2018 OSOS Security Coordinator Training

Systems Unit
August 24, 2018

Good morning everyone and welcome.

I'm Jennifer Dewey with the Systems Unit and I'm here with Rebecca Kline also from the System Unit. We've had the opportunity to correspond and speak with many of you through the OSOS Accounts mailbox where we receive and process requests related to OSOS user accounts.

We are happy to be with you this morning for the 2018 OSOS Security Coordinator Training.

Agenda

- **Security Coordinator Roles and Responsibilities**
- **OSOS/REOS Account Requirements and Forms**
- **Selecting User Permissions**

NEW YORK STATE OF OPPORTUNITY. Department of Labor

In this webinar we're going to discuss security coordinator roles and responsibilities, account requirements and forms for OSOS/REOS access, and how to select user permissions when requesting OSOS access.

We'll also be covering some changes to the process for taking annual confidentiality training.

We're going to start by reviewing the roles and responsibilities of the local security coordinators.

Roles and Responsibilities

- **Secure and Protect Personally Identifiable Information (PII) and Personal, Private and Sensitive Information (PPSI)**
  - Enforce data security requirements related to the use of OSOS and REOS. (Technical Advisory #18-5 issued July 6, 2018)

- **Gatekeeper for System Use**
  - Ensure proper use of the One-Stop Operating System (OSOS) and the Re-Employment Operating System (REOS). (Technical Advisory #17-7 issued June 28,2017)

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Each Local Workforce Development Area has at least two designated Security Coordinators. Generally one is a DOL employee and the other is designated by the Local Workforce Development Area. We expect the Security Coordinators to work collaboratively to ensure appropriate access and use of the systems.

There are two main roles for the local Security Coordinator:

The first is Securing and Protecting confidential information

And the second is serving as the Gatekeeper for OSOS/REOS systems use

Secure and Protect PII/PPSI

All **LWDBs**, **local staff** and **service providers** must ensure a secure physical and electronic/digital environment which will protect **Personally Identifiable Information (PII)** and **Personal, Private and Sensitive Information (PPSI)** in any format including OSOS, REOS, hard copy documents and digital media.

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Technical Advisory 18-5 was recently released, updating and establishing policy relating to Personally Identifiable Information (PII) and Personal, Private and Sensitive Information (PPSI) within the NYS Workforce Development System.

LWDBs, local staff and service providers must take measures to address the following topics to reduce the risks associated with the collection, storage and dissemination of Career Center customer's PII/PPSI:
-Accessing and Sharing of PII/PPSI;
-Security Protocols related to OSOS and REOS;
-Maintaining a Secure Environment; and
-Breaches of Confidentiality.

This TA re-iterates the role of the security coordinator to enforce data security requirements related to OSOS and REOS.

This applies to all local staff – including NYSDOL staff, non-federally funded partner staff in each Career Center, and service providers - who have been provided access to OSOS and REOS through the local area.

6

Secure and Protect PII/PPSI

Two times each program year, local managers/supervisors must conduct and document an environmental assessment in Career Centers to determine whether local staff are maintaining a secure PII/PPSI environment (both physical and electronic/digital).

Attachment A: Confidentiality – Environmental Assessment provides a sample template which may be used. Completed forms must be maintained by the Security Coordinator for three years.

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Per TA 18-5, local management must conduct and document an environmental assessment twice each year to determine if local staff is maintaining a secure environment for both physical and electronic confidential information.

The Technical Advisory includes the Confidentiality Environmental Assessment template as Attachment A.

While it is the local managers and supervisors who are tasked with conducting and documenting this assessment, local security coordinators are responsible for maintaining the completed forms for the three year retention period.

Secure and Protect PII/PPSI

Technical Advisory 18-5

https://labor.ny.gov/workforcenypartners/ta/ta-18-5.pdf

Attachment for Forms

- Confidentiality – Environmental Assessment
  https://www.labor.ny.gov/workforcenypartners/ta/18-5_attachment_a.pdf

NEW YORK STATE OF OPPORTUNITY. Department of Labor

This slide provides the link to the Technical Advisory as well as to Attachment A.

Gatekeeper for System Use

- The New York State Career Center System utilizes two separate systems to effectively and accurately document programmatic and participant data:
  - One-Stop Operating System (OSOS)
  - Re-Employment Operating System (REOS)
- Security Coordinators provide the key role in protecting and maintaining the data security requirements and related documentation for these applications.

NEW YORK STATE OF OPPORTUNITY. Department of Labor

The other role of the Security Coordinator is serving as the Gatekeeper for System Use.

As you know, The New York State One-Stop Career Center System utilizes two separate systems to effectively and accurately document programmatic and participant data: the One Stop Operating System (OSOS) and the Re-Employment Operating System (REOS).

OSOS is the primary case management system used for tracking all services provided to customers throughout the Workforce Development System. OSOS is used to collect substantial information from customers, businesses, and training providers. Much of this information is used to prepare required State & Federal reports. Customer information that is entered in OSOS can assist staff from multiple agencies and organizations in gaining a better understanding of a customer's needs which can lead to more targeted services for the customer and better employment outcomes.

REOS is the primary operating system used for tracking Career Center appointments for customers receiving Unemployment Insurance assistance. REOS is used to schedule UI customers for their mandatory appointments in the Career Center and it

also tracks whether the customers attend these appointments. REOS is connected with the UI Mainframe and can therefore alert UI staff if a customer has an issue or fails to report to their mandatory appointment.

To protect and prevent the misuse of the highly confidential information collected within OSOS and REOS, the Security Coordinators are charged with the enforcement of data security requirements related to the use of these applications.

Gatekeeper for System Use

Technical Advisory 17-7

https://labor.ny.gov/workforcenypartners/ta/ta-17-7.pdf

Attachments for Forms

- Individual Access Agreement for OSOS and REOS
  https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-a.pdf
- State Agency MOU for OSOS
  https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-b.pdf
- State Agency MOU for REOS
  https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-c.pdf
- Interagency Agreement for OSOS
  https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-d.pdf
- Interagency Agreement for REOS
  https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-e.pdf

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Many of you may be familiar with the Technical Advisory 17-7 which establishes the policy on proper use of OSOS and REOS and provides the procedure by which staff can gain access to these systems. It also includes, as attachments the forms necessary for an agency or individual to gain access to OSOS and REOS.

This TA provides the foundation for the next segment of today's webinar…

next slide

…OSOS and REOS Account Requirements and Forms.

