Electronic Signature Types Standard

Innovation, Privacy and Policy Division, Technology and Innovation

Version: 1.1

Approved by: Assistant Deputy Minister, FOIP and Information Management, Service Alberta	**Owner:** Executive Director, Privacy, Policy and Governance Branch	
Approval Date: April 2020	**Last Reviewed:** April 2024	**Next Review:** April 2026
Contact: InformationManagement@gov.ab.ca	**Policy Instrument type:** Standard	

Standard Statement

This standard:

- identifies the different types of electronic signatures used in, or received by, the Government of Alberta (GoA); and
- directly supports the GoA's implementation of electronic signatures.

Authority

This standard is issued under the authority of the *Government Organization Act*, the Records Management Regulation and the *Electronic Transactions Act*.

Under the Records Management Regulation, Technology and Innovation has the authority to establish, maintain, and promote the enterprise policies, standards, and procedures for the creation, handling, control, organization, retention, maintenance, security, preservation, disposition, alienation, and destruction of records in the custody and/or under the control of a Government of Alberta department or departments

Application

This standard applies to all departments defined under section 14 of Schedule 11 of the *Government Organization Act* and agencies, boards and commissions as defined in Schedule 1 of the Freedom of Information and Protection of Privacy Regulation.

Agencies, boards and commissions that are not contained within schedule 1 of the Freedom of Information and Protection of Privacy Regulation are encouraged to align with this standard.

Standard Description

This standard supports business areas considering electronic signature solutions by defining the types of electronic signatures that are in use and/or accepted by the government. Business areas must adhere to the process outlined in the Electronic Signature Solutions Guideline when selecting an electronic signature solution in order to ensure that:

- security risks are identified and mitigated;
- business needs are fulfilled; and
- legal obligations are met.

This standard aligns with the Canadian General Standards Board (CGSB) 72.34-2017, Electronic records as documentary evidence standard established by the Government of Canada.

Standard Specification

The GoA has made available two types of electronic signatures. For information about the technical requirements for electronic signatures, please review the Electronic Signatures Technical Standard.

Basic Electronic Signature: Electronic information that a person creates or adopts in order to sign a record and that is in, attached to, or associated with, the record.

Secured Electronic Signature: An electronic signature for which it can be proved that:

- the electronic signature resulting from the use by a person of the technology or process to create the signature is unique to the person;
- the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to a digital record is under the sole control of the person;
- the technology or process can be used to identify the person using the technology or process; and
- the electronic signature can be linked with a digital record in such a way that it can be used to determine whether the digital record has been changed since the electronic signature was incorporated in, attached to, or associated with, the digital record.

NOTE: A secure electronic signature aligns with the requirements identified in the *Canada Evidence Act*. To determine if this is a requirement for an electronic signature solution, refer to the Electronic Signature Solutions Guideline.

Roles and Responsibilities

See the Electronic Signature Solutions Guideline for information about roles and responsibilities.

Compliance

Consequences of non-compliance with this standard could result in damage to Government of Alberta's reputation, expose Albertans to harm and/or incur unnecessary costs. Depending on the severity of non-compliance:

- either informal or formal requests and/or follow-ups may be made by Innovation, Privacy and Policy Division, Corporate Internal Audit Services, Cybersecurity Services, Office of the Information Privacy Commissioner, Office of the Auditor General and/or Public Service Commission; and
- legislated disciplinary action (i.e., *Public Service Act*) may be taken.

References and Supporting Resources

- Digital Identity and Credential Assurance Standard
- Electronic Signature Solutions Guideline
- Electronic Signatures Technical Standard