Recordkeeping functionality requirements for Business Applications 26](#_Toc458182887)

[5 Metadata Requirements 29](#_Toc458182888)

[6. Metadata requirements - Additional requirements 39](#_Toc458182889)

[7. Infrastructure Management Considerations (On Premise and Cloud) 43](#_Toc458182890)

| **No.** | **Question** | **response** |
| --- | --- | --- |
| 1 **Identifying Business Applications Supporting High Risk Business Processes.** | | |
| The following criteria will identify whether this system supports high risk business processes.  Tick ALL the categories which apply to this system. | | |
| 1.1 | Does the system or the records contained within the system, support or impact on the following? |  |
| 1. Regular, routine or direct contact with individuals (for example, clients, govt, service providers etc) | Yes  No |
| 1. An individual’s rights, entitlements and wellbeing | Yes  No |
| 1. The creation of or determination of policy, rules, by-laws | Yes  No |
| 1. The making of legal agreements | Yes  No |
| 1. Significant investment by the agency | Yes  No |
| 1. An investigation by IBAC, Ombudsman or other watchdog agency where recordkeeping are identified for the process | Yes  No |
| 1. Processes that may be open to corruption or the potential of corrupt behaviour. | Yes  No |
| 1. A significant contribution to the economic and social development and management of VICTORIA either directly or indirectly; management of natural resources, security of the state and/or infrastructure of VICTORIA. | Yes  No |
| 1. A major program of international/national/state significance. | Yes  No |
| 1. Records that are included in the organisation’s vital records register. | Yes  No |
| 1. Significant records relating to Aboriginal people and heritage. | Yes  No |
| 1. Profiling in the media for matters that indicate possible recordkeeping failures. | Yes  No |
| 1. The production of State archives (Note: guidance on State archives can be obtained from the Records Management Unit). | Yes  No |
|  | Outcome: Is this business application high risk?  Is integration with the Electronic Document and Records Management System planned  If yes specify date  If no complete section 4. | Yes  No  Yes  No |
|  | Is the business applications low risk?  Have records management requirements been incorporated in business process documentation. | Yes  No  Yes  No |

| **No.** | **Guidance** | **Question** | **Response** | **Additional Details** | **actions** |
| --- | --- | --- | --- | --- | --- |
| 2 Identifying Recordkeeping Considerations | | | | | |
| The following criteria will identify whether this system creates and hold records supporting the agency’s business.  Tick ALL the categories which apply to this system. Where YES applies, please provide a summary to explain your response further. | | | | | |
| 2.1 | It is important to determine whether the system creates and /or holds information that proves that a particular activity happened and the details relating to it.  *The agency business* relates to any activity undertaken by an individual, team or group, business unit, Faculty/Unit that is done for, or on behalf of, the agency in relation to the agency’s functions and administration.  *Evidence* refers to any information or record that proves that a particular activity occurred, either when, how, by whom or what process, why etc. It provides the proof of that activity. | **Is the information kept within this system evidence of agency business?** | Yes\*  No  \*If YES, provide summary of the business this system is evidence of. |  |  |
| 2.2 | **Are these records already being created and kept in another system?** | Yes\*  No  \*If YES, provide the name of authoritative business system which maintains records. |  |  |
| 2.3 | Similar to 2.1, if the system replaced a another system (whether digital of hard-copy) which created and/or held information that proved that a particular activity happened and details in relation to it, the same requirements may apply to this system. | **Did this system replace a previous system or systems which kept information as evidence of the agency business?** | Yes\*  No  \*If YES, provide details of the system this replaced. |  |  |
| 2.4 | There may be recordkeeping requirements arising from:   * Internal requirements, such as agency polices, directives, or procedures; or * External requirements, such as Victorian legislation, industry codes of practice, or compliance standards.   The requirement to create/hold records may be:   * Specifically defined (e.g. lodgement of forms, government reporting requirements), or * Implied (e.g. an activity may be subject to audits, or decisions resulting from an activity may be subject to appeal. In such cases, it is *implied* that records will be required to support those processes). | **Are there any internal requirements to create and keep records?** | Yes\*  No  \*If YES, provide details |  |  |
| 2.5 | **Are there any legislative or business requirements to make and keep records of the business the system supports?** | Yes\*  No  \*If YES, provide details |  |  |
| 2.6 | Most records will be covered by **General Retention and Disposal Authorities** issued under the *Public Records Act 1973.*  These define the minimum retention requirements for records.  Advice on whether records created/held by the system are covered by retention requirements can be provided by the agency’s records management unit.  The program will take reasonable steps to destroy or de-identify personal information if it is no longer needed for any purpose. | **Does the system create/hold records for business activities which are covered by a General Retention and Disposal Authority RDA?** | X Yes\*  No  \*If YES, provide or a summary of retention requirements (and the main GDA reference number where available). |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | **Guidance** | **Question** | **Response** | **Additional Details** | **actions** |
| 2.7 | The system is supported policy, procedures and business rules that dictate how and what records should be captured into the system are available.  Documentation of the business system’s configuration, metadata schema, data dictionaries, any system customisation and/or enhancements is available.  Documentation is needed to understand and manage the information within the system as well as to assist with any necessary system migration or record export. | Are there policy, procedures and business rules that dictate how and what records should be captured into the system? | X Yes\*  No  \*If YES, provide or a summary of policies, procedures and business rules |  |  |
