



Electronic Signature Policy

Effective Date:
August 27, 2025

Category:
Security

Scheduled Review:
August 2026

1. Authority

[Executive Order 2016-06, Enterprise Information Technology Governance](#)

2. Document Control

This document replaces, in its entirety, the *Electronic Signature Policy*, dated January 6, 2025.

3. Purpose

This Information Technology Policy (ITP) establishes an enterprise-wide approach for the use of electronic signatures in accordance with the *Uniform Electronic Transactions Act (UETA)* which was adopted by the Commonwealth of Pennsylvania in Chapters 1, 3 and 5 of the *Electronic Transaction Act, Act 69 of 1999, 73 Pa.C.S. §§ 2260.101 – 2260.503*.

4. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

5. Policy

For definitions found within this document, refer to the [IT Policy Glossary](#).

Agencies shall comply with all requirements as outlined in the *Uniform Electronic Transactions Act (UETA)*.

Agencies shall treat all electronic signatures as a valid digital representation of a person's Signature. An electronic signature qualifies as an original Signature.

Agencies shall ensure that all electronic signatures are retained in accordance with *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*.

Note that an electronic signature may not be valid if the electronically authenticated records is rendered incapable of retention., i.e. cannot be printed or stored.

Agencies shall determine the appropriate Transaction Security Level and Level of Assurance for transactions involving electronic signatures. Refer to *Transaction Security and Assurance Levels for Electronic Signatures Procedure* for guidance on determining the Transaction Security Level and Level of Assurance for transactions involving electronic signatures.

This ITP does not restrict specific electronic signature technology tools and/or products. Agencies may implement the appropriate solution according to their business requirements that adheres to all Commonwealth policies and is supported by a vendor on state contract. For additional information or guidance on electronic signatures, agencies can refer to the *Electronic Signatures Guideline*.

In general, electronic signatures, regardless of technology, shall ensure:

- Data Integrity: Assurance that your business partner is executing the same document version provided to them for execution.
- Attribution: The intended recipient, and not an unauthorized proxy, is the actual signatory.
- Non-repudiation: This weakens any denial from a signatory that they executed the document.
- Reliability: Mitigation of concerns pertaining to alteration of document following execution.

5.1 Electronic Signature Requirements

Agencies shall give due consideration to the following considerations and the use case of the record. Agencies shall document these considerations and stipulate as follows:

- The manner and format in which an electronic signature is utilized, and the system established for those purposes.
- The type of electronic signature required; manner and format in which the electronic signature shall be affixed to the electronic record; and the criteria that shall be met by any third party assisting a person filing a document to facilitate the process.
- The agency shall be responsible for implementing a control process that ensures adequate preservation, disposition, integrity, security, confidentiality, and audit ability of electronic records.

5.2 Compliance Criteria

If an agency is subject to state or federal regulations pertaining to electronic signatures, nothing in this ITP or its supporting documents shall be interpreted in a way as to prevent an agency from implementing more stringent policies, procedures, and/or controls to comply with such regulations.

For electronic signatures to comply with state laws and statutes, the following criteria must be met to verify an electronic signature:

- Password-based signatures shall be used in conjunction with at least one of the following technologies listed below and be unique to the individual signing regardless of the technology utilized.

Technology	Description	How it works
Public/Private Key or Asymmetric Cryptography	Two mathematically linked keys are generated. One is a publicly available validation key, the other is a private key that cannot be deduced from the public key.	Often utilized within the Public Key Infrastructure (PKI), a signer creates a “digital signature” when utilizing a private signing key. This produces a unique mark, also known as a signed hash, within the document. The recipient can utilize the signer’s public key to authenticate the attached private key to verify no modifications have been made to the document after signing.
Digitized Signatures	A graphic image of a handwritten signature.	This is often accomplished by utilizing an image of a signature (e.g., verifying a signature on the back of a credit card) or through a computer device (e.g., digital pen and pad).
Electronic Seals	A graphic image of a seal from an organization or governmental.	These images are often utilized by legal persons to provide authenticity during the transaction for an organization or governmental entity.
PIN	Unique code, intended to be known only to user, that is assigned to an individual or transaction for the purposes of verification.	Assuming the PIN remains uncompromised, this authenticates the identity of the signatory.
Click-Wrap/ Click-Through	A check box in which a signer agrees or affirms intent by clicking a button.	This approach should only be utilized in low-risk transactions. In some instances, signers are asked to type “I agree” prior to clicking a button to reduce against claims of errors.

- Electronic signatures must be verifiable and attributable to the signatory. Industry standard encryption must be utilized to protect the user’s signatures and the integrity of the documents to which they are affixed. The electronic signature technology being deployed must have a means

of verifying any parties providing signature on the transaction. The ability to provide reverification must be available through the retention period of the documentation.

- The signature must establish the individual’s intent to be bound to the transaction. An individual must be fully aware of the purpose for which the signature is being provided, regardless of underlying technology. Below are a few ways in which this intent can be captured:
 - Require the individual to review the document or content which requires a signature.
 - Require formal acknowledgement by individual of electronic signature prior to application.
 - Format documents requiring electronic signature in a manner that reflects a paper record, so the significance of the signature is apparent to individual signing.
 - Provide a certification statement that is linked to signed record.
 - Alternatively, allowing signer to click “I Accept” “I Agree” or “Reject” to indicate a choice was made.
 - Formally record the date and time stamp of and with the electronic signature (as this may be different than the time the application was accessed or authenticated).

6. Contact

Questions or comments may be directed via email to [OA, IT Policy](#).

7. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the enterprise IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

8. Revision History

This chart contains a history of this publication’s revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document
Revision	08/27/2025	Added document control section Minor clarifications and grammatical updates