OSOS/REOS System Use

- **Partner Agencies**
- **New Accounts**
- **Editing Accounts**
- **Deactivating Accounts**

NEW YORK STATE OF OPPORTUNITY. Department of Labor

First we will discuss Partner Agencies and the process by which they can gain access to the OSOS/REOS system.

Then we will cover what is required for all users to create new accounts, as well as the procedure for editing and deactivating existing accounts.

Partner Agencies

- **Partner Agencies can be either State Agency or Non-State Agency Partners**
- **Memorandums of Understanding (MOUs) or Interagency Agreements are required prior to OSOS/REOS access.**

The process for gaining access to the OSOS/REOS systems varies slightly depending upon whether the user is DOL staff or partner staff from a state or non-state agency.

Partners are described as either State Agency Partners or Non-State Agency Partners.

The New York State Career Center System Partner ~~("Partner")~~ must request access to one or both of these systems by submitting the appropriate interagency agreement or Memorandum of Understanding (MOU) before individual staff users can be granted access to OSOS/REOS.

These agreements provide the authority under which the Partner may access and exchange information through OSOS.

State Agencies

State Agency Partners must execute the appropriate MOU for the exchange of confidential information. The MOUs for OSOS and REOS are presented as Attachments B and C respectively:

- https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-b.pdf
- https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-c.pdf

NEW YORK STATE OF OPPORTUNITY. Department of Labor

When reviewing TA 17-7, you will see that Attachments B and C are relevant for State Agency partners.

State Agency Partners must complete a Memorandum of Understanding (MOU) in order to gain access to OSOS and/or REOS. If the State Agency Partner only wants access to OSOS, then they will only need to complete the MOU for OSOS. However, if they would like access to REOS, then they must sign the MOU for both OSOS and REOS. The reason for this is because access to REOS is granted through OSOS. A user cannot have access to REOS without having access to OSOS.

These agreements are completed only once for the given agency

Non-State Agencies

Non-State Agency Partners must sign the Interagency Agreement for OSOS (**Attachment D**) and/or the Interagency Agreement for REOS (**Attachment E**) for the exchange of confidential information as appropriate for the system(s) they wish to access:

- https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-d.pdf
- https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-e.pdf

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Non-State Agency partners must sign an Interagency agreement in order to gain access to OSOS and REOS. Similarly to State Agency partners, non-state agency partners who only wish to access OSOS will only need to complete and sign the interagency agreement for OSOS. In order to access REOS, they would need to sign both agreements.

Again, these agreements are completed only once for the given agency.

Interagency Agreements

Each agency must sign **THREE** (3) original agreements and send to the below address:

NYS Department of Labor
System Support Unit
Building 12 – Room 428
Harriman State Office Campus
Albany New York 12240

NEW YORK STATE OF OPPORTUNITY. Department of Labor

In order for partner staff from either a state or non-state agency to be granted access to OSOS and/or REOS, the agency must be approved. Each agency must submit three agreements with original signatures to the address listed on the screen: The System Support Unit here in Albany.

Once we receive **three** original signatures of the Agreement, one will be returned to the agency, another will be retained by the Administrative Finance Office and the last will be kept by the Department of Labor's Counsel's Office. A copy of the agreements will also be kept by the DOL System and Support Unit.

It is important to note and inform agencies requesting access - that this process can take approximately 2-4 weeks to obtain the proper signatures.

Once the agency, as a whole, has been approved, then individual users can request their accounts.

New Accounts

- **Required Forms**
- **Cornerstones of Confidentiality**
- **Individual Access and Confidentiality Agreement**
- **OSOS Account Request Form**

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Let's now talk about the procedure for individual user's New Accounts…

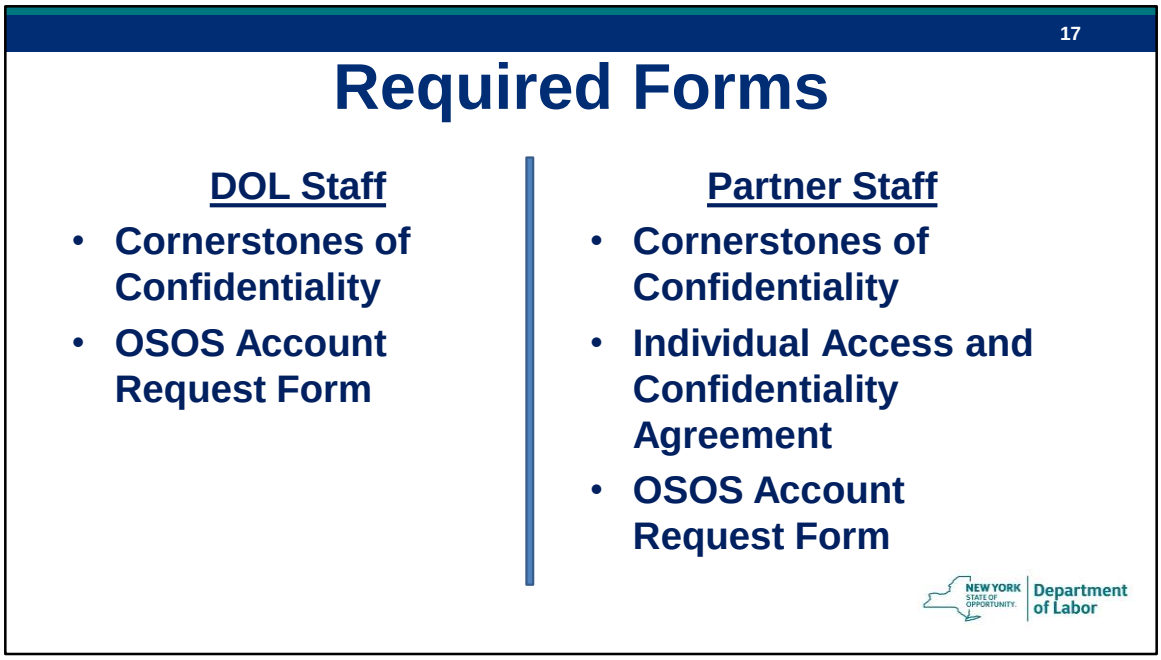
The are three forms which may be required:

The Attestation of Completion for the Cornerstones of Confidentiality training,

The Individual Access and Confidentiality Agreement

And

the OSOS Account Request Form.



Before accessing OSOS/REOS, individuals must complete the required documentation and confidentiality training. They must then request OSOS access through their Local Security Coordinator. Once the security coordinator has reviewed the documentation and approved the request, the security coordinator then forwards the paperwork to us at the OSOS Accounts mailbox. We will provide the address at the conclusion of this webinar.

The required documentation is dependent upon whether the user is DOL or partner staff.

