

<p><b>New York State          Information Technology Best          Practice Guideline</b></p>	<p><b>No:</b> NYS-G07-001</p>
<p><b>Guideline Name:          Identity and Access          Management: Trust          Model</b></p>	<p><b>Effective Date:</b> 01/05/2007</p> <p><b>Issued By:</b>          Melodie Mayberry-Stewart          State Chief Information Officer          Director Office for Technology</p> <p><b>Published By:</b>          Enterprise Strategy &amp; Acquisitions Office</p>

## **1.0 Purpose and Benefits of the Guideline**

In the past, computer systems typically were used by a small set of **users**, within a single agency. Today's computer systems are used by a wide variety of people including citizens and business partners and across various agencies and geographical areas. The Internet has been a major driver of this change by enabling citizens to remotely access agency systems and transact business directly with government. This trend is expected to continue.

Trust in the security of information exchanged over the Internet and other networks during **transactions** will play a vital role in the future. Government must address the issues of user authentication, confidentiality, and integrity of data transferred, and the ability to hold transacting parties accountable when necessary. Thus, solutions that provide this type of

protection are critical components of an organization's information security program. Trusting the identity of users is an important part of such a solution.

Traditionally this is achieved by issuing individual **user**-ids for individual systems. However, the increased number of systems and growing number of **users** has made this approach impractical and insecure. We must move towards an Identity and Access Management (IAM) solution where one **credential** issued to a user can be trusted across systems. A Trust Model is a key element of this solution because it establishes the framework and rules that allow for identity credentials to be trusted across organizations.

In order for **information owners** to be able to trust **credentials** that have been issued to **users**, the **credentials** must have been issued, protected and managed according to some documented, consistent, and agreed on rules. This document outlines these rules, and documents the steps required in the process. In particular it:

- Defines the processes to establish identities and manage credentials;
- Defines the levels of **trust**; and
- Provides detailed procedures to map the identity and credential management processes to the various trust levels.

This model is based on a number of sources, mainly [the E-Authentication Guidance for Federal Agencies](#), issued by the Office of Management and Budget on December 16, 2003 and [NIST 800-63 Recommendation for Electronic Authentication](#), issued September 2004. **Compliance with existing Federal standards represented by these two documents is critical if NYS systems are to continue to interface with, and NYS users use, Federal and other State's systems.**

!	<i>The Personal Privacy Protection Law, Article 6-A of the New York State Public Officers Law, governs the collection or disclosure of personal information by State agencies. Personal information is any information about a person that can be used to identify that person. Section 94 (1) of the Public Officers Law authorizes a State agency to maintain in its records only personal information that is relevant and necessary to either accomplish a purpose required to be accomplished by statute or executive order or to implement a program authorized by law. Nothing in this Trust Model authorizes the collection or disclosure of personal information where such is prohibited or restricted by the Public Officers Law or other provision of law.</i>
---	--

## 2.0 Enterprise IT Policy Statement

---

Details regarding the authority to establish enterprise IT guidelines, policies and standards can be found [in NYS CIO/OFT Policy NYS-PO8-002, Authority to Establish State Enterprise Information Technology \(IT\) Policy, Standards and Guidelines.](#)

Details regarding the criteria for establishing enterprise IT standards can be found in [NYS P02-001, Process for Establishing & Implementing Statewide Technology Policies & Standards.](#)

## 3.0 Scope of the Guideline

---

This Trust Model is applicable to all systems and networks owned and operated by or on behalf of *state entities (SE) and other* New York State (NYS) government agencies which choose to comply. It applies to *SE*, staff and all others, including outsourced third parties, local government staff<sup>1</sup>, which have access to or manage *SE information*. Where conflicts exist between this Trust Model and a *SE's* policy standard, the more restrictive will take precedence. This Trust Model encompasses all *systems* for which the *state* has administrative responsibility, including *systems* managed or hosted by third parties on behalf of the *SE*. It addresses all *information*, regardless of the form or format, which is created or used in support of business activities of *state entities*. This Trust Model must be communicated to all staff and all others who have access to or manage *SE information*.

NYS reserves the right to remove access from NYS workforce, third parties, or any user(s) including local government workforce whose activities or practices jeopardize the confidentiality, integrity, and availability of NYS *systems, information, or physical infrastructure*.

***A restricted version of the NYS Trust Model contains specific security standards and is available through NYS agency CIOs on a need-to-know basis.***

---

<sup>1</sup> This Trust Model only applies to local governments as far as they or their workforce access state entity government networks or systems. It does not apply to networks and systems owned and operated by local governments for local government purposes.

## 4.0 Guideline Statement

---

### TRUST MODEL REQUIREMENTS

---

#### Part 1. Overview

For the purposes of IAM and the granting of access (authorization), two elements must be considered:

- the **classification** of the information; and
- what actions will be performed on the information (the **transaction** type).

