Public Record Office Victoria

GUIDELINE

IMPLEMENTING THE OPERATIONAL MANAGEMENT STANDARD

Version number: 1.0
Issue Date: 2 March 2020
Expiry Date: 2 March 2030

This guideline provides advice on implementing the following areas of the PROS 19/04 Operational Management Standard:

- System planning and procurement
- System maintenance
- Processes
- Training and awareness
- Contracting

Table of Contents

Introduction 3

Public Record Office Victoria Standards 3

1 SYSTEM PLANNING AND PROCUREMENT 4

1.1 IDENTIFY AND ADDRESS RECORDKEEPING AND SYSTEM FUNCTIONALITY REQUIREMENTS 4

CONSIDERATIONS 5

EXAMPLES OF RECORDKEEPING REQUIREMENTS AND SYSTEM FUNCTIONALITY 6

1.2 REVIEW SYSTEMS TO ENSURE RECORDKEEPING REQUIREMENTS CONTINUE TO BE MET 8

2 SYSTEM MAINTENANCE 9

2.1 ROUTINE SYSTEM MAINTENANCE 9

2.2 SYSTEM TRANSITION 10

3 PROCESSES 11

3.1 DESIGNING REQUIREMENTS INTO PROCESSES 11

4 TRAINING AND AWARENESS 12

4.1 TRAINING AND AWARENESS PROGRAMS 12

4.2 MEASURING PROGRAM EFFECTIVENESS 13

5 CONTRACTING 14

5.1 ACTIVITIES COVERED BY THIS PRINCIPLE 14

5.2 CONTRACTING A PROVIDER TO DELIVER A SERVICE OR PRODUCT TO THE PUBLIC OFFICE 14

EXAMPLES OF RECORDKEEPING REQUIREMENTS FOR A PRODUCT OR SERVICE 15

5.3 CONTRACTING A PROVIDER TO DELIVER A SERVICE OR PROGRAM ON BEHALF OF THE PUBLIC OFFICE 16

6 APPENDIX – RECORDKEEPING CLAUSES 18

TERMINOLOGY 18

OWNERSHIP AND CUSTODY 19

RECORD CREATION 20

RECORD FORMAT 20

RECORD METADATA 21

SYSTEMS 21

STORAGE 22

ACCESS AND USE 23

DISPOSAL 23

CONTRACT COMPLETION, EXPIRY OR TERMINATION 24

Introduction

Public Record Office Victoria Standards

Under section 12 of the *Public Records Act 1973,* the Keeper of Public Records ('the Keeper') is responsible for the establishment of Standards for the efficient management of public records and for assisting Victorian public offices to apply those Standards to records under their control.

Heads of public offices are responsible under section 13b of the *Public Records Act 1973* for carrying out a program of efficient management of public records. The program of records management needs to cover all records created by the public office, in all formats, media and systems, including organisational systems.

It is mandatory for all Victorian public offices to follow the principles and comply with the requirements of the Standards issued by the Keeper.

This guideline provides advice on implementing the Operational Management Standard. Further guidance can be found on the PROV website.

1 SYSTEM PLANNING AND PROCUREMENT

PRINCIPLE:	Recordkeeping requirements must be identified and inform system development and procurement decisions

REQUIREMENTS	
1.	When systems are being procured or developed, recordkeeping requirements must be determined and addressed.
2.	Recordkeeping systems must be regularly reviewed for their suitability in meeting the recordkeeping needs and obligations of the organisation.

1.1 IDENTIFY AND ADDRESS RECORDKEEPING AND SYSTEM FUNCTIONALITY REQUIREMENTS

When procuring or developing a system, the functionality needed to meet recordkeeping requirements must be identified and addressed. This is to ensure reliable, trustworthy and usable records can be created and stored in order to meet organisational outcomes and obligations.

The following steps outline actions to be undertaken:

STEP ONE

Start by identifying recordkeeping needs. To do this you will need to understand:

1. the business processes which the system is being procured or developed to facilitate; and
2. any legislative, regulatory, government or organisational requirements in relation to the records the system will create / hold.

For example, you need to understand whether the system will hold information which requires restricted access, or, whether the system will hold data which needs to be retained as a long term or permanent value record.

STEP TWO

Determine what functionality the system will require to meet the recordkeeping needs.

Specifying requirements for those systems storing large quantities of linked data which is frequently updated can be complicated. In this case, focus on what information within the system is likely to be needed to provide evidence of an action or decision and the recordkeeping functionality which would enable this information and associated metadata to be held / exported as a record.

A system which will be used for low value or non-critical purposes may have minimal recordkeeping functionality, whereas a system used for critical purposes will require greater recordkeeping functionality.

STEP THREE

Ensure that the system selected / developed / configured includes the required recordkeeping functionality. Funding is usually limited and there are often competing interests when systems are being procured or developed. Success may depend upon influencing those within the organisation who have the authority to make decisions about the system. Negotiating with decision makers about systems can mean taking a pragmatic approach and concentrating on the most important requirements.

