pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Commonwealth of Pennsylvania Electronic Signature Policy

ITP Number ITP-SEC006	**Effective Date** March 1, 2006
Category Security	**Supersedes**
Contact RA-ITCentral@pa.gov	**Scheduled Review** July 2017

1. Purpose

The purpose of this Information Technology Policy (ITP) is to establish an enterprise-wide approach for the use of standards for electronic signatures.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Definitions

3.1 Electronic Signature – Is "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 all electronic signatures are represented digitally (i.e., as a series of ones and zeros), they can take many forms and can be created by many different technologies. Not to be confused with the *Digital Signature* terminology, which is used in public key cryptography and is outside the scope of this ITP.

3.2 Personal Identification Number (PIN) – A secret number that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.

3.3 Signature – A 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 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, and 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 he or she has had an opportunity to review them.

3.4 Transaction Security Levels – A value assigned to a transaction to determine the level of security that should be applied to the electronic signature of that transaction. The three levels are:

Low Risk / Low Impact Transactions (Level A) - Transactions in this category have little value to potential hackers and would have minimal consequences if compromised.

Low to Medium Risk / Medium to High Impact Transactions (Level B) - Transactions in this category have moderate to high value to potential hackers and/or have moderate to high consequences if compromised.

High Risk / High Impact Transactions (Level C) - Transactions are high risk, high consequence transactions that require high security measures.

4. Policy

The Uniform Electronic Transactions Act (UETA) provides enforceability of electronic contracts with electronic signatures. The objective of the standard is to allow for a wide range of signature types. One of provisions of the Act is defining and giving 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:

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

A key, underlying tenet supporting the use of electronic signatures is that a signature is not part of the substance of a transaction, but rather of its representation or form. Signatures serve the following general purposes:

Evidence: A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.

Ceremony: The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent "inconsiderate" engagements.

Approval: In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it is to have legal effect.

Efficiency and logistics: A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document. Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

In an effort to ensure interoperability, and to be technology neutral, the Pennsylvania 1999 Act 69 Electronic Transactions Act sets the rules for the acceptance and use of electronic transactions by Commonwealth agencies. This statute directs all agencies under the governor's jurisdiction to comply with standards published by the Office of Administration (OA) for the use of electronic signatures.

To the extent that a Commonwealth agency uses electronic records and electronic signatures, the agency, after giving due consideration to security requirements, may specify whether electronic records are to be signed by electronic means and, if so, may stipulate:

- The type of electronic signature required;
- The manner and format in which the electronic signature is to be affixed to the electronic record, and;
- The identity of criteria that is to be met by any third party used by a person filing a

document to facilitate the process.

The agency is 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 are to 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, are to 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 3rd party, actually signed the document?
- Non-repudiation - How do you refute a citizen or business partner's claim that he/she didn't 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 is to be interpreted to prevent an agency from implementing more stringent policies, procedures, and/or controls than are indicated in this document.

This ITP does not put restrictions on specific electronic signature technology tools and products. Agencies may implement the appropriate solution that adhere to all ITPs, meet the 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 forsenic 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-SEC020 *Encryption Standards for Data at Rest* and ITP-SEC031 *Encryption Standards for Data in Transit*)

NIST Special Publication 800-63-2 *Electronic Authentication Guideline* provides technical guidelines that are recommended to agencies implementing electronic signature services.

- Identity proofing and registration of electronic signature applicants should be

conducted

- Tokens (typically a cryptographic key or password) for authentication should be implemented
- Token and credential management mechanism should be used to establish and maintain token and credential information
- Develop procedures and protocols to support the authentication mechanism between the Claimant (party providing the electronic signature) and Verifer (party verifying the authenticity of the electronic signature)
- Develop procedures to provide assertion statements from a Verifer to a Relying Party (a system that pvoides access to a secured application, i.e. a claims-based application)

For additional guidance on identity verification, refer to ITP-SEC037 *Identity Proofing of Online Users.*

5. Guidelines

There are several types of electronic signatures. Each signature type provides different levels of assurance for the key characteristics of an electronic transaction: data integrity, attribution, non-repudiation, and reliability. The decision as to which type of electronic signature is appropriate for a particular type of electronic transaction is determined by the transaction's security risk. A process has been defined to determine the level of transaction security risk. This process is presented below.

Step 1: Define the electronic government transaction
Answer the question: What is the electronic transaction that the agency will need to protect?

It is important to note that separate transactions in support of one electronic government business function may involve different levels of risk, and is to be assessed separately. Most of the time, however, it is the sensitivity of the data that determines the level of risk, and not the medium for moving the data.

Example: The agency will allow citizens to purchase a license online.

Step 2: Identify the type of information necessary for the transaction.
Answer the question: What information is involved in the transaction?

When identifying the type of information necessary for the transaction, it is important to view everything in the electronic envelope as a unit, rather than as separate pieces of paper.

For example, a password is useless until it is associated with a user, logon-id, and an application. Similarly, bits and pieces of information that have no value separately may become very valuable when put together.

Example: Will the submission of credit card information associated with the electronic version of a license application, which will include such items as address, telephone number and other identifying characteristics, be required?

Step 3: Evaluate the consequences of a security breach.
Answer the question: If the information in question is compromised, what would be the

consequence?

To make this determination, the agency is to always consider legal, political and public trust implications. In accordance with the following guidelines, decide if the consequence of compromise would be low, medium, or high.

- **Low-Impact:** If an unauthorized individual views the type of information that was compromised, the consequences to the Commonwealth and citizen would be minimal. Information in this category may already be accessible to the public, or it may be confidential, but not very harmful if released. Generally, this includes information that would cause no major legal problems, and would not be of much interest to the press or the general public.