These two elements will indicate the degree of trust required of the **user's** identity. As an example, 'read' access to publicly available information may require limited verification of the **user's** identity; however, *changing* the information could require a higher degree of verification. Read access to clinical or police records may also require a high degree of verification.

#### Part 2. Process Steps

**Trust** in a **credential** is established by:

- the *vetting process* used to establish the identity of the individual to whom the **credential** was issued; and
- the confidence that the individual who uses the **credential** is the individual to whom it was issued.

Therefore, each step of the process that establishes an identity and manages a **credential** contributes to the trust level. From registration, to issuing **credentials**, to using the **credential** in a well-managed secure application, to record keeping and auditing, each step must meet the minimum standards for a given trust level to avoid compromising the entire process and undermining trust in the **credential**.

The following process steps have been defined and shall be implemented by state entities.

<i>Process Step</i>	<i>Description of step</i>
1. Trust level	Process by which <b>Information Owner</b> assesses the risks, potential

classification

impacts and required trust level to adequately maintain the privacy and security of the information and reduce risk inherent in the transaction. The criteria for determining the trust level required are defined in [Part 9](#).

---

2. Credential issuance	
2.1. Registration	<p>Process by which the <b>user</b> provides sufficient evidence to the <b>credential</b> issuer who <b>independently verifies</b> that the <b>user</b> is who (s)he claims to be.</p> <p>Agencies should be aware that under the Personal Privacy Protection Law (PPPL),<sup>2</sup> they can only collect and maintain personal information that is relevant and necessary to accomplish a purpose authorized by statute or executive order or to implement a program authorized by law. The <b>SE</b> should consult with its counsel's office and knowledge program managers to determine how the PPPL applies in its specific circumstance.</p>
2.2. Issuance	<p>Process by which the <b>credential</b> issuer securely provides to the <b>user</b> their <b>credential</b> and any <b>authentication</b> tokens that are required.</p>
3. Authentication	<p>Process by which the <b>user</b> provides information to establish the validity of the <b>credential</b>. Authentication requirements are defined for <b>remote access to systems</b> and non-remote access later in this document.</p>
4. Management	
4.1. Re-certification	<p>Process by which the <b>credential</b> issuer periodically re-evaluates the status of the <b>user</b> and the validity of his or her associated <b>credential</b>.</p>
4.2. Revocation	<p>Process by which the <b>credential</b> issuer promptly cancels the <b>credential</b> in the event of a change of the <b>user's</b> status<sup>3</sup>.</p>
4.3. Auditing	<p>Process by which the <b>credential</b> issuer reviews the credential issuing process, including the activities of those involved in the registration process, to ensure that <b>credentials</b> are issued in compliance with this Trust Model and identify any irregularities</p>

---

<sup>2</sup> Article 6-A of the New York State Public Officers Law, governs the collection or disclosure of personal information by State agencies.

<sup>3</sup> Examples of change of status include: employment; trust level; upon transfer of ownership of the credential to another issuer.

or security breaches.

---

4.4. Re-assigning authentication	Process by which <b>authentication</b> tokens are reset should the <b>user</b> lose/forget either their <b>credential</b> or associated authentication tokens.
----------------------------------	--

### Part 3. Trust Level Classifications

An appropriate **trust** level for **user credential** and **authentication** must be assigned and implemented to protect the integrity and confidentiality of the **information** and validity of **transactions**.

The four trust levels supported by this Trust Model are:

<i>Level</i>	<i>Description</i>
1	Little or no confidence in the asserted identity's validity.
2	Confidence exists that the asserted identity is accurate.
3	High confidence in the asserted identity's validity.
4	Very high confidence in the asserted identity's validity.

**Information Owners** assign trust levels based on the sensitivity of the information and nature of the transactions performed on the information. The determination of the trust level required, and full definitions are defined in [Part 9](#).

### Part 4. Credential Requirements (TCRs)

For each of the process steps defined in Part 2 (Process Steps), we have defined Trust Level Specific **Credential** Requirements (TCRs). These are **minimum** levels; **credential** issuers can impose more rigorous requirements, but other issuers cannot be required or expected to comply with them.

!	Please note that for all Trust levels, <b>except</b> Trust level 4, registration can be performed through a <b>trusted organization</b> attesting to the identity of a prospective user based on the criteria required for that Trust level. In such case, the identity proofing process may be able to leverage a pre-existing relationship or process (e.g., if an entity's human resources process for new employees and contractors meets or exceeds the registration requirements for a Trust level 2, that entity can
---	---

register those **users** by simply attesting to their identity.