CONSIDERATIONS

- **Speaking the same language**

  It is important to describe the recordkeeping requirements for systems in ways which system vendors / developers, IT staff, business managers and procurement staff can understand and see the value of. Focusing on the costs and risks of not including effective recordkeeping functionality can be a good approach. This can include the loss of evidence to defend actions and decisions, the costs and risks when staff are unable to quickly find complete and accurate information, the impacts on reputation and public trust when the wrong information is used or shared, or when data breaches occur.

- **Routine assessments as part of system development**

  The ideal situation is for an assessment of recordkeeping requirements to be a routine and mandatory part of system procurement or development, with the requirements included in the specification and applied when decisions are made. To achieve this will mean persuading key people or committees within the organisation of the necessity and value of this approach.

- **Governance**

  If there is a governance structure (i.e. a committee) responsible for overseeing or authorising system procurement / development, then including a recordkeeping assessment as a standard part of the planning and approval process could be an effective approach. The assessment would determine the recordkeeping functionality required for inclusion in the system specification. The degree to which the proposed solutions would meet recordkeeping functionality requirements would then be included in the decision-making process.

- **Alternative approaches**

  In some cases, it may be deemed acceptable for the system to not address some requirements. Instead, there may be alternative ways to achieve the desired outcomes. For example, a particular system may be designed to allow the continual overwriting of data, but may allow the automated extraction of specified data to another system to form the record.

EXAMPLES OF RECORDKEEPING REQUIREMENTS AND SYSTEM FUNCTIONALITY

Requirement	System Functionality / Capability
Creation and control of the required records	Workflow functionality Automated population / capture of metadata (i.e. date & time stamping, author details) Ability to set metadata requirements for different types of records Functionality allowing metadata values to be obtained from look-up tables or from calls to the operating system, application platform or other software applications Ability to set metadata requirements at a record, aggregation or system level Format requirements Authorisation controls (i.e. digital signatures, authorisation workflows) The ability to keep a fixed and complete version of a record at specified points in processes (i.e. that the system can capture data / information and associated metadata as a fixed object so that it can be held or exported as a record) Version control functionality Ability to create and maintain relationships between records to ensure they retain context and meaning over time (i.e. emails retain their attached documents, records relating to the same projects or activities are linked in some way) Where the system creates or receives records / data made up of more than one component, ability to maintain the relationships between all components Ability to set taxonomies / classifications / hierarchies Interoperability with other systems - where information / data will be shared or exchanged Able to manage records as aggregations –bulk actions
System security	Access control functionality, so that sensitive or confidential information can only be viewed or used by authorised people Ability to prevent unauthorised actions such as alteration, deletion, copying, printing Audit log / reporting functionality (i.e. to show actions taken, when and by whom) Digital signature functionality. This includes being able to store with the electronic record – the digital signature associated with it and any digital certificates authenticating the signature or other confirmation details. Password controls Encryption functionality – where there is a business need to encrypt electronic records and associated metadata (i.e. for external transmission), the system must store the decryption keys for as long as the record is encrypted and the record must lawfully be retained. The system should also allow the encryption to be removed by authorised users when its sensitivity declines. Hierarchy of user roles, with permissions for different actions (i.e. administrator, creator, viewer)

	User validation functionality Functionality for expunging sensitive information by producing redacted copies of records Functionality for providing an extract or thumbnail
Ability to import and export	Functionality allows selected records / data and associated metadata / system logs to be imported into or exported from the system Functionality allows selected records / data and associated metadata / system logs to be copied from the system Functionality allows specified records / data to be harvested / extracted from the system into other systems (E.g. specific sets of data and metadata to be automatically harvested from a business system into an EDRMS to form the record) Ability to import / export aggregations of records –bulk imports / exports
Retention & disposal requirements	Functionality for setting rules to automate the identification of permanent value records and assign destruction dates for temporary value records Functionality for processes (i.e. workflows) for checking / reviewing / authorising the transfer of permanent records to PROV and the destruction of time-expired temporary records Ability to sentence on creation by automatically or through user action applying a disposal sentence, based on a set of pre-defined instructions System enables permanent value digital records to be held in an approved sustainable format or to be easily, reliably and cheaply converted to such a format System enables the minimum metadata required for permanent value records to be collected and associated with each record Functionality to calculate disposal due dates from triggers Ability to destroy records but retain metadata Ability to send notifications of disposal actions to occur in a specified period of time (i.e. a workflow process) System ensures that destruction results in the complete obliteration or inaccessibility of the record and that it cannot be restored through system features or specialist data recovery techniques
Reporting	System will produce the required reports to show specified actions or issues. For example, reports identifying records which have not been extracted successfully or detailing deleted records
Searching	Functionality to allow the discovery of specific records, using a range of criteria and methods

1.2 REVIEW SYSTEMS TO ENSURE RECORDKEEPING REQUIREMENTS CONTINUE TO BE MET

Systems holding records should be regularly reviewed to ensure that functionality is working as expected. The regularity of this review will depend on the criticality of the system and the information held.