For DOL staff, the Attestation form for completion of the Cornerstones of Confidentiality and the OSOS Account request form are required.

For Partner staff, we require the Attestation of completion for Cornerstones, the Individual Access & Confidentiality Agreement and the OSOS Account Request form. The Individual Access & Confidentiality Agreement is not required for DOL staff as it was completed as part of the onboarding process.

New users are required to:

Submit the completed Attestation form for Cornerstones of Confidentiality,
And the Individual Access & Confidentiality Agreement to their supervisor who will sign all forms and complete the OSOS Account Request form. The forms are then provided directly to the local Security Coordinator for review and approval.
The Security Coordinator the submits all documentation to the OSOS Accounts mailbox for final approval and account creation or maintenance.

Please Note that multiple users cannot be combined on one form.

And with that, I Now introduce Rebecca Kline who will review each form in further detail…

Cornerstones of Confidentiality

- **Mandatory annual training for ALL users.**
- **Available through the State Learning Management System (SLMS) or https://labor.ny.gov/workforcenypartners/osos/video/cornerstones.shtm.**
- **The Attestation of Completion must be signed by user and supervisor and submitted to OSOS Accounts with a copy retained by the local Security Coordinator.**

NEW YORK STATE OF OPPORTUNITY. Department of Labor

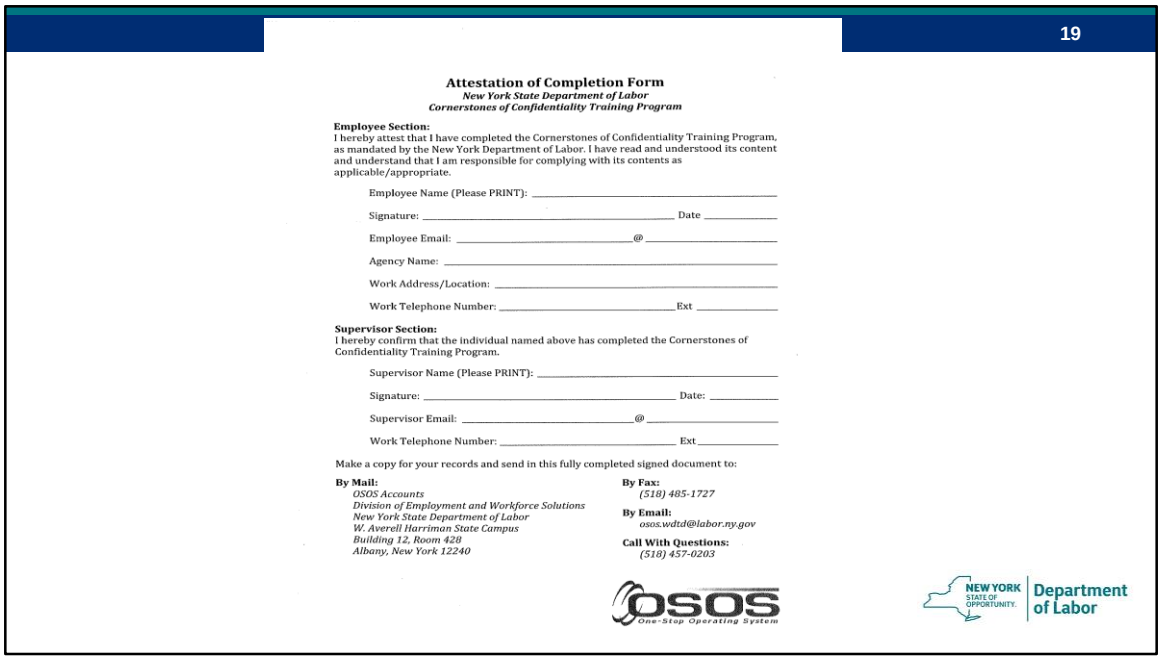
Thank you, Jennifer. And good morning, everyone. Let's start with the Cornerstones of Confidentiality.

The Cornerstones of Confidentiality is a yearly mandatory training for all staff with OSOS access. This includes both partner and DOL staff. All DOL staff using OSOS will be auto-enrolled in the Cornerstones of Confidentiality each year through the Statewide Learning Management System (SLMS). Partner staff are also required to complete this training yearly. They may choose complete the required training on SLMS, although they will not be auto-enrolled, or they may instead choose to complete the training through the link shown.

New DOL staff will also need to access the Cornerstones training via this link, as their SLMS account will not be immediately available to them.

Regardless of whether the training is completed through SLMS or through the link shown, staff must print the Attestation form, complete the Employee Section and submit it to their supervisor. The supervisor must complete and sign the Supervisor Section of the Attestation.
Attestation of Completion forms must be sent to OSOS Accounts at the contact

information provided on the form. Local OSOS security coordinators are also required to maintain OSOS accounts records that include up-to-date Cornerstones attestation forms.



Attestation of Completion Form

New York State Department of Labor

Cornerstones of Confidentiality Training Program

Employee Section:
I hereby attest that I have completed the Cornerstones of Confidentiality Training Program, as mandated by the New York Department of Labor. I have read and understood its content and understand that I am responsible for complying with its contents as applicable/appropriate.

Employee Name (Please PRINT): _____

Signature: _____ Date _____

Employee Email: _____@_____

Agency Name: _____

Work Address/Location: _____

Work Telephone Number: _____Ext _____

Supervisor Section:
I hereby confirm that the individual named above has completed the Cornerstones of Confidentiality Training Program.

Supervisor Name (Please PRINT): _____

Signature: _____ Date: _____

Supervisor Email: _____@_____

Work Telephone Number: _____ Ext_____

Make a copy for your records and send in this fully completed signed document to:

By Mail:
OSOS Accounts
Division of Employment and Workforce Solutions
New York State Department of Labor
W. Averell Harriman State Campus
Building 12, Room 428
Albany, New York 12240

By Fax:
(518) 485-1727

By Email:
osos.wdtd@labor.ny.gov

Call With Questions:
(518) 457-0203

OSOS One-Stop Operating System

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Once a user completes the Cornerstones of Confidentiality, the attestation form shown on this screen will be available for staff to print.

Again, once the form is signed by the user and the supervisor, it must be submitted to OSOS Accounts. The completed forms must either be submitted to OSOS Accounts through the local security coordinator, or the security coordinator must be copied on the emailed Attestation forms. This ensures that security coordinators maintain a copy of all current Attestations of Completions for their local area. The Security Coordinators do need to have the original signed attestation forms on file.