### Section 4.1 TCR definitions

Process step (see part 2)	TCR			
	1 (Low)	2 (Medium)	3 (High)	4 (Very High)
1 Trust level classification	<i>Little/no confidence in asserted identity.</i>	<i>On balance, confidence exists that the asserted identity is accurate.</i>	<i>Transactions needing high confidence in the asserted identity's accuracy</i>	<i>Transactions needing very high confidence in the asserted identity's accuracy</i>
2 Credential issuance		Records of the <b>credential</b> issuance process, including steps taken and copies of any documents examined to verify the <b>user's</b> identity, shall be maintained. Registration and issuance records are retained for seven (7) years and six (6) months beyond the expiration or revocation (whichever is later) of the <b>credential</b> . <sup>4</sup>		Registration and issuance records are retained for ten (10) years and six (6) months beyond the expiration or revocation (whichever is later) of the <b>credential</b> . <sup>5</sup>
2.1 Registration	Self selected by <b>user</b> .	<b>User</b> provides full legal name, and at least one piece of uniquely identifiable information that has been issued by State/Federal government (examples provided in Section 5.1  <b>User</b> -supplied identification information is <b>independently verified</b> through a record check to be on balance valid and consistent. If registration is in person through a visual inspection of a photo-id, the above verification is <b>not</b> required.  OR  A <b>trusted organization</b> attests to the identity of a prospective <b>user</b> based on the above criteria.	<b>User</b> provides full legal name, current address of record and two pieces of valid and unexpired identification ( <b>certified copies</b> or originals) as detailed in <b>Part 5 Section 2</b> .  <b>User</b> -supplied identification information is <b>independently verified</b> through a record check of personnel records, credit records or other comparable databases for validity and consistency.  OR	<b>User</b> provides full legal name, current address of record and personal presentation of two pieces of valid and unexpired identification ( <b>certified copies</b> or originals) as detailed in Section 5.1  <b>User</b> -supplied identification information is <b>independently verified</b> through a record check of personnel records, credit records or other comparable databases for validity and consistency.
2.2 Issuance	N/A- self selected by <b>user</b>	Issue credential to <b>user</b> through delivery channel requested during registration and send notice to address of record.	Issued to <b>independently verified</b> destination. Where multiple elements are required (e.g. <b>user</b> -id and password) they will be issued separately.	Physical, face-to-face delivery of <b>credentials</b> to <b>user</b> , evidenced by <b>all</b> of the following: <ul style="list-style-type: none"> <li>• A record of the date and time of verification and a signed declaration by the person performing the identification that (s)he verified the <b>user's</b> identity;</li> <li>• The biometric of the <b>user</b> (photograph/fingerprint);</li> </ul>

<sup>4</sup> These records retention requirements are based on Federal standard established in [NIST 800-63 Recommendation for Electronic Authentication](#). However, State agencies may not dispose of any records without disposition authorization from State Archives, State Education Department, consistent with provisions of Section 57.05 of Arts and Cultural Affairs Law.

<sup>5</sup> Ibid.

Process step (see part 2)	TCR			
	1 (Low)	2 (Medium)	3 (High)	4 (Very High)
				<ul style="list-style-type: none"> <li>The <i>user's</i> declaration of identity under penalty of perjury, signed with a handwritten signature in the presence of the person performing the identity authentication</li> </ul>
3 Authentication	These are minimum levels of authentication. More robust forms of authentication can be substituted. See Part 6. for definitions and technical requirements. Standards for each authentication methods for described below are available to authorized individuals through the Office of the Chief Information Officer (OCIO)			
<i>Remote access</i>	Self selected <i>user</i> -PIN	Password as defined in Section 6.2	Dual factor <i>authentication</i> and other appropriate controls	Dual factor <i>authentication</i> and other appropriate controls
Non-remote access	Self selected <i>user</i> -PIN	Password as defined in Section 6.2	Password as defined in Section 6.2	<ul style="list-style-type: none"> <li>Dual factor <i>authentication</i> using a password and other appropriate controls</li> </ul>
4 Management				
4.1 Re-certification	Not required	1 year	1 year	3 months
4.2 Revocation	Not required	<i>Credential</i> issuer revokes <i>credential</i> within appropriate time of being notified of change of <i>user's</i> status.	<i>Credential</i> issuer revokes <i>credential</i> within appropriate time of being notified of change of <i>user's</i> status.	<i>Credential</i> issuer revokes <i>credential</i> within appropriate time of being notified of change of <i>user's</i> status.
	<i>Credentials</i> may also be revoked at any time at the discretion of the <i>credential</i> issuer.			
4.3 Auditing	Not required	Audit logs maintained and reviewed in compliance with CSCIC log requirements. <sup>6</sup>	Audit logs maintained and reviewed in compliance with CSCIC log requirements.	Audit logs maintained complying with CSCIC log requirements. Proactive review for unusual credential issuance activities. Review for unauthorized <i>user</i> activity.
4.4 Re-assigning authentication	N/A- <i>user</i> will re-register. <sup>7</sup>	Verification of identity for token reset through ' <i>shared secret</i> '	Authentication token reset and re-issued pursuant to TCR 2.2	Authentication token reset and re-issued pursuant to TCR 2.2

## Section 4.2 Mandatory implementation of TCRs

**Deviation from strict compliance to the TCRs could cause serious security concerns. Therefore, adherence to these trust levels is mandatory.** However, it is realized that different working practices may evolve over time. Where a working practice deviates from the TCR, the practice must be documented and agreed to by the **management authority** for this Trust Model before the practice is implemented.