Examples of checks which should be carried out on a system include:

- access restrictions are working as expected
- correct metadata is being captured and auto-populated where possible
- titling rules are being enforced
- workflow is functioning as expected
- records are held in the correct formats
- unauthorised activities are being prevented (i.e. deletions, alterations)
- audit logs are being correctly generated and stored
- automated disposal requirements are being applied correctly to records
- records remain discoverable and readable over time (i.e. can be found through searching and are not corrupted).

Additional monitoring may be required during times when changes are occurring, such as administrative change, system upgrades or data migrations.

2 SYSTEM MAINTENANCE

PRINCIPLE:	Systems which hold records must be appropriately maintained

REQUIREMENTS	
1.	Maintenance must be resourced and routinely undertaken, to ensure that systems which hold records are reliable and operate effectively.
2.	When systems which hold records undergo transition, arrangements must ensure that the records are protected and remain accessible for as long as lawfully required. Some examples of transition are system upgrade, replacement or decommission and changes to service or hosting arrangements (e.g. outsourcing/ cloud arrangements).

2.1 ROUTINE SYSTEM MAINTENANCE

Public offices must ensure that maintenance activities are routinely undertaken so that systems are operating as expected and business continuity is supported.

Examples of maintenance activities which should be carried out regularly include:

- ensuring that product versions and security patches are kept up to date
- checking that any system interfaces or interdependencies are working correctly
- checking that system functionality is working correctly and reliably
- checking that agreed retrieval times from different storage arrangements are being met
- testing backup arrangements, to check that records and associated metadata remain accessible and uncorrupted
- checking that any system technologies or storage devices (servers, tapes etc.) are held in appropriate environmental conditions, checked for degradation and replaced / rotated as necessary.

A critical aspect is ensuring that documentation about how to maintain the technology and environment is complete and accurate. In addition, the maintenance activities must be accurately logged, so there can be confidence that they are being regularly and properly undertaken.

Maintenance program results should be reported to the appropriate committee or manager and any issues or problems rectified. The results should also be used for system planning. For example, recurrent problems with system functionality might indicate that replacement needs to be planned for. Or, if storage devices such as magnetic tapes are showing signs of degradation, this might indicate that storage conditions are not suitable.

When contracting a supplier to provide and manage information technology, requirements for routine maintenance should be included in the agreement. This includes requiring the supplier to report maintenance program results to the public office and rectify issues within specified timeframes.

2.2 SYSTEM TRANSITION

When systems are being transitioned, arrangements must ensure that records and associated metadata are protected and remain accessible for as long as lawfully required.

Examples of transitions are:

- upgrading a system
- replacing a system – which is likely to involve migrating some or all of the data / records and associated metadata to the replacement system and decommissioning the old system
- changing service or hosting arrangements – for example changing service providers or moving from an in-house hosting arrangement to an externally hosted cloud-based arrangement.

Transitioning a system can place records at risk of loss or corruption. The process needs to be carefully planned and properly resourced to ensure that the organisation can continue to function effectively, with the necessary records accessible and usable for as long as they must lawfully be retained.

When upgrading a system, consideration needs to be given to ensuring that the required configuration will be retained or can be recreated without impacting existing records. For example, by confirming that access controls, workflows and action logs will remain in place. Any integrations will, of course, need to be considered when systems are upgraded.

Any migration of records needs to be carefully planned and undertaken, to ensure that complete records, with all required metadata, are accessible and usable in the new system. The value and usefulness of records will be reduced if contextual metadata such as version information, creation dates, author details, authorisation details or relationships to other records or to projects is lost. Consideration needs to be given to audit logs and action workflows, to determine whether they need to be migrated and, if so, the best technical solution for this.

Systematic and thorough checking of migrated records and required metadata must be undertaken to ensure the process was successful. During this process, all record content and metadata should be retained until the integrity and reliability of the migrated records and destination system has been checked. If it is decided that some records will not be migrated to the replacement system, the public office must ensure that they are preserved and remain accessible until their minimum lawful retention period has expired.

New service agreements must include requirements for ensuring the necessary records are managed appropriately and will be accessible and usable for authorised purposes until they can lawfully be disposed of. Agreements must include mechanisms for monitoring this and rectifying any issues which arise within agreed timeframes.

Any system transitions must ensure that permanent value records are identified and protected, with plans in place to transfer them to PROV when the public office no longer requires ready access to them. Serious consideration should be given to transferring inactive permanent value digital records to PROV as part of the transition project. This can be a logical and efficient use of resources, and be beneficial in reducing risks to the records and preventing double-handling.

3 PROCESSES

PRINCIPLE:	Recordkeeping requirements must be designed into processes, so that records are routinely and automatically created and systematically managed

REQUIREMENTS	
1.	When processes are being determined, recordkeeping requirements must be considered and designed into the process. Records needed for organisational reasons and to meet obligations must be created and managed as part of the process, as automatically and systematically as possible.

