Public Record Office Victoria

GUIDELINE

IMPLEMENTING THE APPROVAL PROCESSES POLICY

Version number: 1.0
Issue Date: 15 July 2022
Expiry Date: 15 July 2027

This guideline provides advice on implementing the following areas of the *Approval Processes Policy*:

- Digital by design processes
- Full and accurate records
- Level of authority / authorisation for the process
- Minimum metadata
- Access and restrictions on access
- Changes to the approval required after it has been completed
- Level of governance
- Checks and balances
- Machine learning

Table of Contents

Introduction

Public Record Office Victoria Standards

Under section 12 of the *Public Records Act 1973*[1], 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 *Approval Processes Policy*[2]. Further guidance can be found on the PROV website.

Purpose and Scope

A robust, monitored, and well-governed approval process documents evidence of who authorised key decisions and actions on behalf of the public office or organisation, and when the authorisation was provided.

Approvals and formal authorisations may be provided by a range of roles that have the relevant delegated responsibility and authority. Approval processes, including the way they are executed, will differ depending on the role and function of the organisation as well as business and other needs.

The purpose of the *PROV Approval Processes Policy* (the policy) is to state PROV's position and clarify recordkeeping requirements.

The policy requires and supports organisations to design and implement approval processes in a manner that provides for appropriate capture of public records as evidence of authentic transactions.

The policy covers approvals processes whether they are fully digital, partially digital, or manual. However, the policy does state that organisations should design and implement digital approval processes where possible.

This aligns with *PROS 19/03 Strategic Management Standard* [3] Principle 5, Requirement 1:

> *Public offices must plan and progressively transform processes so that they become fully digital.*

The policy statements set out PROV's position to give clarity on expectations regarding capturing and managing records of approval processes. Organisations must comply with the PROV Recordkeeping Standards, including relevant retention and disposal authorities, as well as any other relevant legislation or regulations that the organisation must abide by.

---

[1] https://www.legislation.vic.gov.au/in-force/acts/public-records-act-1973/041

[2] https://prov.vic.gov.au/recordkeeping-government/document-library/approvalprocessespolicy-approval-processes-policy

[3] https://prov.vic.gov.au/recordkeeping-government/standards-framework

Authority

The *Public Records Act 1973* (section 13) requires the officer in charge of a public office to undertake a range of actions in relation to the creation, capture, and management of records that document the functions carried out by the office. They are as follows:

- to "cause to be made and kept full and accurate records of the business of the office"
- to "be responsible, with the advice and assistance of the Keeper of Public Records, for the carrying out within the office of a programme of records management in accordance with the standards established under section 12 by the Keeper of Public Records"
- to "take all action necessary for the recovery of any public records unlawfully removed from the office".

The *Approval Processes Policy* **should be implemented in line with the PROV *Value and Risk Policy***[4] so that approval processes and associated records that are high risk or of high value are prioritised, and to minimise impact on resources.

The policy must be implemented in compliance with the PROV Recordkeeping Standards, including relevant retention and disposal authorities, as well as any other relevant legislation or regulations that the organisation must abide by. Examples of relevant legislation, apart from the *Public Records Act 1973*, include the *Evidence Act 2008*, *Electronic Transactions Act (Victoria) 2000*, the *Privacy and Data Protection Act 2014 (Victoria)*, and the *Freedom of Information Act 1982 (Victoria)*[5].

It is expected that the approval process requirements, as well as risks that may require mitigation, be assessed during the design and implementation phases. This includes capturing authorisations and delegations in place to address requirements (such as situations where legislation requires approval to be made by a specific individual or their delegate). Risks should be identified and mitigated in line with the organisation's risk management framework. Tools, such as a privacy impact assessment and security risk assessment, can be used when assessing new technologies for approvals to help identify and mitigate information privacy and information security risk. PROV's Record Keeping Assessment Tool (RKAT)[6] can be used to identify compliance gaps in the approval process design and implementation in relation to PROV Standards.

It is also expected that a robust monitoring and auditing process, that is undertaken by a human being, be in place and implemented throughout the lifespan of the process.

