



ANDREW M. CUOMO
GOVERNOR

State Capitol P.O. Box 2062
Albany, NY 12220-0062

DANIEL C. CHAN
Acting Chief Information Officer
Acting Director of the Office of IT Services

New York State Information Technology Policy	No: NYS-P03-001
Guideline Name: NYS Directory Services – Directory Account Management	Updated: 10/09/2009
	Issued By: NYS ITS State Chief Information Officer Director Office of IT Services Policy Owner: Division of Enterprise Networking & Telecommunications (Client Services)

1.0 Purpose and Benefits of the Policy

This policy describes account management requirements of the New York State Directory Services (NYSDS).

NYSDS is a suite of NYeNet identity management services including authentication and authorization for secure websites, website user tracking and a white pages information service. NYSDS also provides administration tools that allow website owners to control access to their resources and tools that allow Participating Organizations (POs) to control their user accounts.

Single sign-on for secure websites allows registered NYSDS users to be authenticated only once during each browser session, regardless of which PO is hosting the site. The user's credentials are shared among all websites that participate in the NYSDS Authentication and Authorization system.

2.0 Enterprise IT Policy Statement

Details regarding the authority to establish enterprise IT guidelines, policies and standards can be found [in NYS ITS 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 Policy

This Policy is applicable to Participating Organizations (POs) that use the NYSDS.

4.0 Policy Statement

This Policy provides an overview of:

- The "Trust Model" used by the NYSDS
 - Risk Assessment
 - Security Levels and Authentication Methods
 - Entitlements
- Requirements for use of the NYSDS
- Characteristics of NYSDS User Accounts
 - Trusted Identification
 - Required Account Fields
 - User Account Configuration
 - Security Levels and Authentication Methods
 - User Account Types
- Requirements for establishing and administering NYSDS User Accounts
 - User Account Creation
 - User Account Disabling
 - User Account Re-Enabling
 - User Account Reassignment
 - User Account Re-Validation
 - Delegated Administration
 - Administrative Roles
 - Account Functionality

Part 1. Trust Model

The Trust Model in use by the NYSDS consists of the following:

- Each NYSDS Application undergoes a Risk Assessment prior to deployment. Results of the Risk Assessment include a minimum Security Level and allowable Authentication Methods for that NYSDS Application.
- Each NYSDS User Account is assigned a Security Level, based upon the method used to identify the user at the time of account creation or promotion.
- Trusted Identification Methods are standardized and consistently applied to NYSDS User Accounts.
- Each NYSDS User Account is configured with one or more Authentication Methods which can be used to support a login by that user.
- An NYSDS User Account may be assigned an Entitlement to an NYSDS Application, signifying that the NYSDS User has permission to access that application.
- User access to an NYSDS Application will be granted if all of the following conditions are met:
 - The NYSDS User Account's Security Level is greater than or equal to the NYSDS Application's Security Level.
 - The NYSDS User has authenticated with a method that is permitted by the NYSDS Application.
 - The NYSDS User Account has an Entitlement to the NYSDS Application.

A. Risk Assessment

Access to all NYSDS Applications must be properly authenticated and authorized in a manner commensurate with the value of the NYSDS Application and associated data. The Participating Organization (PO) must perform a Risk Assessment of the NYSDS Application based on procedures defined by the New York State Office of Information Technology Services (ITS).

As part of the Risk Assessment, the PO must review both the NYSDS Application and the data which is accessed, created, modified, or otherwise controlled by the NYSDS Application to determine the maximum risk that would result from unauthorized access, specifically, the risk associated with:

- loss of confidentiality (theft of data)
- loss of integrity (unauthorized modification of data), and
- loss of availability of the NYSDS Application.

The factors that must be used to determine the overall risks associated with the occurrence of these events are:

- risk of monetary loss
- reputation risk
- productivity risk
- risk of diminished public safety.

The risk of monetary loss is determined using a variety of elements, including but not limited to:

- average dollar value of transactions
- loss to the government
- loss to a consumer
- loss to a business, state or local government, or other business partners
- rules for reversing and repudiating a transaction
- body of law applied to the transaction
- liability for the transaction (e.g., personal, corporate, insured, or shared).