3.1 DESIGNING REQUIREMENTS INTO PROCESSES

Writing detailed recordkeeping procedures and requiring staff across the organisation to learn and apply them is not always effective. Determining recordkeeping requirements and building them into processes and systems can be a better approach. The aim is to ensure full and accurate records of actions and decisions are routinely captured and systematically managed, with as little user effort and intervention as possible.

Being able to demonstrate that records are created and captured as part of a routine and consistent process will increase their value as evidence – they will be considered more reliable and trustworthy if it is impossible or difficult for people to change or destroy content or metadata without being detected.

Ways to achieve this are increasing with new technologies. Examples of some methods include:

- configuring systems so that as much of the required metadata as possible is automatically captured
- setting up system workflows so that people receive and can action tasks, with records of decisions / authorisations automatically captured
- setting up automated descriptive controls so that users have to make as little effort as possible (i.e. titling, classification, keywords)
- setting up access controls within systems so that users do not have to make these decisions (i.e. so that access permissions and restrictions are applied to user accounts, record types, business units etc.)
- using system functionality to generate alerts when inappropriate action occurs (i.e. attempts at unauthorised access, alteration, transmission, deletion etc.)
- setting up disposal controls within systems so that initial sentencing decisions are made automatically (i.e. based on record type, classification, titling, key words, user account and business unit etc.)
- configuring the system so that version control occurs automatically
- configuring scanners so that the scanned records have the appropriate dpi, colours, formats and some metadata is automatically populated and the images are captured into a particular area or system
- as a security measure, configuring printers so that people have to enter a code / use an access card to collect the printed documents
- as a security measure, configuring scanners so that the scanned documents are emailed to the user or are saved to a secure area or system
- preparing automated templates / forms, with automatic population of metadata and pre-set workflows, classifications, access controls, disposal controls etc.

4 TRAINING AND AWARENESS

PRINCIPLE:	Training and awareness programs ensure recordkeeping requirements and responsibilities are understood and applied across the public office

REQUIREMENTS	
1.	Ongoing training and awareness programs covering recordkeeping requirements, processes and responsibilities must be developed and implemented across the organisation.
2.	The effectiveness of training and awareness programs and activities must be measured, with improvements made as necessary.

4.1 TRAINING AND AWARENESS PROGRAMS

The first step is to identify the recordkeeping competencies (skills and knowledge) required by people in different roles and areas across the organisation. This will allow an ongoing training and awareness program to be developed and delivered which will enable people to develop these competencies.

For some roles, the recordkeeping competencies required may be sufficiently covered by receiving:

- information about recordkeeping responsibilities and processes in the organisation's induction program
- regular recordkeeping reminders incorporate communications
- instructions during training on how to use organisational systems and follow organisational processes (for example, a customer service officer may be given instructions on the level and accuracy of detail they need to input into a system to document interactions and agreements with clients).

Other organisational roles may require more detailed training about how to meet recordkeeping obligations.
For example, staff who are responsible for:

- receiving and responding to critical or sensitive communications (e.g. child protection, protected disclosure, harassment allegations etc.)
- making or documenting critical or contentious decisions
- creating and managing board and committee records
- managing major projects.

The public office must also ensure that any contractors, consultants or volunteers receive recordkeeping training as necessary. For example, if they will be creating records for the public office (e.g. by inputting data into systems) or accessing confidential or sensitive information.

In addition, those in organisational roles which have special responsibility for records management must ensure they achieve and retain the level of skill required to fulfil those responsibilities. This can be through attaining formal qualifications, attending conferences and seminars, joining professional associations and communities of practice, building informal networks of colleagues or through research and reading. This should be ongoing.

The public office must ensure that staff receive training and instruction regularly, not just as a "once off" activity.
In some organisations, staff may receive instruction during the induction process but this is not repeated or expanded on. Working with those responsible for people and culture, organisational development, information access / security and business systems training can be helpful.

Opportunities should be sought for inserting recordkeeping instructions and messaging into other training or communications. For example, recordkeeping instructions or messaging could be included in training and communications about procurement, risk mitigation, business continuity, client services, project management and in training for using organisational systems etc. Using real scenarios and case studies to illustrate the benefits of good recordkeeping and the impacts and costs of poor recordkeeping can also be effective.

4.2 MEASURING PROGRAM EFFECTIVENESS

It is critical that the effectiveness of training and awareness programs and activities is measured, with improvements and additions made when necessary. Changes to systems, processes, legislation or government / organisational policy need to be reflected in any training programs and materials. It is also important to check that staff are actually applying what they have been taught – for example, that staff are inputting the necessary level of detail into a system or applying appropriate security controls.