Individual Access and Confidentiality Agreement

- **Mandatory for all partner staff.**
- **Kept on file by the local Security Coordinator.**
- **Copy submitted to the OSOS Accounts mailbox.**

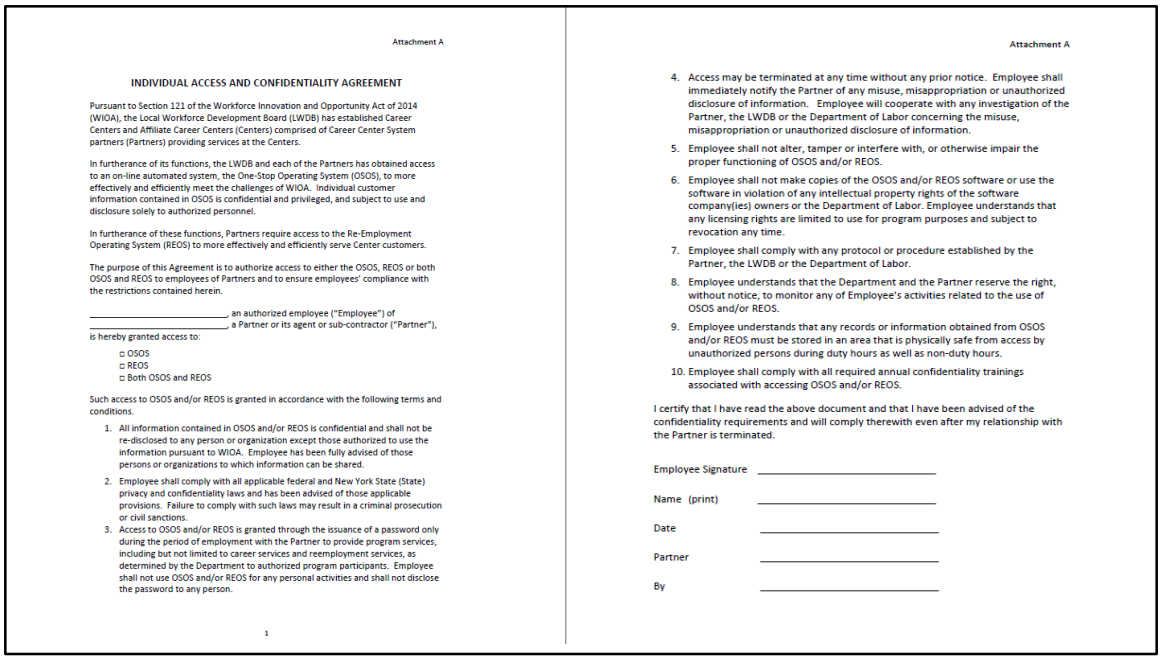
https://www.labor.ny.gov/workforcenypartners/ta/ta-17-7-attach-a.pdf

NEW YORK STATE OF OPPORTUNITY. Department of Labor

The Individual Access and Confidentiality Agreement must be signed by the partner user that is requesting access to the system, regardless of whether they are from a State Agency partner or a non-state agency partner. Again, this form is not required for creation of an OSOS account for DOL staff as it was already completed as part of the onboarding process.

It is on this form that partner staff can indicate whether they are requesting access to OSOS, REOS or both. Once the user completes and signs the Individual Access and Confidentiality Agreement, the original signed agreement must be kept on file by the Security Coordinator and a copy sent to OSOS Accounts with the other user paperwork.

It is the Security Coordinators responsibility to ensure that an executed Interagency Agreement or MOU is in place prior to requesting access for Individual Users.



Attachment A

INDIVIDUAL ACCESS AND CONFIDENTIALITY AGREEMENT

Pursuant to Section 121 of the Workforce Innovation and Opportunity Act of 2014 (WIOA), the Local Workforce Development Board (LWDB) has established Career Centers and Affiliate Career Centers (Centers) comprised of Career Center System partners (Partners) providing services at the Centers.

In furtherance of its functions, the LWDB and each of the Partners has obtained access to an on-line automated system, the One-Stop Operating System (OSOS), to more effectively and efficiently meet the challenges of WIOA. Individual customer information contained in OSOS is confidential and privileged, and subject to use and disclosure solely to authorized personnel.

In furtherance of these functions, Partners require access to the Re-Employment Operating System (REOS) to more effectively and efficiently serve Center customers.

The purpose of this Agreement is to authorize access to either the OSOS, REOS or both OSOS and REOS to employees of Partners and to ensure employees' compliance with the restrictions contained herein.

_____, an authorized employee ("Employee") of _____, a Partner or its agent or sub-contractor ("Partner"), is hereby granted access to:

- □ OSOS
- □ REOS
- □ Both OSOS and REOS

Such access to OSOS and/or REOS is granted in accordance with the following terms and conditions.

1. All information contained in OSOS and/or REOS is confidential and shall not be re-disclosed to any person or organization except those authorized to use the information pursuant to WIOA. Employee has been fully advised of those persons or organizations to which information can be shared.
2. Employee shall comply with all applicable federal and New York State (State) privacy and confidentiality laws and has been advised of those applicable provisions. Failure to comply with such laws may result in a criminal prosecution or civil sanctions.
3. Access to OSOS and/or REOS is granted through the issuance of a password only during the period of employment with the Partner to provide program services, including but not limited to career services and reemployment services, as determined by the Department to authorized program participants. Employee shall not use OSOS and/or REOS for any personal activities and shall not disclose the password to any person.

1

Attachment A

4. Access may be terminated at any time without any prior notice. Employee shall immediately notify the Partner of any misuse, misappropriation or unauthorized disclosure of information. Employee will cooperate with any investigation of the Partner, the LWDB or the Department of Labor concerning the misuse, misappropriation or unauthorized disclosure of information.
5. Employee shall not alter, tamper or interfere with, or otherwise impair the proper functioning of OSOS and/or REOS.
6. Employee shall not make copies of the OSOS and/or REOS software or use the software in violation of any intellectual property rights of the software company(ies) owners or the Department of Labor. Employee understands that any licensing rights are limited to use for program purposes and subject to revocation any time.
7. Employee shall comply with any protocol or procedure established by the Partner, the LWDB or the Department of Labor.
8. Employee understands that the Department and the Partner reserve the right, without notice, to monitor any of Employee's activities related to the use of OSOS and/or REOS.
9. Employee understands that any records or information obtained from OSOS and/or REOS must be stored in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours.
10. Employee shall comply with all required annual confidentiality trainings associated with accessing OSOS and/or REOS.

I certify that I have read the above document and that I have been advised of the confidentiality requirements and will comply therewith even after my relationship with the Partner is terminated.