[4] https://prov.vic.gov.au/recordkeeping-government/document-library/value-risk-policy

[5] https://www.legislation.vic.gov.au/

[6] https://prov.vic.gov.au/recordkeeping-government/learning-resources-tools/rkat

1 Policy Statement 1

All approval processes should be digital by design where possible, so that recordkeeping requirements are incorporated within the technology used.

1.1 Digital by design

Fully digital processes are encouraged where possible. The *Electronic Transactions Act (Vic)* has enabled most approvals to be done electronically rather than via ink signatures on hardcopy documents. Exceptions, where they exist, are recorded in relevant legislation and regulations. This may include sector or organisation specific legislation.

It is expected that all approval processes will be designed to be fully digital unless there is a valid exception. Examples of a valid exception include:

- legislation or regulation requires something to be manual
- the system used to implement the process doesn't have the functionality required for a particular task which therefore must be done manually
- the system has become non-operational and a temporary manual work around is required.

Whether the approval can be automated or is required to be done by a human being will depend on various factors, including level of risk and legislative requirements. The main objective is that the approval be undertaken by an approver with the appropriate authorisation to do so and that it be fully documented.

Recordkeeping requirements for the process should be identified and included during the design and implementation phases so that any controls, configuration settings and all metadata elements required are known and set.

Additional considerations may be whether the process is conducted internally or via a third party and the impact that may have on the record of the approval, triggers for human intervention in primarily automated workflows, and the impact a failure in the process will have on the business and broader community.

Review the approval processes in line with the *PROV Value and Risk Policy*[7] to determine whether any would require a minimised implementation of the *Approval Processes Policy*.[8] For example, some processes may be very low risk and low value and implementing the full Approval Processes Policy may impose an increased burden on resources that would not be justified. The results of the review should be documented and any approval processes that are affected identified.

[7] https://prov.vic.gov.au/recordkeeping-government/document-library/value-risk-policy

[8] https://prov.vic.gov.au/recordkeeping-government/document-library/approvalprocessespolicy-approval-processes-policy

2 Policy Statement 2

Full and accurate records of the approval process and approval should be created, captured, kept for the duration of their retention periods, and document the following:

a) the legislative requirement in cases where the law requires specific people or positions to provide authorisation or approval
b) the level of authority, knowledge, and responsibility, where the approver must hold a specific level
c) the details of the approval, including (at a minimum):

i. the metadata set documented in *PROS 19/05 Specification 2 Minimum Metadata Requirements*

ii. where practical or required, a metadata field, such as a label or protective markings, which denote a record's level of public access or restriction

iii. the trigger for the approval completion, with associated metadata to include the name of the approver, their position or role, and the date and time of approval for each approval point

iv. any authorised changes to the approval, with associated metadata to include the name of the person who authorised the change, their position or role, the date and time of the change, and whether the approval is current or superseded/rescinded.

2.1 Full and accurate

The criteria for determining a full and accurate record are located in *PROS 19/05 Create, Capture and Control Standard* and associated Specifications.[9]

Details regarding what is required for a full and accurate record of the approval are to be determined and built into the process design. Details should include:

- any delegated authority for the approval
- relevant legislative and regulatory requirements
- monitoring and auditing cycles, including frequency
- access restrictions.

Organisations should carefully consider whether ink signatures or paper records of approval are necessary. Points of approval that require ink signatures, for example, usually start with the printing to paper of an electronic record. The paper record is then signed with an ink pen, and then often scanned back to digital format. In most cases the use of an ink signature is because the process specifies it rather than it being required by law.

[9] https://prov.vic.gov.au/recordkeeping-government/standards-framework

2.2 Legislative requirements

While recordkeeping specific legislation includes requirements for all records, there are a range of requirements for records in legislation and regulations that are specific to sectors, agencies or functions that may also need to be considered. Agencies should be aware of their legislative and regulatory environment and consider the impacts of these on approval processes.

2.3 Authorisation and level of authority

The point of approval for a decision or action is the most important part of the record of approval. It will capture who approved what, when, and under what level of authority. This information could be captured using system workflows or audit logs, for example.

