pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Identity Proofing of Online Users

ITP Number ITP-SEC037	**Effective Date** February 10, 2016
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** February, 2017

1. Purpose

The purpose of this Information Technology Policy (ITP) is to establish standards for online identity proofing of public users accessing Commonwealth IT web services or online applications.

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

Account: The online credential being presented as representing a *person.*

Anonymous logon (login): Access to a *system* which does not require any information on the *person* accessing the *system.*

Authentication: The process of establishing confidence in the validity of a person's logon account, usually as a prerequisite for granting access to resources in an information system.

Authentication Method: The type of authentication being used to validate a person's logon account. There are three categories:

- Something you know (e.g. PIN, password, shared information).
- Something you possess (e.g. token, smart card, digital certificate).
- Something you are (biometrics – e.g. fingerprint, voice, iris, face).

Authorization: The process of verifying that an authenticated account is permitted to have access to a system based on the person's business responsibilities.

Directory: Enterprise Directory for "citizens" managed by the Departments of Human Services and Labor and Industry. It allows Persons to self-register and manage their accounts.

FIPS: Federal Information Processing Standard – federal IT standard established by NIST.

Identity Proofing: The process of verifying the real life identity being claimed by a person.

Keystone Key: The online account established for a *person* and stored in the Directory.

Knowledge Based Authentication (KBA): An identity verification method where the person is asked a selection of questions gathered from information on that person from a variety of public and commercial data systems with the assumption that the real person would know the correct answers whereas an imposter would not.

Level of Assurance (LOA): The measurement of the degree or level of confidence that the *person* is who they are claiming to be.

Multi-Factor Authentication: The use of two or more of the *Authentication Methods*. Two-factor would employ one each of two of the methods; three-factor would employ one each of all three methods.
NASCIO: National Association of State Chief Information Officers.
NIST: National Institute of Standards and Technology, a division of the federal Department of Commerce tasked with research and, including establishment of federal IT standards.
NSTIC: National Strategy for Trusted Identity in Cyberspace, a federal initiative for secure, privacy enhancing identities in cyberspace.
OMB: Federal Office of Management and Budget.
Person: A natural person.
Public User: Any *Person* who seeks to permissibly access *Systems* for their own personal business or the legitimate business of another Person or entity, and not in the capacity of, or on behalf of, an owner or manager of the System. .
Self-asserted Identity: the unverified claim of a *Person* of who they are.
Special Publication (SP): Technical or implementation details issued by NIST.
System: Any Commonwealth IT system, web service, or online application which is open to access by Public Users.

4. Background

In today's world there numerous drivers for moving services to the Internet. These include:

- Speed – immediate or near-time response to information requests or applications
- Efficiency – information can be exchanged and verified without need for human intervention
- Cost savings – fewer staff are required to handle public user inquiries or other business

In many instances there is no business need to establish the true identity of the *person* interacting with a *system*. A *person* who is seeking publicly available information on state parks, for example, would not need to provide proof of who they are. A self-asserted identity is sufficient to satisfy the delivery of this type of service.

In other instances the agency or business owners of a *system* may require some knowledge or proof of who the *person* is. That is, is the person really who they are claiming to be?

The federal government established the National Strategy for Trusted Identities in Cyberspace (NSTIC) in 2011 with the goal to establish a user-centric "Identity Ecosystem", an online environment where individuals and organizations will be able to trust each other based upon agreed standards to obtain and authenticate their digital identities—and the digital identities of devices.

The four guiding principles of NSTIC are:

- Identity solutions will be **privacy enhancing** and **voluntary**
- Identity solutions will be **secure** and **resilient**
- Identity solutions will be **interoperable**
- Identity solutions will be **cost-effective** and **easy to use**

The NSTIC program is being promoted through a series of grants issued by the National Institute of Standards and Technology (NIST) to both public and private entities and collaborations. NIST also fostered the establishment of a private entity, the Identity Ecosystem Steering Group (IDESG) to serve as a governance body around NSTIC.

Guidance for NSTIC and related policies at the federal and state levels has been provided through

- Federal Identity, Credential, and Access Management (FICAM)
- Office of Management and Budget M-04-04: E-Authentication Guidance for Federal Agencies
- NIST SP 800-63-2: Electronic Authentication Guide
- NASCIO: State Identity, Credential, and Access Management (SICAM)

In 2013, the Commonwealth Office of Administration, in partnership with the Department of Human Services, was issued an Office of Management and Budget (OMB)-sponsored NIST grant to develop NSTIC programs within state government. In alignment with the federal standards, the Commonwealth has established these policies for levels of assurance and guidance for their application to Commonwealth systems.

5. Objective

The objective of this ITP is to provide standards for identity proofing of public users seeking to access Commonwealth systems.

