

# Enterprise IT Shared Services Service Level Agreement



## Directory Services Details

(Revision Date: September 15, 2010)

---

**DOCUMENT CONTROL  
REVISION HISTORY**

<i>DATE</i>	<i>DESCRIPTION</i>
<b>9.15.10</b>	<b>INITIAL RELEASE</b>

## TABLE OF CONTENTS

### DIRECTORY SERVICES

INTRODUCTION .....	4
SERVICE DETAILS .....	5
Authentication Service to Web Applications .....	5
Authorization Service for Web Applications.....	5
Delegated Administration (DA) .....	5
Self-Care .....	6
ORDER PROCESS.....	7
ROLES AND RESPONSIBILITIES .....	9
SUPPORT .....	13
LEGAL AND SECURITY ISSUES.....	14
RESOURCES .....	15
CONTACT US .....	16

## INTRODUCTION

The purpose of this document is to provide detailed Service Level Agreement (SLA) information about the New York State Directory Services (NYSDS) service.

NYSDS is a secure sign-on directory of user profiles and computer application access. Web-based applications leverage information contained within the directory for authentication, authorization and sharing information across government entities. Participating organizations are given the ability to manage user accounts for the organization within the directory.

A set of administrative procedures are used to establish consistency among the delegated administrators from each program area who are responsible for managing their portion of the directory. The combination of authentication, authorization and administrative procedures creates the security solution needed to best protect applications.

This document is part of a set of SLA documents, and part of a group of documents and web pages that contain information about Directory Services. The Resources Section of this document provides links to Directory Services' resources.

## SERVICE DETAILS

### **AUTHENTICATION SERVICE TO WEB APPLICATIONS**

The NYSDS provides centralized authentication (login) services. Authentication is the process of determining the identity of the user. Authentication typically involves the use of credentials (user id and password and/or token). The NYSDS authentication service includes complete password services including Forgotten Password Services (FPS) and complete password policy enforcement.

Logs are generated for successful and unsuccessful authentications.

### **AUTHORIZATION SERVICE FOR WEB APPLICATIONS**

NYSDS provides centralized authorization (access) services. The authorization process is based on whether or not authenticated users can access protected resources. Application entitlements determine which applications a user is authorized to access.

Authorization is enabled on user profile attributes as designed by the NYSDS customer. Application owners through use of Delegated Administration (DA) can change these user profile attributes to grant or deny access to applications.

Logs are generated for successful and unsuccessful authorizations.

### **DELEGATED ADMINISTRATION (DA)**

Delegated Administration (DA) is a web based software application that provides dual purposes. One purpose is to allow participating organization's administrative users of the NYSDS service to manage their users within their scope (traditionally in their own organization).

They have the ability to create users accounts, update user accounts, promote user accounts, reset user account passwords, enable and disable user accounts, and remove and reclaim user accounts. They also have the ability to generate reports about their users.

The second purpose is to allow application owners (referred to as Entitlement administrators) to grant and revoke access to their application on a statewide basis.

## **SELF-CARE**

NYSDS Self Care consists of four utilities: Self Registration, Self Administration and Forgotten Password Services (FPS), Forgotten User Name.

**Self Registration** is a web application that allows any person to register for a NYSDS account. It can be configured to collect application specific information on a per-application basis if desired. Registrants are allowed to set their own user ID and initial password. Duplicate user IDs are not allowed. Self registered users are considered “anonymous” from a security perspective, and are therefore not granted access to high security applications until they are examined and promoted by an authorized entity.

**Self Administration** is a web based application that is available to all registered NYSDS users. It allows users to update most personal and application specific attributes associated with the account. Users are not allowed to change the user ID, name and various other attributes depending on the designated security level.

**Forgotten Password Services** allows users to reset passwords if they successfully answer a group of previously selected questions specific to the account, and have an email address associated with the account that is not shared by any other NYSDS users.

**Forgotten User Name Services** provides a user his or her user id after they have successfully answered a group of previously selected questions specific to the account.

## ORDER PROCESS

For an organization to become a Participating Organization (PO) of the NYSDS, they must complete the tasks below.

The organization should understand the terms outlined in the Directory Account Management Policy and name the person who will be their single point of contact to CIO/OFT regarding Directory Services. The Participation Request form is submitted by the Information Security Officer (ISO) to create an administrative account containing the high-level role of Participating Organization Directory Services Administrator (PODSA). That account can then be used to access the Delegated Administration tool to administer accounts.

The organization will work with CIO/OFT's Telecommunication staff to gain connectivity to the NYSDS.