> ***Remember*** *- PROV has training resources you can use – check the PROV website for what is available.*

5 CONTRACTING

PRINCIPLE:	Agreements for contracting services, programs or products for a public office or on behalf of a public office specify requirements for recordkeeping

REQUIREMENTS	
1.	When contracting a provider to deliver services, programs or products to the public office or on behalf of the public office, recordkeeping requirements must be identified and included in contracts and agreements. Examples include when a public office contracts a data storage provider or a non-government organisation to deliver services on their behalf.
2.	Provision must be made for any permanent records to be transferred to PROV, at the appropriate time.

5.1 ACTIVITIES COVERED BY THIS PRINCIPLE

Public offices contract a wide range of services, under different models and arrangements. This is often referred to as 'outsourcing'. Tasks or functions can be 'outsourced' to a private sector organisation, a community or not-for-profit organisation, another public office or a consultant. Models can include a 'shared service arrangement' or a 'public-private partnership'.

When making such an arrangement, the public office must:

- create full and accurate records of the procurement process and retain them for their minimum retention period
- create full and accurate records of service provision, to ensure that the services are being delivered in accordance with contractual requirements and so that expenditure of public funds can be justified
- take responsibility for ensuring that the provider creates the necessary records and manages them appropriately, by including recordkeeping requirements in the contract or agreement.

5.2 CONTRACTING A PROVIDER TO DELIVER A SERVICE OR PRODUCT TO THE PUBLIC OFFICE

Public offices regularly contract providers to deliver a product or service to them. For example, to build a system, conduct research, digitise records, write a report, provide consultancy advice, provide payroll and other human resources services, host systems or provide digital or physical storage. Many public offices rely on another organisation to provide IT systems and infrastructure.

When contracting a provider to deliver a product or service to them, it is the responsibility of the public office to ensure that obligations under the PROV Standards and Specifications are met.

The public office must ensure that the budget for the service provision includes sufficient resources to fund any recordkeeping requirements.

Contractual arrangements must include provisions for monitoring and enforcing compliance, such as reporting against set measures or targets, with remedies covered for non-compliance.

Recordkeeping requirements will vary according to the nature and complexity of the service or product being procured.

EXAMPLES OF RECORDKEEPING REQUIREMENTS FOR A PRODUCT OR SERVICE

Product or Service	Recordkeeping Requirements
Consultant led review of a program within a public office	The public office will own all intellectual property developed for and associated with the project The provider must keep confidential any information provided by the public office in respect to the stakeholder consultation. The provider must comprehensively document the public consultation activities and results and provide these records to the public office at the conclusion of the project (the contract / agreement might also specify the format and metadata required) The provider must deliver major drafts of the report, plus the final report, in a specified format.
Provision of systems and IT infrastructure	The provider must ensure that requirements of the PROV Standards and Specifications are met, in respect to the management and storage of the records they are holding. This includes ensuring that: • digital records are in a format that is expected to survive and remain accessible and readable using readily available software for the required life of the record • digital records are held in systems that provide effective export of the records (including metadata) from the system • systems allow efficient capture of permanent value digital records as VERS encapsulated objects (VEOs) and export / transfer to PROV • protection and security controls ensure records can only be accessed, amended, used, released or disposed of, as authorised • a system maintenance program is in place to ensure records remain readable and accessible for the required life of the record. Where issues are identified, they are rectified within an agreed period of time • when systems are being upgraded or replaced, records and associated metadata are protected and remain accessible for as long as lawfully required • systems holding records enable them to be identified, retrieved and used for the period of time they must be retained • storage arrangements ensure that records can be retrieved within agreed timeframes (i.e. with agreed timeframes for different tiers of storage) • effective backup and recovery processes are implemented and regularly tested, with issues rectified within agreed timeframes • records are protected from degradation or damage for the period of time they must be retained.

5.3 CONTRACTING A PROVIDER TO DELIVER A SERVICE OR PROGRAM ON BEHALF OF THE PUBLIC OFFICE

A public office may contract a provider to deliver a service or program to the community or clients on their behalf. For example, delivering counselling or housing support services or managing a licensing process. Typically this means the provider will be acting on behalf of government so good recordkeeping is critical.

When contracting a provider to deliver services or programs on their behalf, it is the responsibility of the public office to ensure that PROV Standards and Specifications are met. The public office is accountable for this – they need to ensure that the provider they choose will create the necessary records and manage them appropriately, in accordance with PROV requirements.

This means that:

- recordkeeping capability needs to be considered and assessed when selecting a provider – do they have the appropriate systems, processes and staff?
- recordkeeping requirements must be clearly set out in the contract or agreement between the public office and the provider – see the Appendix for examples of contractual clauses for recordkeeping.
- the public office must ensure that payments to the provider include costs for meeting the recordkeeping requirements – i.e. creation, management, storage and arrangements for when the contract ends.

It is important when entering into a contract to consider the worst case scenario – if the arrangement breaks down, how the public office can ensure they have the records they need to continue delivery of the service / program and meet current and future obligations.