The reputation risk to the Government in the event of a breach or an improper transaction is determined using elements such as:

- relationship with the trading partner
- public visibility and public perception of programs
- history or patterns of problems or abuses
- consequences of a breach or improper transaction.

Productivity risk associated with a breach or improper transaction is determined using elements such as:

- time criticality of transactions
- scope of system and number of transactions
- number of system users or dependents
- backup and recovery procedures
- claims and dispute resolution procedures.

Assessing these combined risk factors will assist in determination of the proper minimum Security Level and Authentication Method(s) required for use of that NYSDS Application.

The PO must communicate the results of the Risk Assessment to ITS, according to procedures defined by ITS. ITS may participate in or contribute to the Risk Assessment, but the PO retains full responsibility for defining the correct Security Level and applicable Authentication Method(s) for the NYSDS Application.

B. Mandatory and Discretionary Access Controls

Access to NYSDS Applications is controlled by a combination of Mandatory and Discretionary Access Controls. Mandatory Access Controls are those imposed by the system, i.e. the NYSDS. They cannot be overridden by Discretionary Access Controls, which are those controls assigned at user discretion, such as Entitlements to NYSDS Applications.

The results of the Risk Assessment are used to define Mandatory Access Controls for access to the NYSDS Application (Security Levels and Authentication Methods).

A user with an Entitlement to an NYSDS Application who does not meet the minimum NYSDS Application requirements for Security Level or Authentication Method will be denied access to the NYSDS Application.

C. Security Levels

The Security Level defines the degree of trust that may be placed in the Identification of an NYSDS User (i.e. How much do we believe that the NYSDS User is really who he says he is).

The Security Level is enforced as a Mandatory Access Control for each NYSDS Application (the NYSDS will ensure that a NYSDS User Account's security level must be greater than or equal to the NYSDS Application's Security Level).

Security Level 0 signifies "Unvalidated Identity." These are self-registered NYSDS Users for whom the identification information has not been validated.

Security Level 1 signifies "Non-Trusted Identity." These are bulk-loaded or PO (Participating Organization) Delegated Administrator-added NYSDS Users whose identification methods DO NOT meet the criteria for "Trusted Identification" (see Part 3). The PO which creates the account is using its own criteria to identify the NYSDS User. The local identification method should not be automatically trusted by other Participating Organizations without a more detailed understanding of the ID methodology that was used.

Security Level 2 signifies "Trusted Identity." These are NYSDS Users whose identity has been verified using Trusted Identification (see Part 3).

D. Authentication Methods

One or more Authentication Methods can be used to support the login of a NYSDS User. These include passwords, tokens, smart cards, biometrics, certificates, etc. The stronger the

Authentication Method, the more confidence one can have in the belief that the NYSDS User is really who she claims to be.

The Authentication Method is enforced as a Mandatory Access Control for each NYSDS Application (the NYSDS will ensure that an NYSDS User's current login Authentication Method is allowed by the NYSDS Application).

E. Background Investigations

Additional background investigation information may be required by the Risk Assessment to support access to an NYSDS Application. This information requirement can be enforced as a Mandatory Access Control for an NYSDS Application.

F. Entitlements

An Entitlement is granted by the owners of the NYSDS Application based upon their assessment of Need-to-Know and signifies that an NYSDS User has permission to run an NYSDS Application.

Entitlements are enforced as a Discretionary Access Control for an NYSDS Application (controlled by Entitlement Administrators).

Part 2. Requirements for the Use of the NYSDS

A PO which wants to use the NYSDS to store User Accounts and to deploy NYSDS Applications must follow procedures defined by NYSOFT to initiate this use.

The PO must follow the procedures defined by NYSOFT regarding Delegated Administration. A PO must manage user accounts according to the standards defined in this Policy and the procedures defined by NYSOFT. A PO must trust that other POs meet the same standards. The PO must trust the identity of all Security Level 2 users, regardless of which PO added those users.

The PO designates the Security Level of an NYSDS User Account at the time the account is created based upon the Identification Method which was used to identify the user.

To deploy a new NYSDS Application, or make changes to an existing NYSDS Application, a PO must follow the procedures defined by NYSOFT to initiate the use of the new or modified NYSDS Application.