The approval process provides a clear and transparent line of authorisation for actions and decisions undertaken by, or on behalf of, an organisation. Documentation of an approval process includes ensuring that appropriate metadata fields exist and capture relevant data to provide sufficient context for the approval to be understood.

Formally delegated authority and documented lines of responsibility are required to connect any legislative, regulatory, or other responsibilities to the relevant action or decision. Documenting the line of approval ensures the capture of evidence required to confirm that the authorisation was lawfully applied.

2.4 Minimum metadata

The minimum metadata required for all public records is specified in *PROS 19/05 Specification 2*.[10] Additional metadata fields may be needed across the approval process to ensure that the full context of the approval can be clearly understood over time.

Where more than one approver is required, the approval is complete once all approvals have been obtained along with the required contextual information. If workflows do not have the capability to collect details for multiple approvers other means for capturing this information must be applied.

2.5 Access

Ensure that there is a label or other metadata field that can be used to record the access status of the record of approval. This provides the means for any access flags to be added easily throughout the lifespan of the approval process and associated records. For example, access may need to be restricted due to confidentiality or security purposes. Or access may have been evaluated in response to a Freedom of Information (FOI) request from an external party.[11] Access may change over time.

Access to the approval, including its contextual metadata, may be required for various purposes by different people at different times. Under *PROS 19/06 Access Standard*, 'public offices must support open and transparent government by only restricting access to records when required by legislation, regulation, or policy (e.g., FOI law, privacy law, organisational security framework, or other requirements)'.[12]

Identifying levels of access to records of the approval process, including the approval itself, may be managed through a variety of means. These include application of protective markings, indicating level of access in the record itself (such

[10] https://prov.vic.gov.au/recordkeeping-government/standards-framework

[11] https://ovic.vic.gov.au/freedom-of-information/

[12] https://prov.vic.gov.au/recordkeeping-government/document-library/pros-1906-access-standard

as a covering brief with check boxes for level of access), and assigning access permissions within the system. Access restrictions to records will change over time. While some records may be always open for members of the public to view, others may have access limited to authorised people only.

2.6 Restriction on access

In some instances, access to records may be restricted. There may be legislative or regulatory restrictions on releasing information. For example, if personal details of an individual are contained in an approval and releasing them would place the individual at risk, access to the information may be restricted. Where restrictions to access are applied, the reason for the restriction (such as 'required under X Act, section Y') should also be included, where this is practical.

Restrictions on access to records of an approval may be for many years (for example, the lifetime of a person), or they may only be for several weeks (for example, until a key action the approval relates to is completed). The duration will depend on the function that the approval serves and the associated risks with unauthorised people having access to the record. If a restriction on access no longer applies, the organisation should take reasonable steps to update the record to reflect its new level of access.

Flagging whether information or records associated with the approval can be released publicly or must be restricted is beneficial to the organisation and its stakeholders. This is because:

- for permanent records, it helps to flag those that may need to be closed under a section of the *Public Records Act* (and if so, which section) so that access is easier to confirm during transfer projects.
- it promotes transparency and assists with more efficient sharing of information within the organisation and across Victorian government.
- it enables provision of information to the public under and outside of the *Freedom of Information Act 1982 (Vic)*; for example, by enabling informal or proactive release of information.[13]
- it prevents information from being unlawfully disclosed, keeps secure information that is confidential, and helps to protect the privacy of individuals and other stakeholders.

When deciding whether access to a record must be restricted, the decision maker should consider the approval's contextual environment, relevant legislation, regulatory requirements, business needs, stakeholder needs, third party contract requirements, and so on.

For example, organisations subject to the *Privacy and Data Protection Act* 2014 (Vic) must manage public sector information throughout its lifecycle, including managing security risks to the confidentiality, integrity, and availability of public sector information.[14] Organisations must protect personal information they collect, hold, manage, use, disclose, or transfer in accordance with the *Information Privacy Principles* in Schedule 1 of the *Privacy and Data Protection Act.*[15]

2.7 Changes to the approval once completed

Changes cannot be permitted once the point of approval is complete. This is because any changes will cast doubt on the authenticity and integrity of the approval.