| 2.8 | The system is supported training that dictate how and what records should be captured into the system are available. | Is there training that dictates how and what records should be captured into the system? | Yes\*  No  \*If YES, provide the training |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | Guidance | Question | Response | Additional Details | actions |
| 2.9 | The migration of records from predecessor systems, including upgraded versions of the same system, must be planned and carried out in a controlled manner to minimise the risks associated to loss or corruption. Migration plans include:  • processes used to physically carry out the migration between business systems;  • the identification and mapping of metadata migrated and how it is persistently linked to records;  • details regarding any changes or manipulations to records and their metadata necessary during the migration process;  • migration processes are tested before implementation into live system;  • records are maintained post migration. | ***If applicable:***  ***Is the migration of records from one business system to another controlled and fully documented?*** | Yes\*  No  N/A  \*If YES, provide the documentation |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO.** | **GUIDANCE** | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 2.10 | The official record of the agency’s business activities is to be managed in an approved recordkeeping system. An *Official record* refers to a record that is the official copy of a record created or received by the agency in the conduct of its business and/or by individual staff in the course of their duties. In relation to business systems, this may include information and/or digital objects that the system creates and/or holds.  In responding to this question :   * YES, where your system creates/holds the “official record’. * NO, where:   + your system is only a duplicate of the official record, or   + the records are held in another approved digital recordkeeping system, or in the official recordkeeping system. | Is the information kept in this system the ‘official record’ of the business activity? | Yes\*  No  \*If YES, provide summary of the business this system is evidence of. |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NO. | **GUIDANCE** | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3. Identify Privacy Considerations | | | | | |
| 3.1 | **Sensitive Information**  The PDPA contains specific provisions relating to the collection of sensitive information (IPP 10). While there are many types of information that attract a heightened duty of care, for example banking details, the IPPs that specifically apply to sensitive personal information in the PDPA only apply to those in the table below. | **a. Does the application collect, use or disclose personal information?**  A Racial or ethnic origin  B Political opinions  C Membership of a political association  D Religious beliefs or affiliations  E Philosophical beliefs  F Membership of a professional or trade association  G Membership of a trade union  H Sexual preferences or practices  I Criminal record | Yes\*  No  \*If YES, provide outline of the personal information this business application will collect, use or disclose. |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NO. | GUIDANCE | QUESTION | RESPONSE | ADDITIONAL DETAILS | COMMENTS |
| 3.1 | **continued** | b. Sensitive information identified will not be collected unless one of the following apply:   * The individual has consented * The collection is required under law * The collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual that the information is about is physically or legally incapable of consenting or physically cannot communicate the consent * The collection is necessary for the defence of a legal or equitable claim   (IPP 10.1) | Yes\*  No  \*If YES, provide outline of the personal information this business application will collect, use or disclose. |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **GUIDANCE** | | **QUESTION** | | **RESPONSE** | | **ADDITIONAL DETAILS** | | **COMMENTS** | |
| 3.1 | **Continued** | | **C. Will the sensitive information be used for a research purpose?**  If sensitive information is used for research purposes all of the following conditions must be met:   * The collection is necessary for research, compilation or analysis of statistics for a government funded welfare or educational service or if relating to racial or ethnic origin, the information is collected for providing government funded welfare or educational services; AND * There is no reasonably practicable alternative to collecting the sensitive information for that purpose; AND * It is impracticable for the individual to consent.   IPP 10.2(a)(i), 10.2(a)(ii)  10.2(b), 10.2(c) | | Yes\*  No  \*If YES, provide outline of how sensitive information will be used within the business application for research purposes. | |  | |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO.** | GUIDANCE | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.2 | Unique Identifiers The PDPA has specific requirements for the collection, use and disclosure of unique identifiers (IPP 7). The PDPA defines a unique identifier as follows:  Definition – Unique Identifier  Unique identifier means an identifier (usually a number) assigned by an organisation to an individual to uniquely identify that individual for the purposes of the operations of the organisation but does not include an identifier that consists only of the individual’s name, but does not include an identifier within the meaning of the Health Records Act 2001  An example of a unique identifier is a tax file number, a driver’s license number, a passport number or a Centrelink Customer Reference Number. | **a. Does the application collect, use or disclose unique identifiers? (IPP 7.1)** | Yes\*  No  If YES, please explain how the unique identifier is necessary for the program. |  |  |
| **b. Will this application collect, use or disclose a unique identifier created by another organisation? (IPP 7.2)** | Yes\*  No  If YES, please describe the unique identifier, specify the organisation from which the identifier came, and the reason the identifier is necessary for your organisation to carry out its functions*:* |  |  |