Following deployment of an NYSDS Application, the PO must follow procedures defined by NYSOFT regarding Entitlement Delegated Administration. The PO must follow procedures defined by NYSOFT for performing a Risk Assessment and for defining a

minimum Security Level and one or more Authentication Methods for the NYSDS Application.

Part 3. USER IDENTIFICATION

Different forms of identification are required depending upon Security Level, as shown below.

Security Level	ID Verification Required
0	None. Level 0 is a temporary condition for an NYSDS User account.
0	None. Level 0 is a temporary condition for an NYSDS User account.
1	Non-Trusted Identification - The PO shall define the required identifying information.
2	Trusted Identification - Identification which meets the requirements of Part 3A (Trusted Identification) Trusted Identification must be provided to the PO Delegated Administrator. These must be originals or certified copies.

A. Trusted Identification

The following identifies minimum requirements for Security Level 2 accounts.

The classes of identification are those set forth below. All forms of identification must be valid and unexpired.

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 State 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
- Unexpired 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)
- Unexpired Temporary Resident Card (INS Form I-688)
- Unexpired Employment Authorization Card (INS Form I-688A)
- Unexpired Reentry Permit (INS Form I-327)
- Unexpired Refugee Travel Document (INS Form I-571)
- Unexpired 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

To meet the Security Level 2 requirements, the applicant must provide:

One (1) Class A form with a picture PLUS one (1) Class B form

OR

One (1) Class A form with a picture PLUS one (1) Class C form

OR

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

When a PO Delegated Administrator (PO DA) registers a new NYSDS User account at Security Level 2, or promotes an existing NYSDS User account to Security Level 2, the PO DA must follow procedures defined by NYSOFT for identity verification. The PO DA must follow procedures defined by NYSOFT for secure distribution of account and authentication information.

B. Required Account Fields

Depending upon Security Level, different Account information is required to be entered as supporting information, as shown below:

Security Level	Required Information
0	User ID

	<p>Password</p> <p>Shared secret question</p> <p>Shared secret answer</p>
1	<p>Level 0 Requirements, plus: Last Name, First Name, Middle Initial</p> <p>Address - Street, City, State, Postal Code, Country (Home address for account type P; business address for account types B and G)</p> <p>Phone Number</p> <p>Participating Organization</p> <p>Email Address (if applicable)</p> <p>Additional information depending upon requirements of the participating organization.</p> <p>State Driver's License ID or Non-Driver's ID</p>
2	<p>Level 1 Requirements, plus:</p> <p>User ID of the Level 2 PO DA for that PO who created the account and VERIFIED the ID</p> <p>List the TWO forms of identification</p> <p>Method used to present the identification source to the PO DA</p>

Part 4. USER ACCOUNT CONFIGURATION

A. Security Levels & Authentication Methods

Security Levels and allowable Authentication Methods designate the degree of trust associated with an NYSDS User account. See Part 1 for an explanation of Security Levels and Authentication Methods.

B. User Account Types

Each NYSDS User Account has an Account Type. The Account Type specifies the purpose (personal, business, or government) for which the account was created.

For accountability purposes, all NYSDS User Accounts (regardless of Type) are associated with an **INDIVIDUAL** (not a group). The Type designates the role in which that individual is actively functioning (i.e. as a business-related role, a government-employee role, or a personal role). In no case is a user account EVER permitted to be shared amongst multiple persons.

- 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 NYSDS User's employer or the legal entity under which the NYSDS User does business
- Personal (Individual) (P) - An account held by an individual that is for personal use, which is to be used to conduct private business with NYS Government

C. User ID

The User ID for each NYSDS user account shall be unique throughout the NYSDS. The User ID may not be reused by a different individual.

D. Unique Identifier

Each NYSDS user account above Level 0 shall contain an attribute which is an additional Unique Identifier. This Unique Identifier shall be based upon the NYSDS User's State Driver License ID number or non-Driver ID number.

E. Administration Accounts

There are specific requirements for creation of administrative accounts.

An NYSDS User must have an NYSDS user account at Security Level 2 before being granted a Delegated Administrator account. A Delegated Administrator account must be Security Level 2.

Part 5. USER ACCOUNT ADMINISTRATION

This part defines who is responsible for establishing and maintaining user accounts.