### Procedure #1 – Signup Tasks

The person(s) requesting this service should have the authority to give or obtain necessary executive approvals for participation.

1. Contact the CIO/OFT Customer Relations Managers, using the contact information provided at the end of this document, to set up an initial requirements meeting with the appropriate CIO/OFT staff.
2. Obtain and read the NYS Directory Services – Directory Account Management Policy. [See <http://www.cio.ny.gov/technologypolicyindex.htm> under Risk Management, G07-001 entitle “Best Practice Guideline on Identity and Access Management: Trust Model”.]
3. Select the primary contact (PODSA) for your organization.  
*Suggested Guideline* – Consider the PO's Information Security Officer or the Human Resources Director for the PODSA role. At a minimum, involve them in deciding who the appropriate person in your organization is for the role. The PODSA does not need to be a technical person in the organization.
4. The organization's ISO (or in lieu of an ISO, the person in the organization with roles & responsibilities similar to a security officer) will submit a completed [NYSDS Participation Request Form](#) to the CIO/OFT Customer Relations Team.
5. The CIO/OFT Customer Relations Manager will submit the request to the NYSDS shared mailbox, [nysds@cio.ny.gov](mailto:nysds@cio.ny.gov).

6. The Customer Relations Team and The Customer Agency will receive notification from the NYSDS group that a PODSA account has been established in both the development and production environments.

## **Procedure #2 – Accessing the Delegated Administration Tool**

The PODSA, Participating Organization Delegated Administrator (PODA), Help Desk Administrator (HAD), Application Owner (AO) and Entitlement Administrator (EA) (see **Roles and Responsibilities** for detailed description) will be given the ability to access the Delegated Administrative tool.

### **A. For customers having or anticipating NYeNet access:**

1. Test connectivity to the Delegated Administration tool by pointing your browser to the following locations and following the *Access My Account* link to the delegated administration tool:

**Development** → <https://stgws04.nyenet.state.ny.us/>

**Production** → <https://ws04.nyenet.state.ny.us/>

2. The PODSA should contact CIO/OFT Customer Relations group to obtain any necessary training for the Delegated Administration Tool. The PODSA can also use the DA Tool Help Guide. This can be accessed by logging into the DA Tool and selecting Help from menu on the left of the screen.

### **B. For customers without NYeNet access (note, NYeNet access is required to host an application secured by NYSDS):**

1. Contact the CIO/OFT Customer Relations Team, using the contact information found at the end of this document, to request connectivity to the NYeNet.
2. The PODSA should contact CIO/OFT Customer Relations group to obtain any necessary training for the Delegated Administration Tool. The PODSA can also use the DA Tool Help Guide. This can be accessed by logging into the DA Tool and selecting Help from menu on the left of the screen.

## ROLES AND RESPONSIBILITIES

### **Technical Responsibilities**

The following section describes the administrative duties of the customer agency technical staff or system administrators that are responsible for supporting the web servers and application servers for the agency.

#### Security

The Customer Agency is responsible for protecting web and application servers from unauthorized access by following industry standards for security best practices.

Customer agency is responsible for upgrading/maintaining web agents that are hosted at the customer agency data center. NYSDS will notify customer agencies when support for a web agent version is going to end. The notification will be sent as soon as NYSDS is made aware of the end of support date.

#### Application Registration

Technical Staff or system administrators are required to:

- Submit application registration forms at least 3 weeks prior to the application start date.
- Notify NYSDS when an application owner has changed.
- Inform NYSDS of any changes to their infrastructure, software, or procedures that may affect the service offered by NYSDS.

#### Incident Management

Technical Staff or system administrators are required to:

- Provide adequate and timely resources in the event of an incident.
- Perform entry level troubleshooting (i.e. basic connectivity tests) during an incident.

### **User Account Management Responsibilities**

The following section describes the administrative duties of the customer agency technical staff or system administrators that are responsible for supporting the user account management for the agency. The following are roles within the user account management component:

#### ***Participating Organization Directory Services Administrator (PODSA)***

The DA in a participating organization having an account containing the PODSA role is the primary contact between the organization and CIO/OFT. This individual is responsible for

structuring user account management for that organization. There can only be one PODSA for an organization. Functions available to a PODSA role include adding, updating, promoting, and removing user accounts; changing passwords; and disabling and re-enabling accounts. Using the DA application, a PODSA can request to add or remove additional administrative accounts for the purposes of user management. There can be any number of additional administrative accounts established for user management. (See PODA role.)