***Remember** – Permanent value records created or received by the provider on behalf of the public office must be transferred to PROV, at the appropriate time. The public office is responsible for ensuring this happens – arrangements and requirements need to be included in the contract and factored into the cost.*

When entering into an agreement with a provider the following should be considered:

Record creation	What records does the public office need the provider to create and hold, so that the public office can meet obligations and fulfil its functions? What records might be needed in the future by government, organisations and members of the public? (e.g. for a client of the outsourced service to prove their entitlements)
Management and Storage	What controls might need to be imposed on the records to ensure they are full, accurate, reliable and can be accessed and used for authorised purposes? (i.e. formats, metadata, authorisation controls) If the provider will be creating / receiving records which need to be moved to the public office at some point, it may be important to specify the metadata which needs to be captured and the format of the records. It is critical that records are stored in such a way that they will not suffer degradation or damage and will be preserved for as long as required. This means that the contract / agreement may need to specify storage conditions for digital / physical records – for example by specifying that PROV Storage Specifications must be met. Is there a particular system (or systems) the records need to be created and managed in?

Security and Confidentiality	Are there any security or confidentiality requirements which need to be specified? (e.g. if the provider will be collecting personal information in order to deliver a service to clients).
Access and sharing	Does the public office need to be able to access and use the records while they are being held by the provider? Will the provider need to share records / data with other organisations, on behalf of the public office? What arrangements need to be in place to ensure the public office can access records in a timely way for Freedom of Information (FOI) applications or for audits or legal proceedings etc.
Minimum retention	What arrangements need to be made to ensure records are retained for their minimum retention period, in accordance with Retention and Disposal Authorities (RDAs)? Will the provider apply the minimum retention periods and destroy time-expired records on behalf of the public office? Or will they be provided to the public office at the end of the contract, with disposal decisions and actions undertaken by the public office? Or will the records be returned to the public office periodically or at the end of the contract, so the public office takes responsibility for disposal?
Permanent value records	Will the provider be creating or holding records of permanent value? If so, what arrangements are needed to ensure records are returned with the required metadata and in an acceptable format, for transfer to PROV at the appropriate time?
End of contract	What arrangements need to be made for records when the contract ceases? (i.e. specified types of records and metadata are extracted from the providers systems in X format for import into the public office systems). What custody and ownership arrangements will apply when the contract ceases? For example, do the records need to be returned to the public office? • If **YES**, what metadata and formats are required, so that records are accessible and can be used for as long as needed? • If **NO**, how long will the provider be required to retain them? What arrangements will be in place to ensure that the records are preserved and accessible to the public office until their minimum required retention period has expired. (i.e. the public office might require the records to respond to a FOI request, a Royal Commission or a legal matter, etc.)
Monitoring and compliance	How are the recordkeeping requirements going to be monitored by the public office, to ensure that the provider is complying with them? Will the provider be required to submit periodic reports against performance measures? Will the public office conduct checks or inspections?

In contracts where the provider can sub-contract services (wholly or in part) to another provider, recordkeeping obligations must still be met.

A good approach can be for the provider to contract with the sub-contractor on the same terms as specified in their contract with the public office.

6 APPENDIX – RECORDKEEPING CLAUSES

Examples of Recordkeeping Clauses for Contracts and Agreements

The examples provided are for guidance only and can be adjusted for various scenarios.
We strongly recommend public offices seek legal advice before finalising any contracts or agreements.

The recordkeeping clauses provided below cover the following:

- Terminology
- Ownership and Custody
- Record Creation
- Record Format
- Record Metadata
- Systems
- Storage
- Access and Use
- Disposal
- Contract Completion, Expiry or Termination.

TERMINOLOGY

It may be useful to define key recordkeeping terms in the contract. People sometimes have a very narrow understanding of what a record is and may assume the recordkeeping clauses only apply to documents, not records / information / data held within all types of systems and in all sorts of formats.

EXAMPLE CLAUSE

Record means any document within the meaning of the *Evidence Act* 2008 (Vic), including:

a) anything on which there is writing; or
b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; or
c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; or
d) a map, plan, drawing or photograph.

Recordkeeping means creating and maintaining complete, accurate and reliable evidence of activities and decisions in the form of recorded information. Recordkeeping involves the design and management of processes and systems to capture full and accurate evidence of an organisation's activities.

OWNERSHIP AND CUSTODY

A clause such as this probably won't be needed when contracting a provider to deliver a simple service - such as developing a consultancy report - but can be very important when more complex arrangements are made.
For example, when contracting a provider to deliver services to the community on behalf of the public office. In this case, the public office should retain the legal ownership of the records with the service provider responsible for creating and managing records on behalf of the agency.

If the provider operates in an international jurisdiction or uses information technology which is located overseas (e.g. the use of cloud services), the legal requirements of other jurisdictions may need to be taken into account when drafting the ownership clause.

Two forms of ownership relevant to records management are:

- **Legal Ownership**: confers the title and ultimate rights in relation to the record, regardless of which organisation has custody of the record; and
- **Beneficial Ownership**: confers the right to benefit from the record without the legal title (potentially including responsibility for care and physical possession).

