pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Electronic Signature Policy

Number ITP-SEC006	**Effective Date** March 1, 2006
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** January 2025

1. Purpose

This Information Technology Policy (ITP) establishes an enterprise-wide approach for the use of Electronic Signatures.

2. Scope

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

3. Background

The Uniform Electronic Transactions Act (UETA) 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. UETA provides enforceability of electronic contracts with Electronic Signatures. The objective of the standard is to allow for a wide range of Signature types. UETA gives validity to Electronic Signatures. UETA does not mandate the use of either Electronic Signatures or electronic records but provides a means to make electronic transactions acceptable and provide uniformity, if and when they are used.

General provisions of UETA in validating the use of Electronic Signatures include:

- A record or Signature may not be denied legal effect or enforceability solely because it is in electronic form.
- A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
- If a law requires a record to be in writing, an electronic record satisfies the law.
- If a law requires a Signature, an Electronic Signature satisfies the law.

4. Policy

Agencies shall comply with all requirements as outlined in the 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*.

Agencies shall determine the appropriate transaction security level and level of assurance for transactions involving Electronic Signatures. Refer to *OPD-SEC006B, Transaction Security Level and Level of Assurance for Electronic Signatures* (*Authorized Commonwealth access only*) for procedures on determining the transaction security level and level of assurance for transactions involving Electronic Signatures.

This ITP does not put restrictions on 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 *RFD-SEC006A, Electronic Signatures Reference Guide*.

In general, Electronic Signatures, regardless of technology, shall assure:

- Data Integrity: How do you know that the citizen or business partner has signed the document you provided?
- Attribution: How do you know that the citizen or business partner, as opposed to a third party, signed the document?
- Non-repudiation: How do you refute a citizen or business partner's claim that they did not sign the document?
- Reliability: How do you and the citizen or business partner prove that neither has altered the document after execution?

4.1 Security Controls

Agencies shall give due consideration to the following security requirements and the use case of the record. Agencies shall document these considerations stipulating:

- 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.

4.2 Compliance Criteria

Note: If an agency is subject to state or federal regulations, 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.

In order for Electronic Signatures to comply with state laws and statutes, the following criteria must be met to assist in the verification of an Electronic Signature:

- Password-based Signatures shall be used in conjunction with at least one of the following technologies listed below and 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 graphical 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 graphical 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 that is assigned to an individual or individual and transaction for the purposes of verification.	By requiring the signer to provide this additional criterion as part of authentication this assists in validating the identity of the signer.
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 user signing. 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 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 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).

For additional guidance on identity verification, refer to ITP-SEC039, *Keystone Login and Identity Proofing*.

5. Responsibilities

5.1 Agencies shall:

Comply with the requirements as outlined in this ITP.

5.2 Office of Administration, Office for Information Technology shall

Comply with the requirements as outlined in this ITP.

6. Related ITPs/Other References

- Definitions of associated terms of this policy are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/Glossary.aspx*
- Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: *http://www.oa.pa.gov/Policies/Pages/default.aspx*
- *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*
- *Management Directive, 210.12 Electronic Records and Electronic Signatures Initiatives and Security*

- *ITP-ACC001, Information Technology Digital Accessibility Policy*
- *RFD-SEC006A, Electronic Signatures Reference Guide*
- *OPD-SEC006B, Transaction Security Level and Level of Assurance for Electronic Signatures (Commonwealth access only)*
- *ITP-SEC023, Technical Security Assessments Policy*
- *ITP-SEC031, Encryption Standards*
- *ITP-SEC039, Keystone Login & Identity Proofing*
- *NIST SP 800-63-3, Digital Identity Guidelines*
- *Pennsylvania Electronic Transactions Act, Act 69 of 1999, 73 Pa.C.S. §§ 2260.101 – 2260.5101*
- *Uniform Electronic Transactions Act (UETA)*

7. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

8. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication shall be directed to RA-ITCentral@pa.gov.

9. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT policy waiver process. Refer to ITP-BUS004 *IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	3/1/2006	Base Policy	N/A
Revision	9/7/2006	Policy Refresh	N/A
Revision	4/2/2014	ITP Reformat; Merged RFD-SEC006B, OPD-SEC006A into ITP	N/A
Revision	07/01/2016	• Minor formatting • Removed digital signature language that relates to cryptography. • Revised URLs • Added RFD-SEC006A • Revised References Added Exemption section	N/A
Revision	3/23/2021	• Minor grammatical fixes • Policy reference updates	N/A

Version	Date	Purpose of Revision	Redline Link
		• Updated Exemption from This Policy Section	
Revision	06/09/22	• ITP Refresh • General policy language updates • Moved procedural items to RFD. Added reference to RFD in policy. • References added for OPD-SEC006B	N/A
Revision	01/04/2024	• Updated title • Removed definitions and added links. • Updated Scope. • Added reference/policy language to MD 210.5 • Added additional references to OPD-SEC006B & RFD-SEC006A • Updated security control to include the manner and format of which it is utilized. • Added new section headings – 4.1 Security Controls, 4.2 Compliance Criteria • Updated list of signature technologies and added chart which includes description and how it works. • Clarified verification criteria for electronic signatures – must be attributable, use industry standard encryption and provide verification and reverification through retention period. • Added examples of ways to capture intent.	Revised IT Policy Redline <01/04/2024>