<sup>6</sup> NYS Office of Cyber Security and Critical Infrastructure Coordination, Cyber Security Policy P03-002 V2.0 rev. April 4, 2005

<sup>7</sup> System designer may offer password memory hint question, but not required.

## Part 5. Trusted Identification

This Part of the Trust Model defines the documents that may be used in the registration process. The Trust Model does *not* mandate that all the document options must be offered in an IAM implementation.

### Section 5.1 Trust level 2

Serial number from any of the following documents is required for Trust level 2 registration:

- unexpired and valid U.S. Passport;
- unexpired and valid driver's license or ID card (issued by a state or outlying possession of the United States);
- unexpired and valid ID Card issued by US Federal, NY State or NY local government agency or entity;
- unexpired and valid social security card;
- unexpired and valid voter's registration;
- unexpired and valid military dependent's ID;
- unexpired and valid US Coast Guard Merchant Mariner ID;
- unexpired and valid Native American tribal document.

With prior approval by the **management authority**, users can be registered remotely (Internet, postal mail or telephone) at Trust Level 2 through verifying the details of the claimed identity using either:

- credit records or similar databases that **independently verify** the claimed identity exists and is consistent with identity and address information provided; or
- presentation of a valid credit or non-prepaid bank card number, using an address of record for the card number, which is consistent with the address information provided.

### Section 5.2 Trust level

!	<b><i>The classes of identification documents are listed below. All forms of identification must be valid and unexpired.</i></b>
---	--

The following identifies minimum requirements for Trust level 3/4 accounts.

To meet the Security Level 3/4 requirements, the applicant must provide:

One (1) Class A document with a picture PLUS one (1) Class A, Class B or Class C document

OR

Two (2) Class B documents, at least one (1) of which must have a picture.

The classes of identification are those set forth below.

Class A:

- U.S. Passport, with photograph and name of the individual;
- driver's license or ID card issued by a state or outlying possession of the United States with photograph and name of the individual;
- ID Card issued by US Federal, NY State or NY local government agency or entity, with photograph and name of the individual.

Class B:

- social security card;
- voter's registration card;
- military dependent's ID card;
- US Coast Guard Merchant Mariner card;
- Native American tribal document;
- driver's license issued by a Canadian government authority;
- foreign passport with I-551 stamp or attached INS Form I-94 indicating unexpired employment authorization;
- Alien Registration Receipt Card with photograph (INS Form I-151 or I-551);
- Temporary Resident Card (INS Form I-688);
- Employment Authorization Card (INS Form I-688A);
- Reentry Permit (INS Form I-327);

- Refugee Travel Document (INS Form I-571);
- Employment Authorization Document issued by the INS which contains a photograph (INS Form I-688B).

Class C:

Any form of identification with the person's name, which can be verified including a:

- credit or bank card that is verified to be currently valid; or
- current credit check to a recognized resource that confirms the information on the primary photo-ID; or
- student ID that is verified to be current and valid.

## **Part 6. Authentication**

This Part describes and provides technical specifications for the various types of tokens used to authenticate **users** based on the requirements for each Trust Level outlined in Part 4.

The tokens described in this Part are in ascending order of robustness, e.g. a software token is a more robust form of authentication than a password.

### **Section 6.1 User selected PIN**

A pin is selected by the user.

### **Section 6.2 Password**

A password is secret character string that a claimant memorizes and uses to authenticate his or her identity. Passwords must ensure adequate **entropy**.

### **Section 6.3 Soft token**

A soft token is a cryptographic key that is typically stored on disk or some other media. Authentication is accomplished by proving possession and control of the key. The soft token shall be encrypted under a key derived from a password known only to the **user**, so knowledge of a password is required to activate the token. The cryptographic module used with the soft token shall be validated to FIPS 140-2<sup>8</sup>. Each authentication shall require entry of the password and the unencrypted copy of the authentication key shall be erased after each authentication.

---

<sup>8</sup> Security Requirements for Cryptographic Modules (FIPS PUB 140-2), May 24, 2001 (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>).

## Section 6.4 One-time password device token

A one-time password device token is personal hardware device that generates “one time” passwords for use in authentication. The device may or may not have some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port). The passwords shall be generated by using a FIPS approved block cipher or hash algorithm to combine a symmetric key stored on a personal hardware device with a **nonce** to generate a one-time password. The nonce may be a date and time, or a counter generated on the device, or a challenge sent from the verifier (if the device has an entry capability). The device shall be validated to FIPS 140-2<sup>9</sup>. The one-time password typically is displayed on the device and manually input (direct electronic input from the device to a computer is also allowed) to the verifier and as a password.

