Electronic Approval

Standard

Departments must comply with the requirements set out in this standard when implementing an electronic approval process.

Document Control

Applies to	All departments and Victoria Police	**Authority**	CIO Leadership Group
Period	2019-2021	**Advised by**	Enterprise Solutions, Department of Premier and Cabinet
Issue Date	August 2019	**Document ID**	EA-STD-01
Review Date	August 2021	**Version**	1.0

VICTORIA State Government | Premier and Cabinet

Requirements

PLEASE NOTE: This standard does not constitute legal advice. Departments should seek legal counsel in relation to the implementation of an electronic approval process within their organisation.

In this document “electronic approvals” (e-approvals) refers to any method used to approve a process electronically, and “process” refers to any communication, transaction or business process that is transmitted electronically.

Departments must at a minimum:

1) Ensure that when implementing an e-approval process it complies with the requirements of:
   a) the *Electronic Transactions (Victoria) Act 2000*;
   b) the *Evidence Act 2008*;
   c) the *Privacy and Data Protection Act 2014*;
   d) the *Public Records Act 1973*; and
   e) any other relevant department and portfolio legislation, regulations and policies.
2) Observe the following principles:
   a) **Appropriateness and Reliability** – the method used for an e-approval process must be appropriate and reliable for the purpose for which it is being used (having regard to all of the circumstances) and the associated risk. See section Risk based approach to help determine which e-approval process may be appropriate.
   b) **Authentication** – the method used for an e-approval process must identify and verify who was involved (particularly the person ‘signing’ the process) and demonstrate the person’s intent to approve the process electronically.
   c) **Consent** – the person(s) receiving the e-approved process must consent to engaging electronically and the method of e-approval used.
   d) **Data integrity** – the e-approval process cannot be changed, either during transit or once the data is at rest, without detection. To support good practice in providing evidence of data integrity, an audit trail of the e-approval process should be kept. It should not be possible to alter the e-approval without an audit trail being captured, see the section Audit trail.
   e) **Delegation** – an e-approval process must not exceed the approver’s delegation or compromise other departmental delegations of authority, structures or processes.
   f) **Non-repudiation** – the person(s) involved with an e-approval process must not be able to deny their involvement in the e-approval process. Ensure that prior to electronically approving, the person’s attention is drawn to the action or document that is to be electronically approved, the person involved can be identified and consent has been documented.
   g) **Privacy and Security** – security controls are in place that safeguard the e-approval process and e-signature from being altered or manipulated in transmission or once stored.

3) Determine whether the use of and type of e-approval process is appropriate by carrying out:

   a) a risk assessment (see the Victorian Government Risk Management Framework);

   b) a privacy impact assessment (see the Privacy Impact Assessment Template); and

   c) a business process review to ensure that there is a common understanding of approval requirements of the process and the implementation of an e-approval process is not just to 'remove wet signatures'.

See sections 'Supporting Information' and 'Risk based approach' for further information on e-approval mechanisms and risk.

Overview

The purpose of the Electronic Approvals Standard (Standard) is to define the business rules for electronically approving digital processes (including electronic communications and transactions). The aim of the Standard is to:

- reduce the need for hardcopy and move towards a paperless office;
- create consistency in implementation;
- identify and reduce associated risk; and
- ensure legislative and regulatory compliance in implementation.

Rationale

Being able to electronically approve government processes and records is becoming increasingly important as more processes become end-to-end digital and the government pushes towards a paperless office. E-approval processes are essential for increasing the mobility of the Victorian public sector workforce and being able to approve and record outcomes more efficiently and effectively.

E-approval processes (and e-signatures) already exist, to varying degrees, within departments and agencies. Further building on the understanding that exists across departments and agencies, this Standard sets out the key requirements of an e-approval process.

Work is already progressing at a whole of government level in relation to the implementation of the Digital Workplace Strategy. This has included developing requirements for the Born Digital Stay Digital Policy (to be published), implementation of the Automated Briefing and Correspondence Statement of Direction, and the adoption of common policy, standards, guidelines and processes for identity and access management as part of the Workforce Identity and Access Management Statement of Direction.

Scope

All Victorian State departments and Victoria Police, referred to collectively as ‘departments’, are formally in-scope.

While not required, the Standard may be adopted by agencies and partner organisations, if desired.