- **Security Level 0 Accounts:** A Security Level 0 account does not require administration. Account information is created by the NYSDS User during Self Registration.
- **Government and Business Accounts, Security Levels 1 and higher:** These accounts are administered by PO Delegated Administrators from the PO which owns the account.
- **Personal (Individual) Accounts, Security Levels 1 and higher:** These accounts are administered by ITS.

A. User Account Creation

User Accounts can be created in the following ways. NYSOFT will define procedures for each of these ways.

- **Self Registration** - A Security Level 0 account a temporary account created via Self Registration. The account must be user and/or promoted to a higher-level account within a limited period of time, or the account will be deleted based upon procedures defined by NYSOFT.
- **Bulk Load Registration** - Security Level 1 or higher accounts can be created via a Bulk Load Registration, which is performed by the NYSOFT. Bulk user information is provided by the PO. The identification procedures associated with that security level account **MUST** be followed by the PO when distributing the user passwords.
- **DA Registration** - Security Level 1 or higher accounts can be created by a PO Delegated Administrator using a Delegated Administration application. The identification procedures associated with that security level account **MUST** be followed by the PO when providing the NYSDS User with their password.
- **Account Promotion** - Accounts can be promoted by a PO Delegated Administrator using procedures defined by NYSOFT. The person requesting promotion must demonstrate that they are the owner of the lower level account, and that they can meet the ID Verification criteria for a higher Security Level account

B. User Account Disabling

Accounts can be automatically disabled based on login activity, or administratively disabled by either the PO DA or the NYSDS. NYSDS User Accounts cannot be removed once they have been used.

NYSDS User Account Disabling. NYSDS User account shall be disabled under the following conditions. The activity of account disabling must be logged.

Accounts are disabled under the following circumstances:

- After 180 consecutive days of inactivity (all level accounts)
- After 5 consecutive unsuccessful login attempts
- Upon termination of the employment of the NYSDS User, if he is a NYS employee or an employee of a business partner of NYS (for Government or Business accounts level 1 or higher)
- At the discretion of the PO DA or ITS
- Upon transfer of the user account to a different PO. The NYSDS User's account information must remain intact (password, user ID, name, etc.) with the exception of his/her entitlements, which are automatically stripped so that they no longer have access to applications related to their prior position, if any.

C. User Account Re-Enabling

NYSDS User accounts shall be re-enabled under the following conditions:

- At the discretion of the PO DA or ITS
- Upon acceptance of the NYSDS user account by a new PO

D. User Account Revalidation

The PO DA shall ensure that all NYSDS user accounts at Security Level 1 or higher are revalidated at least annually and that account information is updated as necessary.

Part 6. Delegated Administration

Delegated Administration allows distribution of NYSDS User Account Administration functionality while maintaining consistent administration practices. Delegated Administration provides functionality to localized administrators who are best positioned both geographically and logically to manage their NYSDS users. Delegated Administration includes both "PO Delegated Administration" (NYSDS User Account Management) and "Entitlement Delegated Administration" (NYSDS Application Management).

A. Administrative Roles

All Administrative Roles (PO DSAs, PO DAs, Application Owners, Entitlement DAs) will use special accounts which are created solely for the purpose of Delegated Administration. All NYSDS administration accounts are unique and are assigned to individuals, not groups.

PO Directory Services Administrator (PO DSA) - There will be a primary contact who will function as the Directory Services Administrator for each PO. The PO DSA is responsible for all delegated account administration for NYSDS user accounts which are owned by that PO. The PO DSA may perform account management and delegate account management for that PO to PO Delegated Administrators. The DSA role can only be granted and removed by CIO/OFT.

PO Delegated Administrator (PO DA) - There may be one or more PO DAs associated with each PO. The PO DA manages NYSDS user accounts within that PO. The PO DA is accountable to the PO DSA. The PO DA role can be granted and removed by either NYSOFT or the PO DSA.

Application Owner (AO) - The Application Owner is the contact for an NYSDS Application or Applications. The AO is responsible for defining a Security Level and allowable Authentication Method(s) for the NYSDS Application. The AO is responsible for defining the proper access to the NYSDS Application. The AO is an Entitlement Delegated Administrator for the NYSDS Application and may delegate Entitlement Administration for that NYSDS Application to Entitlement Delegated Administrators. The AO role can be granted and removed only by ITS.

