Information Technology Policy

Commonwealth of Pennsylvania Electronic Signature Policy

Number ITP-SEC006	**Effective Date** March 1, 2006
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** June 2023

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 (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Definitions

4.1 Electronic Signature: An electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. Although Electronic Signatures are represented digitally (e.g., as a series of ones and zeros), they can take many forms and can be created by many different technologies. This should not be confused with the *Digital Signature* terminology, which is used in public key cryptography and is outside the scope of this ITP.

4.2 Personal Identification Number (PIN): A secret number that an individual memorizes and uses to authenticate their identity. PINS are generally only decimal digits.

4.3 Signature: Whether electronic or on paper, is first and foremost a symbol that signifies intent. Thus, the definition of "signed" in the Uniform Commercial Code (UCC) includes "any symbol" so long as it is "executed or adopted by a party with present intention to authenticate the writing." A signature may, for example, signify an intent to be bound to the terms of the contract, the approval of a subordinate's request for funding of a project, confirmation that a signer has read and reviewed the contents of a memo, an indication that the signer was the

author of a document, or merely that the contents of a document have been shown to the signer and that they have had an opportunity to review them.

4. Policy

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 either electronic signatures or electronic records, but provides a means to make electronic transactions acceptable, 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.

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 comply with UETA.

Agencies shall determine the appropriate transaction security level. Refer to OPD-SEC006b *Transaction Security Level and Level of Assurance for Electronic Signatures* for procedures on determining transaction security levels.

Agencies shall give due consideration to security requirements and the use case of the record.

Agencies shall document these considerations stipulating:

- The type of electronic signature required;
- The 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.

Procedures implemented by the agency shall comply with policies and procedures established for the maintenance of official records as defined by the Pennsylvania Historical and Museum Commission (PHMC). PHMC requirements and procedures can be referenced through the following link: State Government Services.

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

- Data Integrity – How do you know that the citizen or business partner has signed on 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?

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.

This ITP will not put restrictions on specific electronic signature technology tools and/or products.

Agencies may implement the appropriate solution that adheres to all Commonwealth policies, meets agency's business requirements, and is supported by a vendor on state contract.

In order for electronic signatures to be in compliance with state laws and statutes, the following criteria must be met:

- Password-based signatures should be used in conjunction with at least one of the following: PKI, signature stamps, electronic seals, or simple click-wrap.
- Electronic signatures must be verifiable. Electronic signature technology being deployed should verify in real-time using algorithms or forensic analysis of the signature dynamics or measurements.
- The signature must be unique to the individual whether it is a physical measurement such as a fingerprint or a virtual measurement such as a mouse click.
- The signature must establish the individual's intent to be bound to the transaction. Signatory must be fully aware of the purpose for which the signature is being provided, regardless of underlying technology.
- The signature must be applied in a tamper-evident manner, industry standard encryption must be used to protect the users' signatures and the integrity of the documents to which they are affixed. (Refer to ITP-SEC031 *Encryption Standards*).

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
- 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*
- ITP-SEC023 *Information Technology Security Assessment and Testing Policy*
- ITP-SEC031 *Encryption Standards*
- ITP-SEC039 *Keystone Login & Identity Proofing*
- NIST SP 800-63-2 *Electronic Authentication Guideline*
- Pennsylvania Electronic Transactions Act, Act 69 of 1999, 73 Pa.C.S. §§ 2260.101 – 2260.5101
- Uniform Electronic Transactions Act (UETA) Full Text

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 is to 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 • Updated Exemption from This Policy Section	N/A
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	Revised IT Policy Redline <06/09/2022>