## Section 6.5 Hard token

A hard token is hardware device that contains a protected cryptographic key. Authentication is accomplished by proving possession of the device and control of the key. Hard tokens shall:

- require the entry of a password or a biometric to activate the authentication key;
- not be able to export authentication keys;
- be FIPS 140-2<sup>10</sup> validated:
  - overall validation;
  - physical security.

## Part 7. Protection of authentication information

Authentication information cannot be transmitted or stored in clear text. All encryption or hashing algorithms used to meet this requirement must be approved by a NY State or Local government ISO as approved by the **management authority**.

## Part 8. Credentials

### Section 8.1 Credential Types

Each **credential** is to be categorized according to the purpose (personal, business, or government) for which it was created.

---

<sup>9</sup> Security Requirements for Cryptographic Modules (FIPS PUB 140-2), May 24, 2001 (<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>).

<sup>10</sup> Ibid.

- Government (G) - An account held by employees of Federal, State or Local government or political subdivisions for the purpose of conducting tasks related to their employment
- Business (B) - An account used for the purpose of conducting business with NYS Government on behalf of a business, being either the **user's** employer or the legal entity under which the **user** conducts business
- Personal (Individual) (P) - An account held by an individual that is for personal use, which is to be used to conduct personal business with NYS Government

### Section 8.2 Individual accountability of credentials

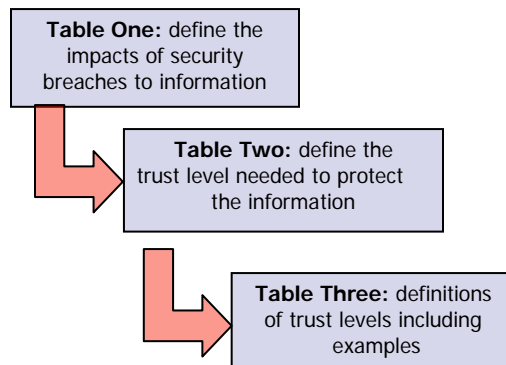
For accountability purposes, no **credentials** are to be shared, i.e. they are to be associated with an individual, not a group, and they are not to be shared among multiple **users**.

### Section 8.3 Uniqueness of User IDs

**User IDs** shall be unique. Therefore, **User IDs** may not be reused and will be archived when the user is **deprovisioned**.

## Part 9. Assigning Trust Levels

This section explains how risks to information are defined (*section 1*), by assessing the security levels needed to protect the information based on the information classification and what actions will be performed on the information (the transaction type). In doing this, both the likelihood and type of risk (*section 2*) must be assessed before being mapped to the necessary 'trust' levels (*section 3*). All tables in this Part are



based on [OMB M-04-04 E-Authentication Guidance for Federal Agencies](#), NYS Policy and Standards related to Information Classification can be obtained from the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC).

## Section 9.1 Risk of Authentication Errors

### 9.1.1 Impact

To determine the appropriate level of criticality and sensitivity, the *information owner* must first assess the potential impact an authentication error would have. Categories of potential impact include:

- Inconvenience, distress, or damage to standing or reputation;
- Financial loss
- Harm to agency programs or public interests;
- Personal safety;
- Civil or criminal violations; and
- Information Classification.

Potential impact is categorized as:

- Low impact;
- Moderate impact; or
- High impact.

Definitions of categories and impacts are outlined in [Table 1](#).

TABLE 1

Potential Impacts of Authentication Errors

Category	Potential Impact Level		
	Low	Moderate	High
<i>Inconvenience or distress.</i>	At worst, limited, short-term inconvenience or distress to any party.	At worst, serious short term or limited long-term inconvenience or distress to any party.	Severe or serious long-term inconvenience or distress to any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).
<i>Financial loss</i>	At worst, an insignificant or	At worst, a serious unrecoverable	Severe or catastrophic

	inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.	financial loss to any party, or a serious agency liability.	unrecoverable financial loss to any party; or severe or catastrophic agency liability.
<i>Harm to agency programs or public interests:</i>	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with <i>noticeably</i> reduced effectiveness, or (ii) minor damage to organizational assets or public interests.	At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with <i>significantly</i> reduced effectiveness; or (ii) significant damage to organizational assets or public interests.	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.
<i>Personal safety</i>	At worst, minor injury not requiring medical treatment.	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.	A risk of serious injury or death.
<i>Civil or criminal violations</i>	At worst, a risk of civil or criminal violations of a	At worst, a risk of civil or criminal violations that	A risk of civil or criminal violations that are of special

	nature that would not ordinarily be subject to enforcement efforts.	may be subject to enforcement efforts.	importance to enforcement programs.
<i>Information Classification</i> <sup>11</sup>	The unauthorized access or disclosure of information would have <b>minimal or no impact</b> to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized access or disclosure of information could have only <b>limited impact</b> to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized access or disclosure of information could <b>severely impact</b> the organization, its critical functions, employees, third party business partners and/or its customers.
<i>Confidentiality</i>			
<i>Integrity</i>	The unauthorized modification or destruction of information would have <b>minimal or no impact</b> to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized modification or destruction of information would have only <b>limited impact</b> to the organization, its critical functions, employees, third party business partners and/or its customers.	The unauthorized modification or destruction of information could <b>severely impact</b> the organization, its critical functions, employees, third party business partners and/or its customers.