Employee Signature _____

Name (print) _____

Date _____

Partner _____

By _____

This is the current Individual Access & Confidentiality Agreement.

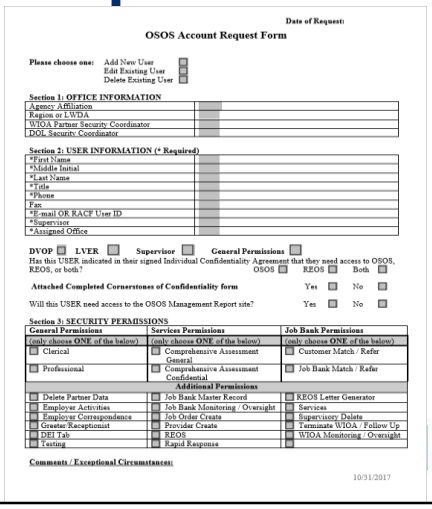
Please be sure to use the current version of this form which references WIOA.

The previous outdated version references WIA and we are unable to accept this form for account creation.

OSOS Account Request Form

- **Mandatory for all new accounts, edits, deactivations.**
- **Kept on file by the local Security Coordinator.**
- **Copy submitted to the Systems Unit.**

- **Linked to the "Accessing the System" OSOS Guide**
  https://labor.ny.gov/workforcenypartners/osos/osos-guide-accessing-the-system.pdf



Date of Request:

OSOS Account Request Form

Please choose one: Add New User / Edit Existing User / Delete Existing User

Section 1: OFFICE INFORMATION

Agency Affiliation	
Region or LWDA	
WIOA Partner Security Coordinator	
DOL Security Coordinator	

Section 2: USER INFORMATION (* Required)

*First Name	
*Middle Initial	
*Last Name	
*Title	
*Phone	
Fax	
*E-mail OR RACF User ID	
*Supervisor	
*Assigned Office	

DVOP LVER Supervisor General Permissions

Has this USER indicated in their signed Individual Confidentiality Agreement that they need access to OSOS, REOS, or both? OSOS REOS Both

Attached Completed Cornerstones of Confidentiality form Yes No

Will this USER need access to the OSOS Management Report site? Yes No

Section 3: SECURITY PERMISSIONS

General Permissions (only choose ONE of the below)	Services Permissions (only choose ONE of the below)	Job Bank Permissions (only choose ONE of the below)
Clerical	Comprehensive Assessment General	Customer Match / Refer
Professional	Comprehensive Assessment Confidential	Job Bank Match / Refer
	Additional Permissions	
Delete Partner Data	Job Bank Master Record	REOS Letter Generator
Employer Activities	Job Bank Monitoring / Oversight	Services
Employer Correspondence	Job Order Create	Supervisory Delete
Greeter/Receptionist	Provider Create	Terminate WIOA / Follow Up
DEI Tab	REOS	WIOA Monitoring / Oversight
Testing	Rapid Response	

Comments / Exceptional Circumstances:

10/31/2017

Department of Labor

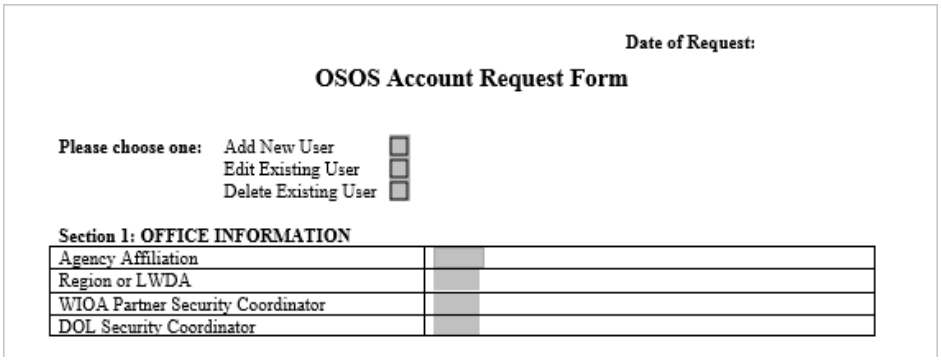
Next is the OSOS Account Request Form.
I'm sure that many of you are familiar with this form

So, as we've mentioned before, an **OSOS Account Request Form** must be filled out for all new users, edits for users, or deactivation of a user

This form must have all User information completed before access can be given. It is important that the Security Coordinator review all of the information on the form to ensure that the users are gaining the appropriate access.

The link to this form can be found in the Accessing the System OSOS Guide, on the Department of Labor's guides page. This link opens up a fillable doc file.

OSOS Account Request Form



Date of Request:

OSOS Account Request Form

Please choose one: Add New User ☐
Edit Existing User ☐
Delete Existing User ☐

Section 1: OFFICE INFORMATION

Agency Affiliation	
Region or LWDA	
WIOA Partner Security Coordinator	
DOL Security Coordinator	

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Section 1 of the form requires the reason for submitting the form, whether adding, editing or deleting a user, as well as office information.

OSOS Account Request Form

Section 2: USER INFORMATION (* Required)

*First Name	
*Middle Initial	
*Last Name	
*Title	
*Phone	
Fax	
*E-mail OR RACF User ID	
*Supervisor	
*Assigned Office	

DVOP ☐ **LVER** ☐ **Supervisor** ☐ **General Permissions** ☐

Has this USER indicated in their signed Individual Confidentiality Agreement that they need access to OSOS, REOS, or both? OSOS ☐ REOS ☐ Both ☐

Attached Completed Cornerstones of Confidentiality form Yes ☐ No ☐

Will this USER need access to the OSOS Management Report site? Yes ☐ No ☐

NEW YORK STATE OF OPPORTUNITY. Department of Labor

The second part of the form is information about the user. Their name, title and contact information are self-explanatory.

Please verify the first and last names are spelled correctly, as that is what will show up on the bottom left hand side of the screen when they sign into OSOS.

Assigned office is the user's primary office. If the user needs multiple offices, please list them in the comments at the bottom of the Account Request Form. To ensure the appropriate office is given, please list the office name as it appears in OSOS.

There are a few categories that can be checked in this section to better identify what type of access a user may need based on their job title.
A Disabled Veterans Outreach Program Specialist, or DVOP, provides case management services as well as a full range of employment services to qualified veterans.
A Local Veterans Employment Representative, LVER, is a staff member who advocates on behalf of veterans with businesses, industry, and community organizations to promote employment and training opportunities for veterans. It is very important that you as Security Coordinators indicate if the user is a DVOP or a LVER. These

fields are used to determine if the customers served by the staff member should be included in the Jobs for Veterans State Grant performance.