| **c. Will a unique identifier of another organisation be used ONLY if one of the following conditions is met? (IPP 7.2)**  It is necessary for your organisation to carry out its functions (this should be described in Table 2 above); OR  The individual has consented to the use; OR  It is an outsourcing organisation adopting the unique identifier of a CSP performing obligations under a state contract  An individual will not be required to provide a unique identifier unless authorised by law or in connection with the purpose for which the unique identifier was originally assigned. | Yes\*  No  If YES, please explain: |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **NO.** | **GUIDANCE** | **QUESTION** | | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.3 | **Health Information**  While the PDPA does not apply to health information, the privacy protections that should be considered are comparable to those necessary for personal information under the PDPA. This is demonstrated by the similarity between the IPPs and the HPPs contained in the HRA.  Definition – Health Information  The HRA defines health information as:  a) information or an opinion about-  (i) the physical, mental or psychological health (at any time) of an individual; or  (ii) a disability (at any time) of an individual; or  (iii) an individual’s expressed wishes about the future provision of health services to him or her; or  (iv) a health service provided, or to be provided to an individual – that is also personal information; or  b) other personal information collected to provide, or in providing, a health service; or  c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or  d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants – but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act. | **Does the application collect, use or disclose health information?** | | Yes\*  No  \*If YES, provide outline of the health information this business application will collect, use or disclose. |  |  |
| **NO.** | **GUIDANCE** | | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.4 | Many applications rely on the use of de-identified or non-identifiable information. When such information is used it needs to be treated with caution and afforded many of the same privacy protections as personal information, where there is the potential for re-identification to occur. This is particularly the case where a program involves data matching/linking activities. For that reason, when assessing privacy of personal information, potentially re-identifiable information should be protected in the same way as personal information.  The National Health and Medical Research Council of Australia provides the following definitions, which should assist in determining when information should be considered re-identifiable (<https://www.nhmrc.gov.au/book/glossary>  Definition – De-identified  The PDPA defines the term de-identified, in relation to personal information as meaning that the information no longer relates to an identifiable individual or an individual who can be reasonably identified.  Definition – Re-identifiable Data  Re-identifiable data is data from which identifiers have been removed and replaced by a code, but it remains possible to re-identify a specific individual by, for example, using the code or linking different data sets.  Definition – Non-identifiable Data  Non-identifiable data is data that has never been labelled with individual identifiers or from which identifiers have been permanently removed, and by means of which no specific individual can be identified. Subsets of non-identifiable data are those that can be linked with other data so it can be known they are about the same data subject, although the person’s identity remains unknown. | | **Will this program collect, use or disclose re-identifiable information?** | Yes\*  No  If YES, please describe the process of de-identification and potential for re-identification. |  |  |
| **NO.** | **GUIDANCE** | | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.5 | **Legislation**  If you have legal authority under your organisation’s enabling legislation to collect, use or disclose personal information for the purposes of this program, please cite the relevant legislation and section within that act and continue with the assessment.  If your enabling legislation does not explicitly permit or require the collection, use of disclosure of the information, please proceed with the rest of the assessment. | | **Does legislation enable explicitly permit or require the collection, use of disclosure of the information?** | Yes\*  No  *Relevant legislation:* |  |  |
| 3.6 | **Information Flow Table/Diagram**  Please be as detailed as possible in describing the elements of personal information involved. This can be done as a flow table or diagram. Please include:   * Each element of personal information, including sensitive information, unique identifiers, health information and re-identifiable information * How each element will be collected, used and disclosed, and by whom * Any transfer of personal information to someone outside of Victoria (other than the organisation or the individual the information is about).   If multiple organisations will collect, use or disclose personal information, the diagram or table should identify how each organisation is involved in the program.  This table/diagram will be used to inform the assessment of the program against the IPPs in section. | | **Does the system integrate with other systems and reuses personal Information?**  **Does the system workflow information and consequently reuses personal Information?** | Yes\*  No  Yes\*  No  **If yes provide a flow diagram** |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO.** | **GUIDANCE** | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.7 | **Collection of Personal Information**  (including sensitive information and unique identifiers)  (Refer to IPPs 1, 7, 8 & 10) | **Collection**  a. Is all the information collected NECESSARY? (IPP 1.1)  b. Is it lawful or practicable for the individual to remain anonymous for the purpose of the program? (IPP 8.1) | Yes\*  No  If YES, please describe how: |  |  |