### ***Participating Organization Delegated Administrator (PODA)***

A Delegated Administrator (DA) in a participating organization having an account containing the PODA role can perform all of the functions of a PODSA except requesting changes to his or other DA accounts.

The PODA role is assigned by a PODSA. There can be multiple PODAs within an organization.

### ***Help Desk Administrator (HDA)***

A DA with an account containing the HDA role can reset user account passwords. An organization may have zero, one, or more HDAs.

Note: CIO/OFT Customer Care Center Help Desk Agents may reset passwords for all users in the directory.

The HDA role for an organization is assigned by the PODSA.

### **User Account Disabling**

NYSDES User accounts can be automatically disabled based on login activity, or administratively disabled by the PODSA.

NYSDES User account shall be disabled under the following conditions.

- Transactions regarding disabling or archiving are logged
- After 180 consecutive days of inactivity (all level accounts)
- After 5 consecutive unsuccessful login attempts
- Upon termination of the employment of the NYSDES 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 PODSA or CIO/OFT
- Upon transfer of the user account to a different PO. The NYSDES 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.

### **User Account Removal**

NYSDS user accounts can be removed by the PODSA or PODA. The removal process places the user account into the Archive branch of the directory, the account is not deleted.

Administrative accounts in the Directory will be archived by the NYS Directory Services Technical team upon the approval of the PODSA, or agency ISO.

### **User Account Reclaim**

The Reclaim Process allows a Delegated Admin the ability to reclaim an account that has been removed, or placed into the archive branch of the directory. This feature is extremely useful for employees that have transferred from one agency to another.

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

- At the discretion of the PODSA or CIO/OFT
- Upon acceptance of the NYSDS user account by a new PO

### **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.

### **User Account Management Scopes**

User account management scope refers to the range of accounts that can be managed by a specific administrator. A PODSA, PODA, or HDA administrator's scope identifies the organizations that they can manage. Typically, the scope will include the organization to which the administrator belongs, but may also include any organizations that have proxied management rights.

### **Application Entitlement Management**

The following are roles within the application entitlement management component:

#### ***Application Owner (AO)***

The Application Owner of an application will have an administrative account in the directory with the application role associated to it. The AO role serves as the primary contact between that application and the CIO/OFT, and is the person responsible for structuring the entitlement management for that application. Functions associated with an AO role include granting and revoking application entitlements to user accounts. There can only be one AO for each application. Using the DA application, an AO can request to add or remove additional entitlement management accounts for the application. Any number of additional administrative accounts can be established for this purpose. (See EA role.)

### **Entitlement Administrator (EA)**

The Entitlement Administrator will have an administrative account in the directory with the application role associated with it. An administrator with an EA role can perform all of the functions of an AO except requesting modifications to other EA accounts. The EA role for an application is assigned by the AO of that application. There can be multiple EAs for an application.

### **Application Entitlement Scopes**

There are two types of scope with regard to application entitlement: *application scope* and *limiting organization scope*.

Application Scope is mandatory for both AO and EA roles and refers to the list of applications covered by that role. For example, an AO role with an application scope of “Application 1” and “Application 2” indicates those two applications are owned by that account holder.

Limiting Organization Scope is not applicable to the AO role, and is optional within each application for the EA role. If present, this scope limits an EA’s ability to administer entitlements for that application to users within the organizations listed in the scope. If no limiting organization scope is present, the EA will be able to administer entitlements for the application over the entire directory. The AO role will always have full privilege to administer entitlements for their applications over the entire directory.

### **Security**

CIO/OFT will:

- Provide a secure environment for the NYS Directory Service. This includes authentication and access, and audit trails.
- Software Patches: CIO/OFT shall proactively monitor appropriate media to identify security risks in the NYS Directory Services environment.
- Physical Security: CIO/OFT will provide a physically secured area that will house NYS Directory Services servers, data storage and related equipment in full compliance with CIO/OFT policies and standards. This area will be controlled twenty-four hours per day, seven days per week.

### **NYSDS Maintenance**

The standard NYSDS maintenance windows are Wednesdays and Fridays, from 4:30AM to 7:00AM. NYSDS will send a Customer Notification prior to any maintenance being performed on the service. There may be instances when a larger maintenance window is required due to the type of maintenance being performed. NYSDS is sensitive to the critical nature and availability of the individual agency applications. NYSDS changes are reported to the CIO/OFT change board prior to the scheduled change.