This does not prevent approvals to be rescinded or for authorised amendments to be made. Records of both the rescinded approval and its amended version will need to be kept.

---

[13] Read OVIC's practice notes on proactive and informal release here: https://ovic.vic.gov.au/freedom-of-information/practice-notes/.

[14] https://ovic.vic.gov.au/data-protection/.

[15] https://ovic.vic.gov.au/privacy/.

3 Policy Statement 3

Approval processes should be appropriately governed to demonstrate integrity and accountability, with documentation to include:

a) the level of governance required for the approval, with details based on an assessment of:

i. how critical the actions or decisions being approved are to the business, to government, to stakeholders and to the community

ii. the associated risks or possible impacts for each approval process

b) the checks and balances in place to:

i. prevent inappropriate or unlawful actions or decisions, especially those that would result in harm

ii. maintain the integrity of the approval record for the duration of its retention period

iii. protect any security, privacy or sensitivity requirements regarding information held

iv. provide transparency regarding the approval and the approval process.

c) Where automation or machine learning is used to make decisions as part of an approval process documentation should cover:

i. the points at which an approval decision or action should be undertaken by a human being, including how this is determined, justified, and designed into the approval process

ii. details regarding a program of regular monitoring and auditing of the automated process by a human being, including how this is designed, documented, and implemented.

3.1 Level of governance

The degree to which approvals will need to be governed and documented will depend on how critical they are and on anticipated risk. This means taking a systematic approach to the design, implementation, governance, and management of the approval process so that its value can be determined. This also requires an assessment of the risks associated with the process and its related records so that effective mitigation can be implemented.[16]

[16] See the Value and Risk Policy for PROV's position on a taking a value and risk-based approach to resourcing and implementing records management programs and initiatives. https://prov.vic.gov.au/recordkeeping-government/a-z-topics/policies

For example, processes that are critical for business operations, for holding government to account, for the lives and well beings of stakeholders and the community, will require a high level of documentation and rigorous governance. Processes where an incorrect approval or poor documentation may result in harm or damage will also require a high level of documentation and rigorous governance.

The level of quality assurance required for good governance will depend on the importance of the approval, as well as the consequences of incorrect or inappropriate approval decisions and actions. More stringent quality assurance should be applied to high value high risk areas. This includes manual processes that are only put in place when there is a malfunction or breakdown in the system. Measures used to determine good governance should be appropriate to the type of approval as well as to its value and level of risk.

Factors to take into consideration when determining appropriate levels of governance and quality assurance include:

- the value of the approval to the business and broader community
- the consequences of risk not being mitigated in relation to the approval process
- budget, system constraints and other factors that impact on the governance that can be applied to the approval process and what work arounds might be needed
- sensitivity of information held as part of the approval process.

3.2 Checks and balances

Strong governance processes are required to ensure that information needing to remain private or confidential due to legislation, regulation, or contractual obligations is kept secure both throughout the approval process and after the approval has been completed.

Digital approval processes often use third party software or cloud environments, which provide different governance depending on the functionality of the system, software or environment used. While some electronic environments for approval processes may include governance, auditing and monitoring capabilities, others may need an alternative solution. For example, the system may need to be configured differently to enable good governance, or it may need to be integrated with additional software to achieve an appropriate level of governance.

The criteria for appropriate governance are listed in PROV Standards, including:

- *PROS 19/03 Strategic Management Standard* (especially principle 1 Valuing Records, principle 2 Establishment, Governance and Accountability, principle 3 Strategic Planning, and principle 6 Assessment and Measurement)
- *PROS 19/04 Operational Management Standard* (especially principle 1 System Planning and Procurement, principle 2 System Maintenance, principle 3 Processes and principle 5 Contracting
- *PROS 19/05 Create, Capture and Control Standard*.

Approval processes, including use of workflows and audit logs, should align with governance structures to ensure that appropriate controls are in place. Approval processes should be included in risk management strategies with appropriate levels of mitigation in place. System and software procurement, including contracting, should consider the records management aspects required for approval processes so that any functionality or configuration required to ensure transparency, integrity and accountability is in place.