- Provide standard processes to verify or proof the online identity of a public user
- Establish levels of assurance aligning with the degree of confidence in the identity of the person attempting to access Commonwealth
- Provide guidance for use of these processes and levels of assurance

6. Policy

The scope of this ITP is limited to identity proofing levels and corresponding authentication requirements. Authorization focuses on the actions or activities the public user is permitted after authentication has occurred and is outside of the scope of this ITP. This ITP DOES NOT seek to establish or to impose business requirements on agency applications or services, particularly with regard to authorization of a public user. Such requirements are left to the agency and/or the appropriate business unit within the agency to determine.

The following levels of assurance (LOA) are established for the commonwealth:

LOA P1: Self-asserted identity with little or no confidence in who the *person* behind the identity is. This is the lowest level of assurance and should only be used in circumstances where anonymous logons would be allowed and where the true identity of the person is irrelevant.

Examples of such use would include:

- Portal logon to greet returning people
- Dissemination of publicly available information
- Preliminary application or registration for a program where the identity is established at a later step.

LOA P2: Identity for which there is some level of confidence in who the *person* behind the identity is. The identity may be verified in a number of ways such as presentation of proofing materials (e.g. driver's license) or something that they have knowledge of (e.g. knowledge based Q&A). A minimum of userID and password is sufficient for authentication and are to be in compliance with current commonwealth password policies (ITP-SEC007 *Minimum Standards for User IDs and Passwords*). This level is generally sufficient for most online interactions.

LOA P3: Identity for which there is a high degree of confidence in who the *person* behind the identity is. The identity proofing process for this level requires verification of the identifying materials and information. LOA P3.0 requires multi-factor authentication.

LOA P4: Identity verification must include face-to-face, in-person proofing. The authentication process must include token-based multi-factor authentication (something the user possesses).

The identity verification process and the derived outcome for LOA's 2, 3, and 4 shall be valid for a period of three (3) years from the date of the verification action (effective date). Current LOA and effective date will be stored in the user account record in the Directory.

Use:
In determining the appropriate level of assurance to engage for an application or system, the agency must perform a risk assessment and evaluate **the potential harm or impact** resulting from access by an unverified or erroneous identity as well as **the likelihood** of such harm or impact actually occurring.

Categories of harm and impact include[1]:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive or private information
- Personal safety
- Civil or criminal violations

By assigning potential impact values to these categories – Low, Moderate ("Mod"), High ("N/A" if there is no potential impact) the following table can provide guidance as to the necessary assurance level

	Assurance Level Needed			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive or private information	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

[1] For an example see, OMB M-04-04: *E-Authentication Guidance for Federal Agencies* and FIPS 199: *Standards for Security categorization of Federal Information and Information Systems* for detailed discussion.

The level of assurance needed is determined by the *highest* impact rating. For example, if five of the above categories call for a Level 1, but the remaining one calls for a Level 2, the then application would require Level 2.

Example 1: If an application that is only serving up publicly available information (e.g. State Park schedules) the likely evaluation of the application is as follows since the information is in the public domain. Comparing this to the above we can conclude that an assurance level 1 credential (i.e. no identity verification) is adequate.

Category	**Evaluation**
Inconvenience, distress, or damage to standing or reputation	Low
Financial loss or agency liability	Low
Harm to agency programs or public interests	N/A
Unauthorized release of sensitive or private information	N/A
Personal safety	N/A
Civil or criminal violations	N/A

Example 2: If an application contains background check information, a user wants to know who is trying to access the application and that they are authorized to do so. Financial information, criminal violations, etc. are potentially available in such an application and the user might evaluate it as follows. This would require an assurance level 3 as determined by the "Unauthorized release…" and "Civil or criminal violations" categories.

Category	**Evaluation**
Inconvenience, distress, or damage to standing or reputation	Mod
Financial loss or agency liability	Mod
Harm to agency programs or public interests	Low
Unauthorized release of sensitive or private information	Mod
Personal safety	N/A
Civil or criminal violations	Mod

7. Responsibilities

Agencies under the Governor's Jurisdiction: Determine and categorize access to their applications and systems per the guidance provided herein.

8. Related ITPs/Other References

- OMB M-04-04 - *E-Authentication Guidance for Federal Agencies*
- NIST SP 800-63-2 - *Electronic Authentication Guide*
- FIPS 199 - *Standards for Security categorization of Federal Information and Information Systems*
- National Strategy for Trusted Identities in Cyberspace (NSTIC)
- *NSTIC Strategy*
- Identity Ecosystem Steering Group (IDESG)
- Federal Identity, Credential, and Access Management (FICAM)
- State Identity, Credential, and Access Management (SICAM)
- ITP-SEC007 - Minimum Standards for User IDs and Passwords

9. Authority

Executive Order 2011-05 - *Enterprise Information Technology Governance*

10. Publication Version Control

It is the user's responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

11. Exemptions and Waivers

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 a waiver is to be completed and submitted via the Commonwealth of Pennsylvania Policy and Procurement Action Request (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	02/10/2016	Base Policy