| **Notice**  c. Have you taken reasonable steps to ensure that the individual whose information is collected is made aware of the information below? (IPP 1.3) | Yes\*  No  If YES, please describe how:  The identity of the organisation and how to contact it The fact that the individual can access their information  The purpose for the collection To whom the organisation will disclose the information Any law requiring the information to be collected Consequences, if any, to the individual if the information is not provided |  |  |
| d. Is the collection done by a law enforcement agency for a law enforcement function or activity? | Yes\*  No |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO.** | **GUIDANCE** | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.7 cont | **Collection of Personal Information**  (including sensitive information and unique identifiers)  (Refer to IPPs 1, 7, 8 & 10) | **Direct/Indirect Collection**  Is the information being collected DIRECTLY from the individual? (IPP 1.4)  Will any information also be collected INDRECTLY about the individual? | Yes\*  No  Yes\*  No  If yes,  Reasonable steps have been taken to ensure the individual whom the information is about has been made aware of the information (IPP 1.5)  OR  It would pose a serious threat to the life or health of any individual if the matters were communicated to the individual |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO.** | GUIDANCE | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.8 | Use and Disclosure of Personal Information(Refer to IPPs 2 & 7) | a. Information will ONLY be used or disclosed for the primary purpose identified.  b. In addition to using and disclosing information for the primary purpose it was collected, personal information will be used or disclosed for a secondary purpose. | Yes\*  No  Yes\*  No  If YES, please check which of the following secondary purposes below apply :  a) The secondary purpose is related to the primary purpose, or for sensitive information, directly related to the primary purpose; AND  b) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO.** | **GUIDANCE** | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.8 | Continued |  | If YES, please describe the secondary purpose:   * The individual has consented (express or implied) to the use or disclosure * As necessary for research, or the compilation or analysis of statistics   IN THE PUBLIC INTEREST   * Where necessary to lessen or prevent a serious and imminent threat to an individual’s life, health, safety or welfare; or a serious threat to public health, public safety or public welfare * Where necessary on suspicion or unlawful activity as part of its investigation or reporting its concerns to relevant persons or authorities. * As required or authorised by law   If YES, please site the relevant law. |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **NO.** | **GUIDANCE** | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.8 | Continued |  | By or on behalf of a law enforcement agency for one of the following purposes:  (\* a written note must be made of any use or disclosure made under this section)   * The prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction * The enforcement of laws relating to the confiscation of the proceeds of crime * The protection of the public revenue * The prevention, detection, investigation or remedying of seriously improper conduct * The preparation or conduct of proceedings or implementation of the orders of any court or tribunal * As requested, in writing by the Australian Security Intelligence Organisation (ASIO) or the Australian Secret Intelligence Service (ASIS) * The use or disclosure is by a law enforcement agency for a law enforcement function or activity. |  |  |
| **NO.** | **GUIDANCE** | **QUESTION** | **RESPONSE** | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.9 | **Use and Disclosure of a Unique Identifier (assigned by another organisation)** | The application will use or disclose a unique identifier assigned to an individual by another organisation | Yes\*  No  If YES, please check which of the following apply :  The unique identifier assigned to an individual by another organisation will not be used or disclosed unless one of the following apply:   * It is necessary for the organisation to fulfil its obligation to the other organisation * The individual has consented   One or more of the following apply: (see IPP 2.1(d)-(g) for full conditions)   * A serious threat to individual or public health, safety or welfare * Reporting a suspected unlawful activity to the relevant person or authority as part of an investigation * It is required or authorised by law   *If YES, please site the relevant law:*  The organisation reasonably believes the use or disclosure is reasonably necessary by or on behalf of a law enforcement agency. |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NO. | **GUIDANCE** | **QUESTION** | RESPONSE | **ADDITIONAL DETAILS** | **COMMENTS** |
| 3.10 | **Data Quality** | **Please describe steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date.**  For example, check to see that the information was obtained from a reputable source such as another government agency, ensure the system is regularly tested for accuracy, conduct periodic reviews of the information, a retention schedule in place that deletes information that is over a year old, staff are trained in the use of the tools and receive periodic updates, reviews of audit trails are undertaken regularly, independent oversight, incidents are reviewed for lessons learnt and systems / processes updated appropriately |  |  |  |
| 3.11 | **Security of Personal Information**  The application has taken reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. | **Please describe steps.**  For example, the application should have data protection governance arrangements in place covering all the security domains including: Security policies and procedures, security risk management, information access, security training and awareness, security incident management, business continuity management, third party management (CSPs/government services), information security, information sharing, personnel security, ICT security, physical security. |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NO. | GUIDANCE | QUESTION | RESPONSE | ADDITIONAL DETAILS | | COMMENTS |