Related documents, tools and references

- Electronic Approvals – What to consider when planning Electronic Approval Processes (Public Record Office Victoria (PROV))
- Electronic Signatures – Advice about using electronic signatures during transactions (Public Record Office Victoria (PROV))
- *Electronic Transactions (Victoria) Act 2000*
- *Electronic Transactions (Victoria) Regulations 2010*
- *Evidence Act 2008*
- *Privacy and Data Protection Act 2014*
- *Public Records Act 1973*
- Victorian Government Risk Management Framework (VMIA)
- Victorian Protective Data Security Framework
- Born Digital, Stay Digital Policy (to be published)
- Digital Authorisations and Workflows (National Archives Australia)
- Digital Signature Standard (National Institute of Standards and Technology)
- Electronic Approval Guideline (Queensland Health)
- Electronic Approval Impact Assessment Checklist (Queensland Health)
- Electronic Approval Policy (Queensland Health)

Glossary

Definition	Description
Electronic approval or e-approval	An electronic approval or e-approval refers to any method used to approve a process electronically, and “process” refers to any communication, transaction or business process that is transmitted electronically.
Electronic signature or e-signature	An electronic signature or e-signature is any method which applies a “signature” to an electronic process.
Digital signature	A digital signature is a specific type of e-signature, which provides additional features to help manage risks associated with e-signing.
Wet ink signature	A wet ink signature is also known as handwritten or physical signature, that is used when a person physically signs a document.

Further information

For further information regarding this standard, please contact Enterprise Solutions, Department of Premier and Cabinet at: enterprisesolutions@dpc.vic.gov.au.

Supporting information

E-approval processes

E-approval processes can take many forms, including:

- email approval of an action or document; and
- electronic approval via a system workflow, where tasks are routed and assigned to individuals to undertake, including review and approve an action or document.

Automated workflow systems

An automated workflow system allows for an e-approval to be assigned to specific approvers and can provide functionality to track and report on the status of an e-approval. Some of the benefits of an automated workflow system are:

- improved productivity and process efficiency;
- reduction in manual process errors; and
- the potential to capture records in a compliant records management system.

Electronic signature (e-signature)

As part of an e-approval process an e-signature may be used. An e-signature is any method which applies a “signature” to an electronic process. Examples of different e-signatures include:

- a typed name at the end of an email;
- an image of a handwritten signature on an email or digital correspondence;
- a scanned “wet ink” signature, also known as a digitised signature; or
- a digital signature.

Digital signature

A digital signature is a type of e-signature that has additional controls to manage risks in relation to the authenticity of the person electronically signing and the integrity of the action or document signed.

A digital signature is the most secure type of e-signature, providing the highest level of confidence that your e-approval is both legally compliant and secure.

A digital signature uses encryption technology to digitally sign and authenticate a document and helps to guarantee that the e-approval has not been altered in transit. Digital signatures are underpinned by Public Key Infrastructure (PKI[1]).

A digital signature implementation should:

[1] PKI is a secure method of exchanging information. PKI is a combination of software, encryption technologies and services that enables organizations to protect the security of their electronic communications and on-line transactions: https://www.qgcio.qld.gov.au/publications/qgcio-glossary/public-key-infrastructure-pki-definition

- help with identifying and managing changes to an electronic record once the e-signature has been applied (maintaining integrity of the document that has had a digital signature applied).
- authenticate the person signing the document and prevent the person from credibly denying their identity (non-repudiation).
- meet a digital signature standard such as the National Institute of Standards and Technology's Digital Signature Standard and the ISO/IEC 14888-3 Information Technology–Security Techniques–Digital Signatures.

Considerations for departments

- The *Electronic Transactions (Victoria) Regulations 2010* outlines exemptions for the use of an e-signature in Victoria. Departments should also review other relevant legislation to determine if there is a requirement for a "wet ink" signature.
- Documents which require witnessing are not excluded from the intent of the Victorian legislation, though practical considerations as to witnessing a document may mean that the witnessing be undertaken by "wet ink" rather than e-signature.
- As with "wet ink" signatures, an e-signature can be contested regarding its lawfulness.
- It is good practice to ensure that when an e-signature is used, it forms part of the final e-approval record.
- When a document requires multiple signatures, a preferred solution would ensure that all e-signatures use the same e-signature approach, this will help retain intent, integrity and information relating to the e-approval.
- Technical considerations for an e-signature must consider the risks and security measures required in relation to meeting the needs of the document/business process. This should include user identity and access management processes that underpin the e-approval system.
- The implementation of an e-approval process may impact existing departmental processes. Consideration should be given to the efficiency and business benefits of an e-approval process and e-signature implementation.

Electronic signatures and the law

In Victoria legislation supports the use of e-signatures and as with the Commonwealth and other state and territory governments, electronic transaction legislation provides the regulatory framework for the use of e-signatures. The *Electronic Transactions (Victoria) Act 2000* provides the regulatory framework in Victoria.

The *Electronic Transactions (Victoria) Regulations 2010* outlines exemptions to the *Electronic Transactions (Victoria) Act 2000* and when it is not possible to use e-approvals. A general guide of document types that can be signed electronically can be found at the General Guide – Document types section.

As with “wet ink” signatures, an e-signature can be contested as to its lawfulness. Departments should therefore review all relevant legislation to determine if there is a requirement for a “wet ink” signature and should seek legal counsel in relation to the use of e-signatures within their organisation.

Risk based approach

The Victorian Government Risk Management Framework provides the minimum risk management Standard for the Victorian Public Sector. The Victorian Managed Insurance Authority has developed a Practice Guide to help departments and agencies meet their risk obligations and accountability.