Entitlement Delegated Administrator (Entitlement DA) - There may be one or more Entitlement DAs associated with each NYSDS Application. The Entitlement DA is able to grant and remove entitlements to the NYSDS Application to all NYSDS user accounts (regardless of PO). The Entitlement DA is accountable to the AO.

B. Account Functionality

PO Delegated Administrator - A PO DA performs the following NYSDS User Account administration functions for NYSDS User accounts within their PO:

- Create an NYSDS user account
- Promote or demote an NYSDS user account
- Disable or enable an NYSDS user account
- Reset an NYSDS user's password
- Modify certain information within an NYSDS user account, but not user ID.

Entitlement Delegated Administrator_- An Entitlement DA performs the following user account administration functions for all NYSDS user accounts:

- Grant an entitlement to an NYSDS user account for an application managed by that Entitlement DA
- Remove an entitlement from an NYSDS user account for an application managed by that Entitlement DA

5.0 Policy Compliance

All participating organizations in the NYeNet shall comply with all relevant technology policies, standards, procedures, or best practice guidelines as required by ITS.

The CIO may periodically review compliance by state government entities with this policy. Such review may include, but is not limited to, review of the technical and business analyses required to be developed pursuant to this policy, and other project documentation, technologies or systems which are the subject of the published policy or standard.

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> .

Account Promotion The process of changing the Security Level of an account from a lower level to a higher level using applicable Identification Methods.

Application Owner The point of contact for an NYSDS Application.

Authentication Method The authentication mechanism used at the time of user account login.

Bulk Load Registration An account creation process used for the initial loading of a large number of user accounts.

Delegated Administrator An administrator account, either a PO Delegated Administrator or an Entitlement Administrator.

Directory Services Administrator (DSA) The primary contact for each Participating Organization.

Discretionary Access Controls Access Controls which are enforced by Entitlements, based on the need-to-know defined by the Entitlement Delegated Administrator.

Entitlement Administrator An administrator account which is able to grant and remove NYSDS Application entitlements to User Accounts, potentially across POs.

Identification Method The technique used to obtain information regarding the user's identity; typically done as part of user account creation or promotion.

Mandatory Access Controls Access Controls which are enforced by the NYSDS, based on the Security Level and allowable Authentication Methods of the NYSDS Application.

NYS Directory Services (NYSDS) The infrastructure run by NYSOFT which enables the centralization of authentication and access control for applications on the NYeNet, and which provides single sign-on functionality for applications on the NYeNet.

NYSDS Application An NYSDS Application is an application whose authentication and authorization is controlled by the NYSDS.

NYSDS User Any person authorized to access the NYSDS.

NYSDS User Account An account in the NYSDS as identified by a User ID. An NYSDS User Account may be authorized to perform specific functions within the NYSDS.

Participating Organization (PO) The State Government entity, political subdivision of the State, corporation, trust, estate, incorporated or unincorporated association or other legal entity that either establishes and maintains user accounts on the NYSDS, and/or provides applications which use the NYSDS.

PO Delegated Administrator An administrator account which is able to manage user accounts owned by a PO.

Risk Assessment Review of an NYSDS Application to determine the potential for loss of reputation, productivity, or financial assets, given an exposure to vulnerabilities.

Security Level The degree of trust that is associated with a user account, based upon Identification Method; one of the attributes of a user account.

Self Registration The degree of trust that is associated with a user account, based upon Identification Method; one of the attributes of a user account.

User ID A unique alphanumeric identifier within the NYSDS.

7.0 ITS Contact Information

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

Attention: Policy Owner
New York State Office of the Chief Information Officer and Office for Technology
State Capitol, ESP, P.O. Box 2062
Albany, NY 12220

Questions may also be directed to your ITS Customer Relations Manager at:
Customer.Relations@cio.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

8.0 Revision Schedule and History

Date	Description of Change
04/03/2003	Original Policy Issued.
10/9/2009	Reformatted and updated to reflect current CIO, agency name, logo and style.
09/12/2012	Reformatted and updated to reflect current CIO, agency name, logo and style.