Selecting the check box for Supervisor Permission will allow the user to view their staffs' inbox "reminders" in OSOS.

You can also indicate in this section if access to OSOS management reports is required. If required, it is important to note for all partner staff that each user must have an NY.GOV account as well as their OSOS account, before they will be able to access the management reports. If access to the Management Reports is requested and additional information is needed, OSOS staff may reach out to the Security Coordinator to obtain the required information in order to grant access to the user.

OSOS Account Request Form

Section 3: SECURITY PERMISSIONS

General Permissions	Services Permissions	Job Bank Permissions
(only choose **ONE** of the below)	(only choose **ONE** of the below)	(only choose **ONE** of the below)
☐ Clerical	☐ Comprehensive Assessment General	☐ Customer Match / Refer
☐ Professional	☐ Comprehensive Assessment Confidential	☐ Job Bank Match / Refer
Additional Permissions		
☐ Delete Partner Data	☐ Job Bank Master Record	☐ REOS Letter Generator
☐ Employer Activities	☐ Job Bank Monitoring / Oversight	☐ Services
☐ Employer Correspondence	☐ Job Order Create	☐ Supervisory Delete
☐ Greeter/Receptionist	☐ Provider Create	☐ Terminate WIOA / Follow Up
☐ DEI Tab	☐ REOS	☐ WIOA Monitoring / Oversight
☐ Testing	☐ Rapid Response	☐

Comments / Exceptional Circumstances:

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Section 3 of the form identifies the Security Permissions required by the user.

It is an important part of the Security Coordinator's responsibilities to ensure permissions requested are both appropriate and necessary for the user to effectively serve their customers.

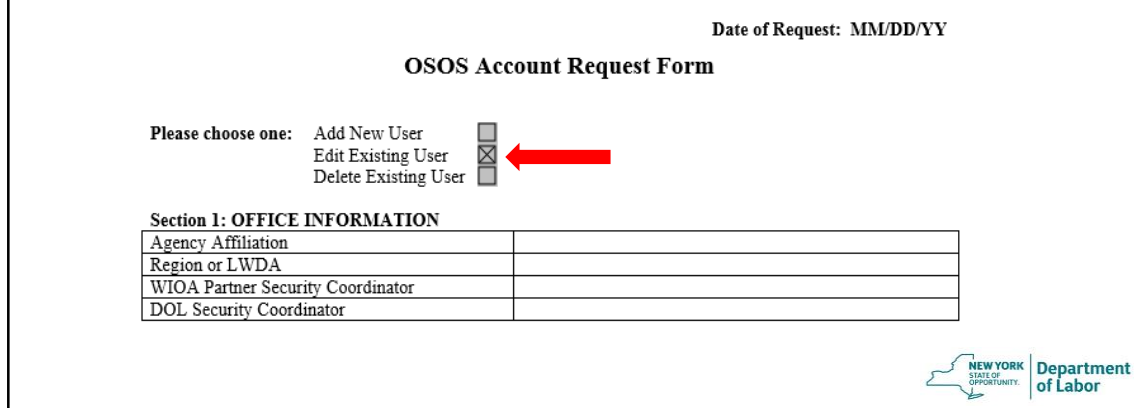
For example, a career center staff person serving youth customers will need the Services permission in order to record youth program services and follow up. Whereas, Job Order Create would be an unlikely permission for the same career center staff member.

We will be providing more detail regarding the permissions shortly.

Additionally, any comments or exceptional circumstances would be described here, at the bottom of the form. As discussed earlier, this is also where you would list additional offices that the user will need access to.

Editing Accounts

OSOS Account Request Form



Date of Request: MM/DD/YY

OSOS Account Request Form

Please choose one:
- Add New User ☐
- Edit Existing User ☒
- Delete Existing User ☐

Section 1: OFFICE INFORMATION

Agency Affiliation	
Region or LWDA	
WIOA Partner Security Coordinator	
DOL Security Coordinator	

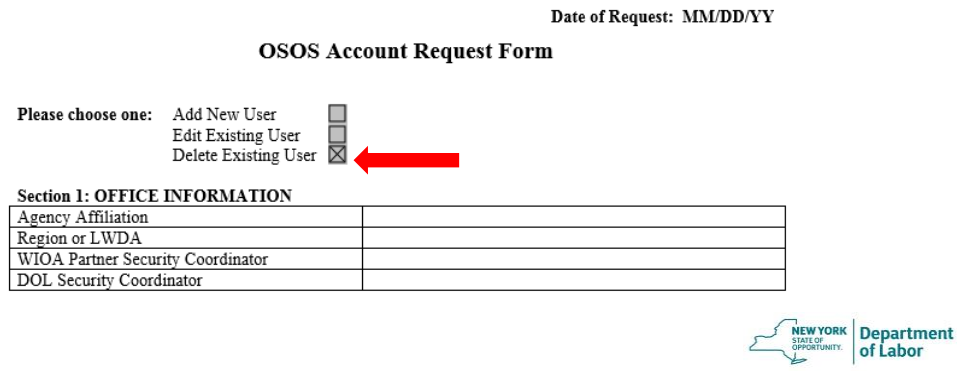
NEW YORK STATE OF OPPORTUNITY. Department of Labor

The same OSOS Account Request form is also used when Users require their account to be edited. An example of this would be when a staff member's primary office, name or contact information changes. A change in OSOS permissions may also be necessary if the staff's job duties or title changes.

In this case, the edit request would be submitted through the security coordinator, who would in turn submit an OSOS Account Request form to the OSOS Accounts mailbox, detailing the change to be made and ensuring that the Edit Existing User box is checked at the top of the page.