A risk analysis is to some extent a subjective process, in which the **information owner** must consider harms that might result from, among other causes, technical failures, malevolent third parties, public misunderstandings, and human error. The **information owner** should consider a wide range of possible scenarios in seeking to determine what potential harms

---

<sup>11</sup> NYS Policy and Standards related to Information Classification can be obtained from the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC).

are associated with their business process. It is better to be over-inclusive than under-inclusive in conducting this analysis.

9.1.2 Likelihood

The **Information owner** must also determine the likelihood that a risk will materialize and the impact occur. There are many ways to determine the likelihood of an impact. The **Information owner** should consider the nature and capability of the threat, nature of the vulnerability, existence and effectiveness of current controls, and past history. Regardless of the method used, likelihood should be defined in concrete terms such as impacts are likely to occur daily, weekly, yearly, every decade, or “once in a career.” After determining likelihood a higher or lower Trust level may be required (see Table 2).

**Section 9.2 Determine Assurance (Trust) Level**

**Information** will be classified by the **information owner** based on its value, sensitivity, consequences of loss or compromise, and/or legal and retention requirements. Associated authentication requirements will be based on the **information** classification together with any other requirements of the **information/transaction** (e.g. regulatory or to reduce the risk of repudiation) being processed.

Map the potential impacts (Low, Moderate or High) defined in Table 1 to the four trust levels (1, 2, 3, 4) contained in Table 2 below. This will identify the level of trust required. Minimum requirements for the various processes associated with each trust level are contained in Part 4. Additional security controls should also be implemented for higher trust levels (e.g. audit logging, data authentication, granularity **access** rights, data validation and verification controls, user **authentication**).

TABLE 2

Trust level determination

Category	Required trust level			
	1	2	3	4
<i>Inconvenience or distress</i>	Low	Mod	High	High
<i>Financial loss</i>	Low	Mod	Mod	High
<i>Harm to agency Programs or public interests</i>	N/A	Low	Mod	High
<i>Personal safety</i>	N/A	N/A	Low	Mod/High
<i>Civil or criminal violations</i>	N/A	Low	Mod	High

<i>Information Classification</i>	<i>Confidentiality</i>	Low	Mod	High	High
	<i>Integrity</i>	Low	Mod	High	High

### Section 9.3 Trust classifications

To help protect the **confidentiality** and to assure the **integrity** of **information**, the **information owner** must determine the degree of verification (or **trust**) needed for **users** to perform **transactions** using that **information**. For example, the current national security alert status (blue, yellow, amber or red) is public information, however the transaction to *change* the rating (information **integrity**) must be tightly controlled.

Table 3 provides further information regarding the four identity **trust** levels for **users** performing **transactions** upon **information**.

**Credentials** are assigned to **users** based on the level of trust required by the sensitivity of the information and the nature of the transaction.

**TABLE 3**

Information Sensitivity - Trust level Classification

<i>Trust Level</i>	<i>Description</i>	<i>Typical users</i>
1	Little or no confidence in the asserted identity's validity.	<p>Level 1 is appropriate when the exposures associated with identity are minimal. Such a credential could be used to customize a web page or participate in a discussion group.</p> <p>Level 1 can be used for transactions where a specific identity is not critical but some assurances are necessary that the same <b>user</b> is accessing a system. For example a Level 1 <b>credential</b> is issued when a user registers to receive routine e-mail notifications or newsletters. A self-selected Level 1 user-id could be used to access the user profile that determines what types of notifications are sent. In such a case, the exposures are very low and the <b>information owner</b> only needs some minimum assurance that the same <b>user</b> that created the profile has changed it.</p> <p>Level 1 can also be used in some instances where identity is not critical at the first interaction between an agency and a <b>user</b> but is assured at a subsequent stage in the process. For example, a Level 1 credential is required for a <b>user</b> to submit an initial request for a government service where later in the application process or to actually receive the service</p>