Providers may have custody (and beneficial ownership) of the records they create and manage on behalf of the public office while delivering the service. However, upon termination or completion of the contract, government / the public office should become the custodian (and beneficial owner) of the records.

If the public office does not have the capacity to manage and store the records upon termination or completion of the contract, a new contract with the provider should be put in place for them to retain custody of the records. This will need to include arrangements for:

- any permanent records to be identified and transferred to PROV
- the lawful retention and disposal of records
- any security and confidentiality requirements
- providing access to the records to ensure government / the public office can obtain records they need for inquiries and legal and administrative purposes and that the public can exercise their rights to information (i.e. under FOI legislation).

EXAMPLE CLAUSE

The ***< Victorian Government or name of local council / public office >*** retains legal ownership of all records of the services provided by ***< service provider >*** under Schedule **X**.

Upon termination or completion of this Agreement, the beneficial ownership of all records of the services provided by ***< service provider >*** under Schedule **X**, will be transferred to the ***< Victorian Government or name of local council / public office >***.

RECORD CREATION

It is critical that records are created to meet the current and future information and evidence needs of the government and any stakeholders, including members of the public. Future needs might include legal proceedings, parliamentary inquiries, FOI applications or Royal Commissions.

EXAMPLE CLAUSE

< Service provider > must create and maintain records that fully document the operation and delivery of ***< the service / program >***, including (but not limited to):

< state types of records which must be created and maintained >

Example – details of services delivered to individual clients, including service delivery dates, locations and the staff member providing the service.

Example – records that detail how and why grant funding decisions were made, provide evidence of how grant funding was authorised and distributed and document how grant funding recipients spent the funding.

RECORD FORMAT

This clause may not be required if the records have a short retention period (as specified in the applicable RDA). However, even if the minimum retention period is short and there is a possibility that the service arrangement will cease prior to the lawful disposal period, it may be sensible to specify a format(s) which can be migrated easily into public office systems.

If the provider will be creating and holding permanent value digital records on behalf of the public office, the records need to be in an approved long term sustainable format or be able to be converted to one. This is because they will need to be transferred to PROV at an agreed point as VEOs.

See: *PROS 19/05 S3 Long Term Sustainable Formats Specification* for further information.

EXAMPLE CLAUSE

< Service provider > must ensure that records of **< the service / program >** are maintained in a format that is expected to survive for the required life of the record and be easily migrated to the ***<public office >*** systems.

The acceptable formats are:

< state the formats here or state they must comply with PROS 19/05 S3 Long Term Sustainable Formats Specification >

RECORD METADATA

It is critical that adequate and accurate metadata is created and captured with records. This is particularly important if the public office will take custody of the records, either throughout or at the end of the contract. I This will help ensure records can be identified and managed and can be understood, trusted and relied upon.
For example, the public office might need to be certain that a particular record is a true copy of the final authorised version which was sent to a client.

If the provider will be creating and holding permanent value records on behalf of the public office, they will need to ensure the required metadata is associated with each record. This is because they will need to be transferred to PROV at an agreed point.

See *PROS 19/05 S2 Minimum Metadata Requirements Specification* for further information.

EXAMPLE CLAUSE

< Service provider > must ensure that sufficient metadata is created and maintained to allow records of ***< the service / program>*** to be identified, managed and used for current and future purposes.

The metadata required is:

< state the metadata required here or state they must comply with PROS 19/05 S2 Minimum Metadata Requirements Specification >

SYSTEMS

In some cases the public office may wish to specify that records are created or held within a particular system (or type of system).

This includes:

- if data is going to be shared between the provider system and the public office system
- if the public office knows it will need to take custody of a large number of documents at the end of the contract, it may be helpful to specify that the provider needs to hold the records in an electronic document and records management system (EDRMS) and meet PROV Specifications – 19/05 S3 and 19/05 S2, as previously mentioned.

EXAMPLE CLAUSE

< Service provider > must create and maintain records of ***< the service / program >*** in:

< state the name of the system, the type of system or specify if there are particular requirements the system must meet >

STORAGE

The public office needs to ensure that the service provider will store any records it is creating or holding on their behalf appropriately. This includes ensuring that records will be protected from loss, damage, degradation, theft or unauthorised access or release. It may also be necessary to ensure that records can be accessed within agreed timeframes.

Inclusion of storage requirements in the contract becomes particularly important in cases where the provider will be holding critical records or records which are of permanent or long term temporary value.

For digital records

There may be different retrieval timeframes agree to for records held in different storage arrangements (i.e. online versus offline storage, different storage tiers).

Where digital records of the service / program will be stored in a cloud-based arrangement, it may be necessary to specify limitations or additional requirements in the contract. Risks can arise if data is stored in a jurisdiction that does not maintain appropriate standards or is not legislatively comparable to that of the public office.

To reduce the risks associated with storing digital information in unknown jurisdictions, it is advised that:

- contracts specify the location of servers or specify any limitations on the location of servers; and
- specify that any subcontractors must adhere to the same contractual agreements as the service provider.