Deactivating Accounts

OSOS Account Request Form



Date of Request: MM/DD/YY

OSOS Account Request Form

Please choose one:
- Add New User ☐
- Edit Existing User ☐
- Delete Existing User ☒

Section 1: OFFICE INFORMATION

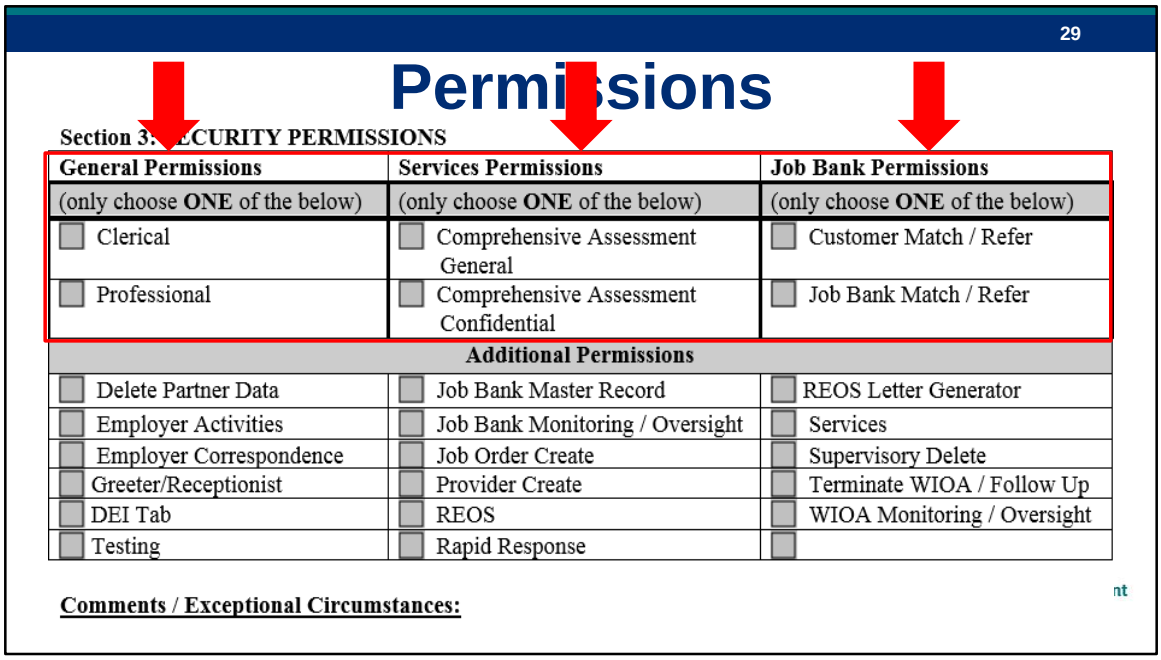
Agency Affiliation	
Region or LWDA	
WIOA Partner Security Coordinator	
DOL Security Coordinator	

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Circumstances may arise which require an OSOS account to be deactivated. The most common reason for this when the user is no longer employed by the Department of Labor or partner agency.

In this case, the security coordinator must submit the OSOS Account Request form, checking the Delete Existing User box at the top of the page and providing the user's information, as well as the reason for deactivation.

Now we want to talk in more detail about OSOS user permissions.



Let's discuss General Permissions first:

There are two options in this group – clerical and professional. Clerical provides simple data entry permissions while Professional allows the staff advanced permissions beyond basic data entry functions.

In the Services Permissions group, there are two options: Comprehensive Assessment General or Comprehensive Assessment Confidential.
The Comp Assessment Confidential permission provides full access to all enabled tabs within the Comp Assessment window.
The Comp Assessment General permission does not allow users to view information on the financial, family, or legal tabs within the Comprehensive Assessment window.

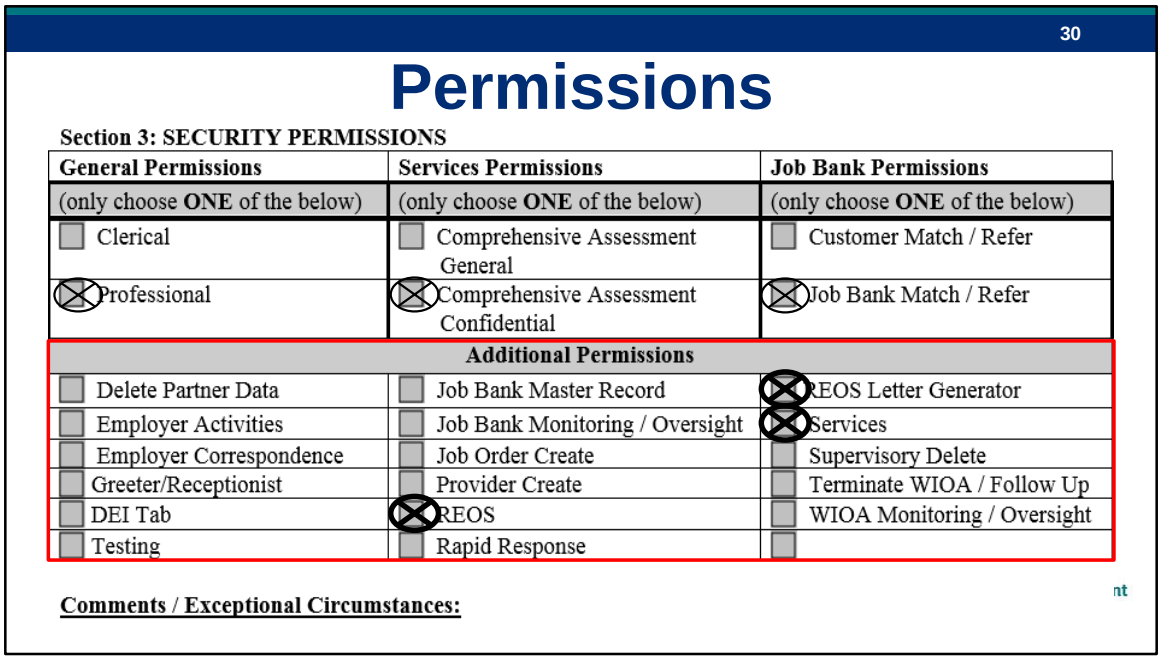
Example: An LSR or Career Advisor working with customers requires the Comp Assessment Confidential permission in order to appropriately document barriers to employment and comply with WIOA regulations.

If the clerical Permission is chosen without selecting either Comp Assessment General or Confidential, the staff person will not be able to see or access any of the

Comp Assess information.

For Job Bank Permissions:
The Customer Match/Refer permission allows staff to match a customer to potential job openings, while Job Bank Match/Refer will allow staff to match a job order to customers with relevant skill sets.
Only users with the Job Bank Match Refer permission will be able to see the match tab within the job order.

It’s important to note that only ONE permission from each of these three categories must be selected.



Moving on to the Additional Permissions…

Some career center staff may require additional permissions.

For example, a Labor Services Representative would most likely need Services, REOS and REOS Letter Generator.

The Services permission allows the user to record services in the services window of the system and attach the appropriate funding, such as adult dislocated worker or youth, for example.

The REOS permission is what grants REOS access to a user, whereas REOS Letter Generator will notify us that the user requires access to the Letter Generator for scheduling purposes.