Records of approval processes will need to be accessible and managed for the duration of their retention period as defined by the retention and disposal authorities issued by the Keeper of Public Records.[17]

[17] https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas

3.3 Machine learning

A human being is usually needed to authorise approval decisions or actions that involve a high level of risk or that have major consequences if an incorrect decision or action is made.

Focusing on what points must be done by a human being rather than which can be automated accepts that automation / machine learning is already being used for parts of the approval process. A point where a value judgement or complex decision or action is required is more likely to need to be done by a person to minimise risk. Justifying these points helps with fleshing out what the approver needs to consider and why.

Using human centred design principles when developing approval processes that will use machine learning or automation ensures that points where it may have a harmful impact on the business or broader community are detected and replaced with intervention by a human being. For example, if personal harm to individuals may result, then approval should be undertaken by a human being.

In higher risk situations, automation or machine learning may be used to assist with the decision-making process that will be undertaken by a human being but not to action the approval (i.e., is not the approver). Inferences made by machine learning or statistical decision tree models are recommendations only, and not actual approvals or authorisations.

4 Key Concepts

Concept	Description
Approval Point:	An approval point is a point at which an approver authorises an action or decision as part of an approval process. There may be one or multiple approval points in a process where authorisation is required for the approval process to be considered complete.
Approval Process:	An approval process is a method used by organisations to approve decisions or actions.
Approver:	An approver is the entity used to approve or authorise a decision or action. It may be a human being or machine driven.
Approval via Digital signature:	A digital signature is a cryptographic technique that creates a unique and unforgeable identifier in an electronic document. This type of signature can be checked by the receiver to verify the identity of the author and that it has not been interfered with. Common forms of digital signatures use public key infrastructure (PKI), including digital certificates, for authentication purposes and to demonstrate integrity. Note that the practical strength of a digital signature is less than its theoretical strength. This is because users must use systems to apply digital signatures. Anyone who can use the system as if they were that person (for example, logging into a computer as that person, or using an unlocked computer) can apply the digital signature.
Approval via Electronic signature:	An electronic signature (or e-signature) on an electronic document is intended to perform the same purpose as a handwritten signature on a paper document. Types of e-signatures include: • typing your name at the bottom of an email • using a generic email signature • placing a digitised image of a handwritten signature on a scanned copy of a document or a born-digital document • typing a name and then clicking 'accept' to agree to terms and conditions on a website • handwriting a signature onto a hardcopy document and then scanning it to digital form • using a digital pen to manually sign on an electronic device Note that electronic signatures vary in their strength; some are very robust at associating a person with an action, others are relatively weak. The legal intention is for robustness to match the importance of the document. A very small number of documents must have a handwritten (referred to as ink in this policy, also known as wet) signature. Such cases are an exception as most tasks are now digital, and may be required due to: • legislation or regulation requiring something to be manual • the system used to implement the process not having the functionality required for a particular task which therefore must be done manually • the system becoming non-operational and a temporary manual work around is required.
Authenticity	The *Australian Standard on Records Management* (AS ISO 15489.1) defines an authentic record as being one that can be proven: • to be what it purports to be • to have been created or sent by the person purported to have created or sent it • to have been created or sent at the time purported.
Automated system / workflow functionality:	Electronic business systems usually contain some automation functionality that enables specific data to be collected by the system in accordance with business rules. Workflow functionality is built to require authorisation steps. It is set up so that certain people are authorised to perform specific steps; and it records the identity of the person that performs them. Note that this identity is subject to the same limitation as a digital signature in that anyone who can log on as the person with authority to do so can perform the step.

Integrity	The Australian Standard on Records Management (AS ISO 15489.1) defines the integrity of a record as referring to the record being complete and unaltered.
Reliability	The *Australian Standard on Records Management* (AS ISO 15489.1) defines a reliable record as having contents that can be trusted to be a full and accurate representation of the transactions, activities, or facts to which they attest, and which can be depended upon during subsequent transactions or activities.
Transparency	In recordkeeping, transparency means ensuring that full and accurate records are captured, maintain their integrity over time, and remain readable and understandable so that it is easy to perceive or detect the actions and decisions of Government. This helps to hold Government accountable.