| 3.12 | **Policy Documentation**  The system is supported policy, procedures and business rules that dictate how personal information should be captured and accessed via the business application.    The Access and Correction principle (IPP 6) entitles individuals to view and obtain copies of their personal information and to correct personal information held about them. IPP 6 is designed to supplement existing access and correction rights under the Freedom of Information Act 1982 (FOI Act). Information held by a Victorian public sector organisation is subject to the FOI Act and therefore do not need to assess against IPP 6. | Are there policy, procedures and business rules that dictate personal information should be captured, managed, corrected and accessed via the business application? | X Yes\*  No  \*If YES, provide or a summary of policies, procedures and business rules |  |  | |
|  |  | |
| 3.13 | **Training**  The system is supported training that dictate how personal information should be captured and accessed via the business application | Is there training that dictates how personal information should be captured and accessed via the business application**?** | Yes\*  No  \*If YES, provide the training |  |  | |

| **No.** | **Guidance** | **Question** | **Response** | **Actions** |
| --- | --- | --- | --- | --- |
| 4. Recordkeeping functionality requirements for Business Applications | | | | |
| 4.1 | The system needs to be able to store read-only versions of digital records.  This applies in particular to scans or other document based objects. However, data held by a system may also need to be read only.  There should also be an audit trail of changes made to official records within the system. | **Does the system capture read-only versions of digital records it holds?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 4.2 | The system needs to produce information and other document objects in a form that can be easily read by a person, whether on screen, as an exported or printed report or extract etc. | **Does the system display the digital records in a format that can be read and understood by a person?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 4.3 | The system needs to be able to restrict read/write access to some or all information depending on the types of information being created and held by the system.  For very specific systems there may not be a need to limit access to records within the system, but there may still need to be limitations on administrative activities, such as amending data and user permissions. | **Does the system restrict access to digital records to specific individuals or groups as required?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 4.4 | The business system maintains an audit log of changes or additions made to records.  An audit log should be maintained to identify which users have accessed records as well as any actions performed on or by the system.  Audit logs give the ability to detect breaches of security, the inappropriate alteration or deletion of records and ensure that actions are being carried out according to assigned roles and responsibilities. | **Does the business system have an audit log of any actions and activities performed in or by the system?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 4.5 | The business system is capable of capturing full and fixed records in a variety of file formats.  Hardcopy systems are required to handle multiple formats of physical records. Business systems need to be able to have the same ability to capture records in a variety of formats. The business system should allow users to capture and store records received by the system in their native format.  Business processes are increasingly being carried out online and the information created by these activities may be the only evidence available of some transactions or decisions. | **Does the business system capture full and fixed records in a variety of file formats?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 4.6 | The business system is able to identify software applications used to create records.  The application name and version used of all software applications are required to assist in accessing records at risk of software obsolescence. Identification can be defined at:  • the system or module level where data is unstructured and created using the same application;  • the system or module level where all records are structured and created through the same application; and  • the individual record level where a variety of digital | **Does the business system identify the software application used to create each record?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 4.7 | Business systems need to present data and other document objects in a form which allows for human viewing that is easily understood. This can be on screen, as an exported or printed document/extract, or other suitable method. | **Does the business system retrieve and display records in a human readable form?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 4.8 | The business system ensures the interoperability of records across platforms and domains of use over time.  Interoperability means the business system will work with other systems or products. Records will often need to be kept beyond the life of the hardware and/or software used to create them. Records should always be readable and able to be converted, where necessary, for migration to other technology platforms. | **Can the business system ensure the interoperability of records across platforms and domains of use over time?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 4.9 | An upgrade strategy for the business system has been developed.  An upgrade strategy provides a plan for the continuation of the business system. In many instances, the records contained in the business system will be required beyond the potential ‘life’ of the software application.  The upgrade strategy provides for an evaluation of the expected lifespan of the current business system and how any future transitions (e.g. to new versions of the software) will occur. | **Is there an upgrade strategy for future development of the business system in place?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |

| **No.** | **Guidance** | **Question** | **Response** | **Additional Details** |
| --- | --- | --- | --- | --- |
| 5 Metadata Requirements | | | | |
| **5.1 Point of Capture Metadata**  Definition: *Point of Capture* refers to a point in time when a record entered the system and actions undertaken at that time. | | | | |