Permissions

Section 3: SECURITY PERMISSIONS

General Permissions	Services Permissions	Job Bank Permissions
(only choose **ONE** of the below)	(only choose **ONE** of the below)	(only choose **ONE** of the below)
☐ Clerical	☐ Comprehensive Assessment General	☐ Customer Match / Refer
☒ Professional	☒ Comprehensive Assessment Confidential	☒ Job Bank Match / Refer
Additional Permissions		
☐ Delete Partner Data	☐ Job Bank Master Record	☐ REOS Letter Generator
☐ Employer Activities	☐ Job Bank Monitoring / Oversight	☒ Services
☐ Employer Correspondence	☐ Job Order Create	☐ Supervisory Delete
☐ Greeter/Receptionist	☐ Provider Create	☐ Terminate WIOA / Follow Up
☐ DEI Tab	☐ REOS	☐ WIOA Monitoring / Oversight
☒ Testing	☐ Rapid Response	☐

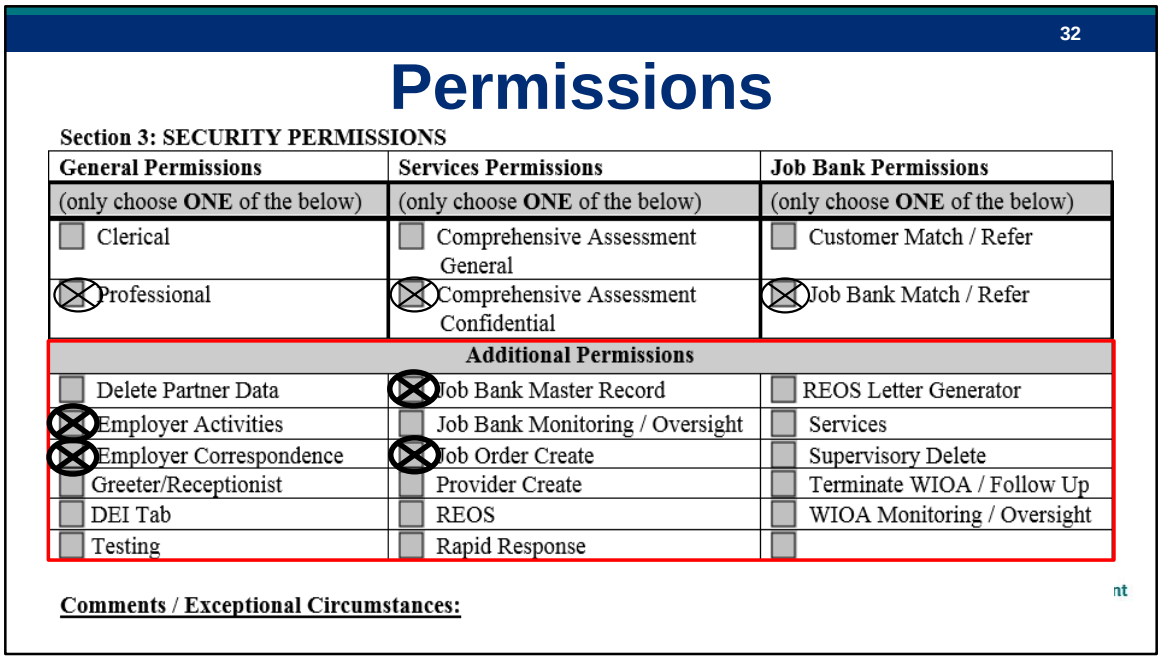
nt

Comments / Exceptional Circumstances:

A Youth Coordinator role would typically require Testing and Services.

The Testing permission allows the user to record testing results for a customer on the testing tab of the system. This also allows users to record information in the LIT/NUM pop up within the services window.

And Services, as previously mentioned, allows the user to record services in the services window of the system and attach the appropriate funding.



32

Permissions

Section 3: SECURITY PERMISSIONS

General Permissions	Services Permissions	Job Bank Permissions
(only choose **ONE** of the below)	(only choose **ONE** of the below)	(only choose **ONE** of the below)
☐ Clerical	☐ Comprehensive Assessment General	☐ Customer Match / Refer
☒ Professional	☒ Comprehensive Assessment Confidential	☒ Job Bank Match / Refer
Additional Permissions		
☐ Delete Partner Data	☒ Job Bank Master Record	☐ REOS Letter Generator
☒ Employer Activities	☐ Job Bank Monitoring / Oversight	☐ Services
☒ Employer Correspondence	☒ Job Order Create	☐ Supervisory Delete
☐ Greeter/Receptionist	☐ Provider Create	☐ Terminate WIOA / Follow Up
☐ DEI Tab	☐ REOS	☐ WIOA Monitoring / Oversight
☐ Testing	☐ Rapid Response	☐

nt

Comments / Exceptional Circumstances:

A Business Services staff member would most likely need permissions including Employer Activities, Employer Correspondence, Job Bank Master Record and Job Order Create.

Employer Activities permission allows the user to enter activities into the business jacket.

Employer Correspondence allows staff to send emails and/or letters to the Businesses through the OSOS Correspondence function.

Job Order Create allows the user to create job orders in the employer module. It does not allow the creation of the business jacket.

Job Bank Master Record is the only permission that allows users to create a new business jacket within the system. Any staff that work with businesses and are required to create business jackets must have this level of access.

Other ad hoc permissions include Delete Partner Data and Supervisory Delete. These are granted in limited circumstances and usually at the supervisor/manager level

only.

The Delete Partner Data allows users to delete funding and services from a customer record while Supervisory Delete allows users to delete activities from a customer record.

Please note that if users need information deleted from a customer record, they can always email the OSOS Help desk for assistance.

Recap

- **Security Coordinator Roles and Responsibilities**
- **OSOS/REOS Account Requirements and Forms**

NEW YORK STATE OF OPPORTUNITY. Department of Labor

To recap:
The security coordinator's role is critical to maintaining the integrity of OSOS, REOS, PII and PPSI in accordance to Technical Advisories 17-7 and 18-5.

OSOS/REOS Account requirements do vary slightly, but all user accounts require the OSOS Account Request Form, with appropriate permissions selected, and the Attestation of Completion for Cornerstone of Confidentiality. If the user is partner staff, then the Individual Access and Confidentiality Agreement is also required. All forms must be approved by the local Security Coordinator prior to submission to the OSOS Accounts mailbox.

Questions?

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Does anyone have any questions on anything that we've covered?

If you are looking for any further guidance or have any questions that we did not address in this training, you can look at our OSOS and REOS Guides located on the NYSDOL website or you can email the help box at the address listed on the screen.

We are in the process of developing a Security Coordinator guide and a desk guide that will be posted to the site upon completion.

Thank you everyone!