  Example: A hacker intercepts someone's telephone number.

- **Medium-Impact:** If an unauthorized individual views the type of information that was compromised, the consequences to the Commonwealth and citizen could be significant. Information in this category is generally not accessible to the general public, and may cause harm to the protected individual if released. Generally, improper release of information in this category would likely be noticed by the press, and could cause legal problems for the Commonwealth.

  Example: Someone's credit card information is compromised.

- **High-Impact:** If an unauthorized individual views the type of information that was compromised, the consequences to the Commonwealth and citizen would be extremely serious. This category includes information of a highly confidential nature that could cause significant hardship or embarrassment to the protected individual if improperly released. The compromise of information in this category could result in considerable legal problems for the Commonwealth, and would significantly erode public trust in the integrity and security of information collected/managed by Commonwealth agencies.

  Example: Someone's record of psychiatric treatment is made public, or a hacker downloads thousands of social security or credit card numbers.

Step 4: Plot the security breach impact result on the Security Assessment Matrix below.
Based on the answers to Steps 1 through 3, identify the level of impact (i.e., low, medium, or high) and plot the result on the matrix below.

Step 5: Evaluate the security breach risk.
Answer the question: What is the likelihood that someone with malevolent intentions would actually try to compromise the information in the transaction?

To make this determination, evaluate how valuable the information in question may be to potential hackers. Keep in mind that "value" does not always imply monetary value; it could also pertain to the information's shock value, and in severe cases, whether the information could be of value to terrorists. In addition, the volume of transactions involved is to be taken into consideration as well.

Decide which of the following categories best describes the security breach risk for the application/transaction in question.

- **Low-Risk Security Breach.** Information in this category is of little interest/use to potential hackers, and even if an unauthorized individual viewed the information [the information were viewed by an unauthorized party], it would be of very little value.

  Example: Although John Doe may not want his age to be disclosed, few people would be interested in the age of a single individual.

- **Medium-Risk Security Breach.** Information in this category may have value to hackers and could be a target for a privacy violation.

  Example: Intercepting someone's credit card information.

- **High-Risk Security Breach:** Information could be extremely valuable to hackers.

  Example: Intercepting thousands of credit card numbers.

Step 6: Plot the security breach risk result on the matrix below.
Based on the answer to Step 5, identify the application/transaction risk level (Low, Medium, or High) and plot the result on the matrix below.

Step 7: Review the results of the Security Assessment Matrix.
Use the matrix below to determine the appropriate level of security for the application/transaction. The intersection of the Impact Assessment Result (Step 4) and the Risk Assessment Result (Step 6) on the Security Matrix will indicate the level of security your agency is to consider for the application/transaction in question.

If the assessment determines there is no impact or risk associated with the application/transaction in question, the assessment will not yield results on the matrix, and the agency is not required to consider a security procedure. For example, posting non-sensitive information to a web site for access by the public would be considered a no-risk, no-impact e-government activity.

Security Assessment Matrix

Impact	**Risk**		
	Low	**Medium**	**High**
Low	Level A	Level B	Level B
Medium	Level B	Level B	Level B
High	Level B	Level B	Level C

It is the responsibility of the agency to follow industry standards and Commonwealth best practices when determining which products will be used to implement the desired security level.

Once the Security Risk Assessment for the electronic transaction has been completed, the most effective type of electronic signature for this type of transaction can be determined. The following chart describes the types of electronic signatures that can be used, considering the transaction security level (security risk and impact level), with examples for each type.

In Pennsylvania, electronic records and signatures satisfy requirements of a written signature. In addition, when using one of the electronic signature technologies in the chart,

certification procedures may be required to establish a presumption that they are the records or signatures of the person identified by the technology.

Electronic Signature Examples	Examples of Transactions using Electronic Signature based on Risk and Impact Level
Low Risk / Low Impact Transactions – Level A	
• Name typed at the end of an email. • "I Agree" button on a web page • Digitized image of signature (Signature scanned from an original written signature)	• Non-sensitive e-mail correspondance • Letter providing general information to citizens or business partners. • Acknowledgement that you read and agree with the information presented.
Low to Medium Risk / Medium to High Impact Transactions – Level B	
• User ID and Password (with SSL) • User ID and PIN	• Online credit card payments • Sensitive e-mail correspondence • Online procurements • An agency provides PIN numbers to citizens to authenticate their identity for online tax filing. When combined with SSL, this provides sufficient authentication.
High Risk / High Impact Transactions – Level C	
• Digital Certificate • Biometrics	• JNET / Criminal Justice • On-Line Medical Records Transmission

6. Related ITPs/Other References

- RFD-SEC006A **–** *Electronic Signatures Reference Guide*
- ITP-SEC020 - *Encryption Standards for Data at Rest*
- ITP-SEC023 – *Information Technology Security Assessment and Testing Policy*
- ITP-SEC031 - *Encryption Standards for Data in Transit*
- ITP-SEC037 - *Identity Proofing of Online Users*
- NIST SP 800-63-2 – *Electronic Authentication Guideline*
- Pennsylvania Electronic Transactions Act 1999 Act 69 Full Text
- Uniform Electronic Transactions Act (UETA) Summary
- Uniform Electronic Transactions Act (UETA) Full Text (.pdf)

7. Authority

- Executive Order 2016-06, Enterprise Information Technology Governance

8. Publication Version Control

It is the 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 are to be directed to RA-ITCentral@pa.gov.

9. Exemption from This Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Agency CIO approval is required.

This chart contains a history of this publication's revisions:

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