| 5.1.1 | The system needs to allocate a unique identifier to each record.  Usually this can be achieved through using an identification number. This would normally be an alphanumeric code or a serial number, such as a URI (uniform resource indicator) or Primary Key. | **Does the system create a Unique Identifier for each record?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 5.1.2 | The system needs to capture an appropriate, meaningful description of each record, to explain what the record is about.  This may not necessarily be called the Title or Subject field, but should serve the same purpose. | **Does the system capture a Title for each record?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 5.1.3 | The system needs to capture the date the record was created.  Note: The creation date may be different from the date the information is entered into the system, in particular where the record is object based (e.g. a document may be created on 1/2/2010 but not registered into the system until 3/2/2010). | **Does the system capture the date each record was created?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 5.1.4 | The system needs to capture the identity of the person, process, or system that created a record within in.  Note: A record may be generated by a process or other business system, not necessarily by an individual user of the system. | **Doe the system identify who or what process created the record?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 5.1.5 | The system needs to identify the business function the record relates to.  This may be defined at:   * the system or module level (e.g. all records in the system or module relate to the same function, and this is identified), or * an individual record level (e.g. application of a keyword from the Classification System, such as Financial Management defines the business function at a file level.) | **Does the system identify the business function and/or process that the record relates to?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 5.1.6 | The system needs to identify what software application was used to create the record.  This may be defined at:   * the system or module level (e.g. where data is unstructured and created using the same application), or * the system or module level (e.g. all records in the system or module are created through the same application), * an individual record level (e.g. for digital objects, whether they are MS office documents, PDFs, TIFFs etc. The application name and version used are required to assist in accessing records, future migration, and identifying records at risk of software obsolescence. | **Does the system identify the software application used to create the record?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 5.1.7 | The system needs to identify the type of record being held.  This may be defined at:   * the system or module level (e.g. where all records are of the same type), or * the system or module level (e.g. all records in the system or module are of the same type), * an individual record level (e.g. identifying whether the record is a letter, memo, email etc.) | **Does the system identify the format or record type for each record?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| **5.2 Metadata required relating to the registration process**  Definition: *Registration* refers to the process of entering the record into the system, and/or data related to that process. | | | | |
| 5.2.1 | The system needs to detail when each record was first registered into it.  This can be the same as the date created, but may differ if the record was captured into the system at a later stage. | **Does the system capture the date the record was registered into the system?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 5.2.2 | The system needs to identify the person, process, or system that registered the record into it.  Note: A record may be registered automatically by a process or other business system, not by an individual staff member etc., through. | **Does the system identify who or what process registered the record?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |

| **No.** | **Guidance** | **Question** | **Response** | | **Additional Details** |
| --- | --- | --- | --- | --- | --- |
| **5.3 Metadata required relating to the application of, or changes to, access rules**  Definition: *Access rules* refer to the rules that govern who can view and or edit the record within the system.  NOTE: Some of the following metadata elements may be captured outside the business system in supporting and approval documentation. Such documentation is considered part of the system for the purpose of this assessment. | | | | | |
| 5.3.1 | The system needs to capture the date access rights on a record were changed.  Subsequent changes to access rules also need to be captured.  This information may be captured automatically in an audit log, or a separate field. Alternatively it may be captured in system/approval documentation. | **Does the system capture the date and access rule was applied to a record and when it was changed?** | | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 5.3.2 | The system needs to identify of the person, process, or system that changed an access right to a record.  This information may be captured automatically in an audit log, or a separate field. Alternatively it may be captured in system/approval documentation. | **Does the system identify who or what process changed an access rule?** | | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| 5.3.3 | The system needs to identify what access rule is in place.  This information may be captured automatically in an audit log, or a separate field. Alternatively it may be captured in system/approval documentation. | **Does the system identify what access rule was applied or changed?** | | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this |  |
| **5.4 Metadata required relating to the transfer of control of a record**  Definition: *Control* refers to who has ownership of the record at an organisational level (i.e. THE AGENCY will have control of records within its systems). Transfer of control may occur if there is a transfer of the University’s functions to another agency (e.g. some part of the University’s academic program may transfer to another University; or research may be transferred to another institution when an academic moves). Transfers of control can also occur by court order, or where control of permanent records (State Archives) is transferred to State Records after 30 years.  NOTE: Some of the following metadata elements may be captured outside the business system in supporting and approval documentation. Such documentation is considered part of the system for the purpose of this assessment. | | | | | |