		he or she is required to personally appear, fill out additional forms, or provide more detailed personal information. In this case, the Level 1 credential can be used to track the progress of the application.
2	On balance, confidence exists that the asserted identity is accurate.	<p>A Level 2 credential is appropriate for transactions that require a previously verified identity assertion. Level 2 is appropriate where there is only a moderate risk of unauthorized release of personal information; the impact of inaccurate information would have only moderate impact on the submitting user. This level will likely be sufficient for most e-government transactions.</p> <p>For example, a user could use a Level 2 credential to submit an application or information such as a tax return or permit application where an assertion of identity and certification of accuracy of submitted information is important. It could be used to update or change previously submitted information.</p>
3	High confidence in the asserted identity's validity.	<p>A Level 3 credential can be used without the need for additional identity assertion controls for transactions that may involve significant risk. A government employee could use a Level 3 credential to access information at a "High" classification level or for a contractor to provide similarly sensitive <b>information</b> or remotely access government resources. It is appropriate for transactions that may involve significant financial exposure such as a large procurement.</p>
4	Very high confidence in the asserted identity's validity.	<p>A Level 4 credential is appropriate for access to highly restricted resources and for transactions that have a significant risk to health or safety, or a significant impact on an agency's operations. The following are examples of situations in which a Level 4 credential may be appropriate:</p> <ul style="list-style-type: none"> <li>• Law enforcement access to a database containing criminal records. Unauthorized access could raise privacy issues or compromise an investigation;</li> <li>• Critical medical transaction such as dispensing a controlled drug, entering a diagnosis that might result in a medical procedure, accessing patient medical records;</li> <li>• Upgrading a Level 3 credential to a Level 4 credential.</li> </ul>

!	There is a natural tendency to require the highest levels of <b>trust</b> , however higher
---	--

	<p>trust level credentials take longer to issue and will be more expensive to implement and manage. It may also deter citizens from using the <b>systems</b>.</p> <p>Careful design of the business processes, with steps to validate and verify data with independently collected information, may allow lower trust levels to be used. An example could be the on-line collection of tax returns. With no independent verification of the tax data provided, a high trust level (typically level 3) would probably be required. With verification of data to independent sources (e.g. key elements of previous years tax returns), a lower trust level (e.g. level 2) may be deemed appropriate.</p>
--	---

In summary, to determine the required trust level, the **information owner** must classify the information and identify exposures inherent in the transaction process, using the impacts and categories as defined in Table 1.

The **information owner** should then map the potential impact category outcomes to the trust level, choosing the lowest level of trust that will cover all of the potential impacts identified (as defined in Table 2). Thus, if five categories of potential impact are appropriate for Level 1, and one category of potential impact is appropriate for Level 2, the transaction would require a trust Level 2 **credential**. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, the information should be mapped to the risk profile identified under Level 4, even if other consequences are minimal.

In analyzing potential exposures, the **information owner** must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or impacts to more than one person.

## 5.0 Policy Compliance

---

Not Applicable.

## 6.0 Definitions of Key Terms

---

A complete listing of defined terms for NYS Information Technology Policies, Standards, and Best Practice Guidelines is available in the "NYS Information Technology Policies, Standards, and Best Practice Guidelines Glossary" at: <http://www.cio.ny.gov/policy/glossary.htm>.

The following defined terms are used in this Guideline.

**Authentication** Confirming a **user's** claim of identity. Authentication tokens are something that a **user** possesses and controls that can be used to authenticate the **user**. There are three main factors of authentication, as described below with examples of each:

- *Something you know:* (e.g. user-id, passcode, memorized personal identification number (PIN) or password);
- *Something you have:* something you own (e.g. a secure authentication token, Smart card, a one-time password); and
- *Something you are:* biometrics (e.g., finger-print, retina scan).

Dual factor (or strong authentication): An authentication scheme using two independent factors, e.g. something you know and something you have.

**Certified copy** A duplicate of an original official document, certified as an exact reproduction by the officer responsible for issuing /keeping the original..

**Clear text** Any message or text that is not rendered unintelligible through an encryption or hashing algorithm.

**Credential** An object that is verified when presented to the verifier in an authentication transaction. A common **credential** is a **user-id** and associated password.

**Confidentiality** "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..." [44 U.S.C., Sec. 3542] A loss of **confidentiality** is the unauthorized disclosure of information.

**Deprovision** The act of retiring a user's identity and terminating his or her access to IT systems and services.

**Entropy** A measure of the amount of uncertainty that an attacker faces to determine the value of a secret such as a password. Entropy is usually stated in bits. See NIST 800-63 Recommendation for Electronic Authentication.

**Independently verified**

Information provided by a **user** is verified to a source that is independent of the **user** (most often a trusted database) that the claimed identity exists and is consistent with the identity and address information provided. An **independently verified** destination is where **credentials** and tokens are issued

or renewed in a manner that binds the verified **user** with an independently verified

- postal address of record of the **user** (for example, by mailing an authenticator to the address of record);
- telephone number of the **user** (for example, by requiring a call from or to the applicant's telephone number of record).

**Information** Any *information* created, stored in temporary or permanent form, filed, produced or reproduced by, regardless of the form or media. *Information* shall include, but not be limited to:

- Personally identifying information;
- Reports, files, folders, memoranda;
- Statements, examinations, transcripts;
- Images; and
- Communications.
- If *information* is already legally in the public domain (e.g. under FOIL), it can be considered as 'public' information. As such security controls are not required to maintain its confidentiality.