## SUPPORT

### **Service Support**

CIO/OFT Customer Relations Manager is the main contact point for State and local government Directory Services customers. Customer Relations Managers can be reached by phone at 1-866-789-4638 or by email at [customer.relations@cio.ny.gov](mailto:customer.relations@cio.ny.gov). For a list of Customer Relations Managers by State agency see <http://www.cio.ny.gov/support/ContStateCRMs.htm>

### **Technical Support**

CIO/OFT supports and maintains the core NYS DS infrastructure, network availability, overall directory, backup and restore, and issue resolution. The Customer Care Center (CCC) provides Level 1 support to Customer Agency help desks for NYS Directory Services.

**The Customer Care Center (CCC)** is the main contact point for all CIO/OFT customers. The CCC Level 1 technicians are highly experienced and trained in resolving incidents. If an incident cannot be resolved during the initial call, a ticket is generated and assigned to the appropriate resolver for resolution.

The Customer Care Center is staffed 24x7x365 days a year, and can be reached at 1-800-697-1323. Each call to the CCC will incur a fee to the agency.

## LEGAL AND SECURITY ISSUES

### Acceptable Use Policy

This application uses the New York State (hereinafter State) Central Directory Service of the NYeNet for authentication and authorization. In addition to any obligations arising under acceptable use policies or terms of service implemented by NYeNet Participating Organizations, logging into this application indicates customer agency's agreement to abide by the following:

- Use this application only for purposes directly related to the conduct of official business with the State or its agencies and the application shall not be used for nonpublic purposes including, but not limited to, the pursuit of personal activities, the mass distribution of unsolicited messages ("spamming"), and the promotion of commercial ventures or religious or political causes;
- Are responsible for acquiring and safeguarding your own user ID and password used to access this application;
- Are responsible for any activity attributable to the use of your account whether by you or any other person;
- Shall not engage in activities that may cause interference with or disruption to any network, information service, equipment or user thereof;
- Shall comply with all applicable confidentiality and security requirements as set forth in any applicable acceptable use policies or terms of service implemented through this application directly or by NYeNet Participating Organizations, and shall not seek information on other users or attempt to obtain access to, copy, or modify other users' files without express permission;
- Shall not violate the rights of any person or entity protected by copyright, trade secret, patent, or other similar laws or regulations;
- Shall not use this application for any fraudulent or illegal purpose, including, but not limited to, the transmission of obscene or harassing materials; and
- Must report any abuse or misuse of this application to OFT and you shall cooperate fully in any investigation into any such abuse or misuse.
- Understand and agree that the State reserves the right to revise, amend, or modify this Acceptable Use Policy or other policies and agreements at any time in any manner. Notice of any revisions, amendments, or modifications will be posted on this and/or other State sites.

### Encryption

Authentication and authorization services are encrypted via proprietary vendor software. This traffic is additionally encrypted via VPN tunnel to the Directory Service.

## RESOURCES

**Service Level Agreement Home Page**

<http://www.cio.ny.gov/SLA.htm>

**NYS Directory Services Account Management Policy**

<http://www.cio.ny.gov/Policy/NYSTechPolicyP03-001.pdf>

**Customer Care Center Home Page**

[http://www.cio.ny.gov/customer\\_care\\_center](http://www.cio.ny.gov/customer_care_center)

**Protection of CIO/OFT's Information Assets**

[http://www.cio.ny.gov/Policy/p04-003/files/Protection\\_of\\_OFTs\\_Digital\\_Assets-FINAL.pdf](http://www.cio.ny.gov/Policy/p04-003/files/Protection_of_OFTs_Digital_Assets-FINAL.pdf)

**NYS Office of Cyber Security and Critical Infrastructure Coordination - Information Security Policy**

[NYS Office of Cyber Security](#)

**NYS CIO/OFT Identity and Access Management Trust Model**

<http://www.cio.ny.gov/Policy/G07-001/G07-001.pdf>

## CONTACT US

### Customer Relations Managers listed by State Agency

<http://www.cio.ny.gov/support/ContStateCRMs.htm>

Contact CIO/OFT Customer Relations Managers or the Customer Care Center at

**1-866-789-4638 or 518-402-2537**

#### When You Call

**Option 1:** Technical Support

Additional Choices:

1. Customer Care Center
2. Data Center Operations
3. NYeNet Network Operations Center (NOC)
4. Voice Services

**Option 2:** State and Local Government Customer Service (for Customer Relations Managers)

**Option 3:** New York State Directory Assistance Operator

**OR by E-Mail at:** [customer.relations@cio.ny.gov](mailto:customer.relations@cio.ny.gov)

**Contact NYS Directory Services at:** [nysds@cio.ny.gov](mailto:nysds@cio.ny.gov)