| 5.4.1 | The system needs to identify if a record from it has been transferred from the agency’s control.  This information may be captured in the system, or in system/approval documentation. | **Does the system identify that a record was transferred from the agency control?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  N/A | |  |
| 5.4.2 | The system needs to capture the date a record from it was transferred from the agency’s control.  This information may be captured in the system, or in system/approval documentation. | **Does the system capture the date a record was transferred from the agency control?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  N/A | |  |
| 5.4.3 | The system needs to identify the person, process, or system that organised the transfer of the record from the agency’s control.  For example, whether the transfer required by State Records, court order, agreement with another institution etc.  This information may be captured in the system, or in system/approval documentation. | **Does the system identify who or what process transferred the control of a record?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  X N/A | | . |
| 5.4.4 | The system needs to capture any relevant reference numbers authorising the transfer.  A transfer of control should be accompanied by an authorisation, such as a court order number or a General Retention and Disposal Authority reference.  This information may be captured in the system, or in system/approval documentation. | **Does the system capture the reference number of the authorisation for the transfer of a record from THE AGENCY control?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  X N/A | |  |
| 5.4.5 | The system needs to identify which agency received a record transferred from the agency’s control.  For example, the new owner/recipient of the record.  This information may be captured in the system, or in system/approval documentation. | **Does the system identify who the control of a record was transferred to?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  X N/A | |  |
| **5.5 Metadata required relating to the destruction/deletion of a record**  Definition: *Destruction/deletion* refers to the permanent and irreversible removal of the record from the system. This does not encompass migration or transfer to another system. Most records will require destruction at some stage. Few are recognised as permanent the agency archives or State archives (the latter are defined in GDA and RDA’s issued under the Public Records Act 1973.  NOTE: Some of the following metadata elements may be captured outside the business system in supporting and approval documentation. Such documentation is considered part of the system for the purpose of this assessment.  NOTE: Records relating to the destruction of records are required to be retained for 20 years. | | | | | |
| 5.5.1 | The system needs to identify whether a record exists or has been destroyed/deleted.  This information may be captured in the system, or in system/approval documentation. | **Does the system identify that a record was destroyed/deleted from the system?** | X Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  You cannot delete infringements once issued and sync’d to Pinforce. In regards to the lookup data (street name, suburbs, offences and etc.) you can only soft delete. | |  |
| 5.5.2 | The system needs to capture the date a record was destroyed/deleted.  This will be required to authenticate that a record was retained for its minimum legal retention timeframe.  This information may be captured in the system, or in system/approval documentation. | **Does the system capture the date a record was destroyed/deleted from the system?** | X Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  You cannot delete infringements once issued and sync’d to Pinforce. In regards to the lookup data (street name, suburbs, offences and etc.) you can only soft delete. | |  |
| 5.5.3 | The system needs to identify who undertook the destruction/deletion process.  NOTE: Automated bulk destruction/deletion based on pre-defined coding within a system is not recommended. Minimum retention requirements can change and there may be other requirements for records which cannot be identified through an automated process (e.g. legal cases, ongoing administrative need etc.).  The actual destruction/deletion process needs to be undertaken by someone once appropriate authorisation has been obtained through the completion of an **Authorisation form for the Destruction of Records**.  This information may be captured in the system, or in system/approval documentation. | **Does the system identify who or what process destroyed/deleted the record from the system?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  X No, the system is currently not capable of this  You cannot delete infringements once issued and sync’d to Pinforce. In regards to the lookup data (street name, suburbs, offences and etc.) you can only soft delete. | |  |
| 5.5.4 | The system needs to capture relevant reference number authorising the destruction/deletion.  Destruction/deletion should be accompanied by an authorisation (e.g. a General Retention and Disposal Authority reference number).  This information may be captured in the system, or in system/approval documentation. | **Does the system capture the reference number of the authorisation for the destruction/deletion of the record from the system?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  X No, the system is currently not capable of this  You cannot delete infringements once issued and sync’d to Pinforce. In regards to the lookup data (street name, suburbs, offences and etc.) you can only soft delete. | |  |
| **5.6. Metadata required relating to the migration of a record**  Definition: *Migration* refers to the movement of a record from one system to another system which will take on responsibility for the record.  NOTE: Some of the following metadata elements may be captured outside the business system in supporting and approval documentation. Such documentation is considered part of the system for the purpose of this assessment. | | | | | |