#### **Information Classification**

- See Table 1

#### **Information owner**

An individual or organizational unit responsible for making classification and control decisions regarding use of *information*.

#### **Integrity**

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity..." [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information.

- *Authenticity* - A third party must be able to verify that the content of a message has not been changed in transit.
- *Non-repudiation* - The origin or the receipt of a specific message must be verifiable by a third party.

- *Accountability* - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

#### **Management authority**

The entity authorized by the NYS Chief Information Officer (CIO) to implement, manage, and interpret this Trust Model.

#### **Nonce**

A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.

#### **Physically secured area.**

Area that is secured by an access control systems (ACS) comprising the following requirements. The ACS will:

- Require dual factor authentication to access;
- Be designed to prevent abuse of the system, for example: 'Tailgating'; and rendering the system inoperable (by wedging doors open);
- hold a record of those allowed access;
- print a list of those allowed entry to the room;
- print a log of all those who enter the secure area;
- If the device relies on physical tokens (such as magnetic cards) it should be possible *at any time* to account for the location of all such tokens;
- 'fail-safe' in the event of failure.

**Remote access** Any access coming into the NYS government's network from outside the NYS private, trusted network. **Any and all wireless networks are considered remote access.**

**Shared Secret** In the context of this Trust Model a "shared secret" refers to secret information shared by a **user** for the purpose of confirming that user's identity. Shared secrets are often used to authenticate a **user** for the purposes of conveying a credential or resetting a **credential** such as a password.

#### **State [Government] Entity (SE)**

shall have the same meaning as defined in Executive Order No. 117, first referenced above; and shall include all state agencies, departments, offices, divisions, boards, bureaus, commissions and other entities over which the Governor has executive power and the State University of New

York, City University of New York and all public benefit corporations the heads of which are appointed by the Governor; provided, however, that universities shall be included within this definition to the extent of business and administrative functions of such universities common to State government.

**System** An interconnected set of *information* resources under the same direct management control that shares common functionality. A system normally includes hardware, software, applications, and communications.

**Third parties ('Non-Government workforce')**

Anyone directly or indirectly providing goods and services to the *SE* who is not under the direct control of the government entity (see *workforce* below). Such personnel are typically not subject to the rigorous selection and screening processes that apply to the government workforce.

In addition, by their very nature, services provided by non-government workforce are typically of a short-term nature, focusing on clearly defined and narrow roles and responsibilities. This means that without impacting their overall effectiveness, their 'need-to-know' Agency information assets can be similarly defined and restricted.

**Transaction** A discrete event between *user* and systems that supports a business or programmatic purpose. Typical *transaction* types are: Read; Write; Execute (a program); Purge.

**Trust** Trust is defined as:

- the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the *credential* was issued,
- the degree of confidence that the individual who uses the *credential* is the individual to whom the *credential* was issued.

**Trusted organization**

A State, local or Federal government entity with which the state entity has established a business relationship to issue *credentials* through a service level agreement, memorandum of understanding or other comparable mechanism, or, a private entity that has a similar contractual relationship with the government entity. The process for issuing *credentials* must be clearly documented and agreed by the Trust Model's *management authority*.

The definitions for the following terms apply for this guideline only:

**User** Any individual using a state provided **system** for a legitimate government purpose.

**Note: this definition is changed from the usual definition of a ‘user’ since it specifically includes members of the public.**

**User ID** The unique name that identifies a **user** on a system or network. User IDs are unique on to a given system or network- no two users can have the same user ID. A user ID is also known also usernames or account names.

**Workforce** State employees—and other persons whose conduct, in the performance of work for the government entity, is under the direct control of the government entity, whether or not they are paid by the Agency.

In this Model, ‘State personnel’ or ‘State government employees’ shall mean anyone in the State government workforce.

## 7.0 CIO/OFT Contact Information

---

Submit all inquiries and requests for future enhancements regarding this policy to:

**Attention: CIO/OFT Enterprise Strategy and Acquisitions Office  
Enterprise Strategy and Governance Services  
New York State Office of the Chief Information Officer and Office for Technology  
State Capitol, ESP, P.O. Box 2062  
Albany, NY 12220  
Telephone: 518-473-0234  
Facsimile: 518-473-0327  
Email: [oft.sm.policy@cio.ny.gov](mailto:oft.sm.policy@cio.ny.gov)**

The State of New York Enterprise IT Policies may be found at the following website:

<http://www.cio.ny.gov/policy/technologypolicyindex.htm>

## 8.0 Revision Schedule and History

---

Date	Description of Change
01/05/2007	Original Policy Issued.
10/6/2009	Reformatted and updated to reflect current CIO, agency name, logo and style.