For physical records

In cases where the public office may need access to physical records created or held by the service provider, it may be necessary to include retrieval timeframes. If the service provider will need to place records it is creating or holding on behalf of the public office with a commercial storage provider, this must be an Approved Public Record Office Storage Supplier (APROSS).

EXAMPLE CLAUSE

< Service provider > must ensure that records of ***< the service / program >*** are kept in a stable, secure, maintained environment and protected from damage or degradation or unauthorised access and release.

< state any further requirements for the storage of digital or physical records or state that PROV Storage Specifications must be met >

Examples of other requirements:

- Effective backup and recovery processes for digital records of ***< the service / program >*** are implemented and regularly tested, with any issues rectified within ***< X timeframe >***.
- A Disaster Preparedness Plan must be created and provided to the public office which specifies how ***< service provider >*** will protect and recover records in the event of a disaster.
- Physical records of ***< the service / program >*** may only be stored in commercial storage sites certified by PROV as an Approved Provider.
- Digital records of ***< the service / program >*** may only be stored on servers located within Australia.

ACCESS AND USE

The public office must ensure that it can obtain access to records needed:

- to meet its own business needs and obligations;
- to respond to FOI requests and any information provision or data sharing obligations; and
- for legal proceedings including Royal Commissions or parliamentary inquiries.

The public office must ensure that the service provider controls access to records and does not release or use them inappropriately (i.e. for commercial profit or their own marketing purposes). This is particularly important where the service provider will be creating or receiving personal, confidential or sensitive material, on behalf of the public office.

EXAMPLE CLAUSE

< Public office > retains the right to access any records of ***< service provider >*** relevant to the delivery of ***< the service / program >***.

< Service provider > must ensure that records can be identified and provided to ***< public office >*** within ***< X timeframe >***.

< Service provider > must ensure that access to records is appropriately controlled. Third parties cannot be given access to public records without written agreement from ***< public office >***.

< Service provider > may not use the information contained in the records for purposes other than delivering the services specified in this contract, unless otherwise allowed in the contract or authorised by ***< public office >***.

< Specify any security or privacy requirements which must be met >

(For example, the service provider must comply with the *Privacy and Data Protection Act 2014* or the provisions of the Victorian Protective Data Security Framework).

< Specify any sharing or release requirements >

(For example, the service provider must share de-identified data with other specified service providers upon request).

DISPOSAL

The public office responsible for the records must prevent service providers from inappropriately disposing of the records they hold on their behalf, including by:

- unauthorised destruction;
- transfer to a third party;
- transfer out of Victoria;
- neglect or damage; or
- unlawful alteration.

The public office must ensure that the service provider does not destroy or dispose of records created or received on their behalf, except in accordance with PROV Standards, such as RDAs. In addition, the public office needs to ensure that any records which are reasonably likely to be required as evidence in a legal proceeding, including Royal Commissions or parliamentary inquiries, are not destroyed.[1]

[1] The *Crimes (Document Destruction) Act 2006* makes it an offence to destroy records which are reasonably likely to be required as evidence in a legal proceeding.

EXAMPLE CLAUSE

> ***< Service provider >*** must only dispose of a record in accordance with Standards issued under the *Public Records Act 1973* and in accordance with any instructions provided by ***< public office >***.
> This includes ensuring that records which are of permanent value are identified and returned to ***< public office >***.
>
> OR
>
> ***< Service provider >*** is required to retain records of ***< the service / program >*** in its office for a period specified in Schedule **X** and then return the records to ***< public office >*** for disposal.
>
> ***< Service provider >*** is not permitted to transfer records of ***< the service / program >*** to another party for any purpose unless authorised to do so by ***< public office >***.

CONTRACT COMPLETION, EXPIRY OR TERMINATION

The contract need to specify what will happen to records created or held on behalf of the public office when the contract ends.

If records will be transferred to the public office, the contract will need to specify requirements for this i.e. which records, what formats, what metadata etc. Consideration should be given to any control records or additional information which will be needed by the public office to access, use and manage the records. For example, is a database schema needed to assist with importing data into an organisational system.

The public office may require the service provider to store and manage records for the minimum retention period specified under an RDA. In this case, the public office must ensure the service provider has the capability and capacity to store, manage and dispose of records appropriately and that sufficient funding is included for this process.

EXAMPLE CLAUSE

> Upon completion, expiry or termination of the contract, ***< service provider >*** will transfer all records created and maintained for ***< the service / program >*** under Schedule **X** to ***< public office >*** in the agreed format and with metadata specified by the ***< public office >*** in Schedule **Y**.
>
> If ***< service provider >*** fails to provide all public records to ***< public office >*** within ***< X timeframe >*** and in the format and with the metadata required, penalties for breach of agreement will apply.
>
> Once ***< public office >*** has confirmed the records have been successfully transferred to them, ***< service provider >*** must delete the records from their system(s).