| 5.6.1 | The system should indicate where a record was migrated from a predecessor system.  This information may be captured in the system, or in system/approval documentation. | **Does the system identify that a record was migrated into the system from another system?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  X N/A  Records are not been migrated from another system. | |  |
| 5.6.2 | The system needs to capture the date a record was migrated to the system from another system.  This information may be captured in the system, or in system/approval documentation. | **Does the system capture the date a record was migrated into the system from another system?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  X N/A  Records are not been migrated from another system. | |  |
| 5.6.3 | The system needs to identify who or what process migrated the records into the system.  This information may be captured in the system, or in system/approval documentation. | **Does the system identify who or what process migrated the records into the system from the other system?** | Yes, within the system  Yes, in system/approval documentation  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  X N/A  Records are not been migrated from another system. | |  |

| **No.** | **Guidance** | **Question** | **Response** | **Additional Details** |
| --- | --- | --- | --- | --- |
| 6. Metadata requirements - Additional requirements | | | | |
| 6.1 | The system needs to ensure that the metadata elements (as specified under section 2) remain linked to the record throughout its existence, including if it is migrated to a new system in the future.  Note: This includes where records are transferred out of their original creating environment through subsequent migrations. | **Is the metadata as specified in section 2, linked to the record and the aggregation of records?** | Yes  No, but can be done with a change to system configuration and/or procedures  No, the system is currently not capable of this  N/A |  |
| 6.2 | The destruction of metadata within the system needs to be approved using an **Authorisation form for the Destruction of Records**.  Metadata has minimum retention timeframes as do the records they describe. Sometimes the metadata retention can be longer that the records themselves.  Note: This is a procedural matter, as opposed to a system design feature. | **Is the destruction / deletion of all recordkeeping metadata authorised using an Authorisation form for the Destruction of Records.?** | Yes  No  N/a. No metadata has ever been deleted from this system.  X N/A |  |
| 6.3. | An up-to-date metadata map is required for the system, which maps the metadata elements (as specified under section 2) to the fields within this system, or the location of this metadata in system/approval documentation. | **Is there an up-to-date metadata map for this system?** | X Yes  No |  |

**Section 2: Digital Recordkeeping Metadata Map Template**

|  |  |  |
| --- | --- | --- |
| System Name | PinForce | |
| Completed by |  |  |

|  |  |  |
| --- | --- | --- |
| **Required metadata** | **Location of metadata** | **Field name (if in system)** |
| **Metadata - point of capture** |  |  |
| Unique identifier |  | X |
| Title |  | X |
| Date of creation |  | X |
| Who / what created the record |  | X |
| Business function/process the record relates to |  | N/A |
| Creating application |  | N/A |
| Record type (e.g. letter, report memo, email etc) |  | N/A |
| **Metadata – registration process** |  |  |
| Date of action re registration or data entry |  |  |
| Who/what undertook the action re entering record |  |  |
| What action was undertaken |  |  |
| **Metadata – change access rules process** |  |  |
| Date of action re change to access rule |  |  |
| Who/what undertook the action re change to access rule |  |  |
| What action was undertaken re change to access rule |  |  |
| **Metadata – transfer of control process** |  |  |
| Date of action re transfer of control |  |  |
| Who/what undertook the action re transfer of control |  |  |
| What action was undertaken re transfer of control |  |  |
| Authorisation reference for the action re transfer of control (e.g. GDA reference) |  |  |
| **Metadata – destruction process** |  |  |
| Date of action re destruction/deletion |  |  |
| Who/what undertook the action re destruction/deletion |  |  |
| What action was undertaken re destruction/deletion |  |  |
| Authorisation reference for the action re destruction/deletion (e.g. GDA reference) |  |  |

# 7. Infrastructure Management Considerations (On Premise and Cloud)

| **No.** | **Guidance** | **Question** | **Response** | **actions** |
| --- | --- | --- | --- | --- |
| **7.1** | **Cloud infrastrcuture**  A detailed risk assessment of the recordkeeping risks associated with cloud computing has been carried out. Risks include:   * the inability to adequately control records e.g. security or privacy; * entities in another State or country may take control or claim ownership of the records; * records may not be returned upon request at the finalisation of a contractual arrangement; * the storage provider goes out of business.   Contracts for cloud storage arrangements need to ensure that the Victorian Government has the continuing responsibility for the full management and access of any records held by the provider. | **Have all risks associated with storing records in a cloud environment been identified and managed?** | Yes  No  N/a.  If yes please provide risk assessment. |  |
| **7.2** | **BACK UP** | Assess the adequacy of the back up procedures. | X Yes  No  N/a. |  |
| **7.3** | **DisaSter Recovery**  Regular testing is carried out on the recovery and restoration processes of the business system.  Regular testing ensures that recovery and restoration processes are understood and can be effectively implemented in a disaster recovery environment. | Assess the adequacy of the disaster recovery procedures.  Is regular testing done on the recovery and restoration processes of the business system? | Yes  No  N/a. |  |
| **7.4** | **TERMINATION OF CONTRACT** | Does the agency have an export process for digital content that can be actioned upon termination of contract ? | Yes  No  N/a. |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Mitigation Table** | | | | |
| Identified Risk | Mitigation Strategy or Action | Likelihood | Impact | Risk Rating |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**9. Risk Mitigation**