Using a risk-based approach to implement an e-approval process will help to identify and assess common and known threats and vulnerabilities related to e-approvals, including any risks related to the approval mechanism used and associated security controls.

To determine the right type of e-approval process to use, departments need to consider the regulatory framework and the business risks associated with the e-approval process.

The most common mechanisms used by departments are outlined in the following table:

Table 1 – Risk level versus mechanism[2]

Type	Suitable for	Risk mitigation should
Electronic signature	Low to medium risk	Connect the approval with key contextual information regarding who applied what signature, in accordance with what process, and when. Link the approval clearly with what is being approved. Conduct routine audits of the approval process to demonstrate its application is consistent.
Digital signature	High risk	Manage the Public Key Infrastructure and digital certificate information appropriately so that secure information remains secure and authentication of signatories is ensured.
Email*	Low to medium risk	Ensure adherence to department email and security policies. Capture the decision made by email in a suitable business system / compliant records management system.
Automated system / workflow functionality	Low, medium and high risk	Conduct regular audits of the system and workflow functionality. Automate collection of essential contextual information where possible. Lock down audit logs. Maintain good identity and access management processes and culture.

[2] Adapted from Public Record Office Victoria ‘Electronic approval type and risk mitigation’: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/electronic-approvals

Type	Suitable for	Risk mitigation should
Wet ink signature (Hardcopy signature)	High risk	Retain hardcopy to enable forensic assessment and confirmation that the wet ink signature matches the person authorised to sign (as signatures can be forged). Connect the approval with key contextual information regarding who approved what and when, by requiring signers to write their name and or role, and to date the signature. Initial each page as well as sign the document containing what is being approved for more serious transactions.

* Email may be part of an e-approval process and include one of more of different mechanism types. For example, email could include approval via a typed signature within the email; or an email could be digitally signed; or an email could be captured as part of a fully documented workflow process, each of which will need to be considered relative to the e-approval process risks identified.

Electronic approval implementation

Steps to take prior to implementation

Prior to the implementation of an e-approval process (including the use of e-signatures) departments should:

1. Understand the purpose of any approval and signature as part of the business process in question – i.e. identify the intent of the signature. For example, is it used:
    - to bind a person to the terms of a contract;
    - to confirm approval of the contents of a document, for example brief or correspondence;
    - to signify the signatory authored the document; or
    - as an approval required by law.
2. Perform a review of legislation to determine if there are any requirements for a “wet ink” signature. This includes reviewing the *Electronic Transactions (Victoria) Regulations 2010* and other legislation relevant to the situation to determine if there are exemptions for the use of an e-signature. Legal counsel may need to be sought to assist with this review.
3. Determine the implementation approach to ensure all departmental delegation authorities are maintained by considering the delegation authority for the e-approval.
4. Identify any privacy implications by undertaking a Privacy Impact Assessment.
5. Identify any security implications. Refer to the department’s security policy and the Victorian Protective Data Security Framework to identify any data security obligations.
6. Undertake and document a risk assessment of the e-approval process. If a high level of risk is identified, seek legal counsel to help develop a risk mitigation approach.
7. Obtain consent from all parties involved by ensuring all stakeholders consent to sending and receiving information electronically. For example, an email system authenticates the sender and the act of sending the email signifies approval and consent.

Audit trail

An audit trail provides a chronological record of modifications that relate to an electronic process. By ensuring each e-approval process is supported by an audit trail, evidence of each of step of the approval process is captured. The minimum elements that should be captured as part of an audit trail include:

a) date and time of the approval; and

b) the identity of each person involved in approving the process.

An audit trail can provide evidence of alteration or manipulations of a record once it has been stored.

General Guide – Document types

PLEASE NOTE: The following table does not constitute legal advice. Departments should seek legal counsel in relation to the implementation of an electronic approval process and e-signature within their organisation.

Document type	E-signatures can be used	E-signatures can be used with caution	E-signatures cannot be used
Briefs	✓		
Confidentiality Agreements (also see 'Deeds' below.)	✓		
Conflict of Interest Declarations	✓		
Correspondence – email	✓		
Correspondence – letter	✓		
Correspondence – notice required by law		✓	
Deeds		✓	
Employment Contracts	✓		
Internal processes requiring approval	✓		
Letter of Offer	✓		
Memorandum of Understanding	✓		
Policy or procedures	✓		
Procurement Documentation	✓		
Property Documents	✓		
Service Level Agreements		✓	
Services Contracts		✓	
Trust Documents. e.g. Wills, codicils and testamentary trusts			✓

Table 2 – Document versus e-signature use

Document Control

Approval

This document was approved by the Whole of Victorian Government Chief Information Officer Leadership Group on 28 August 2019 and applies from the date of issue (see first page).

Version history

Version	Date	Comments
0.1	14/06/2019	First draft
0.2	5/07/2019	Second draft, following first round of review across all departments
0.3	9/08/2109	Third draft
1.0	28 August 2019	Approved by CIO Leadership Group