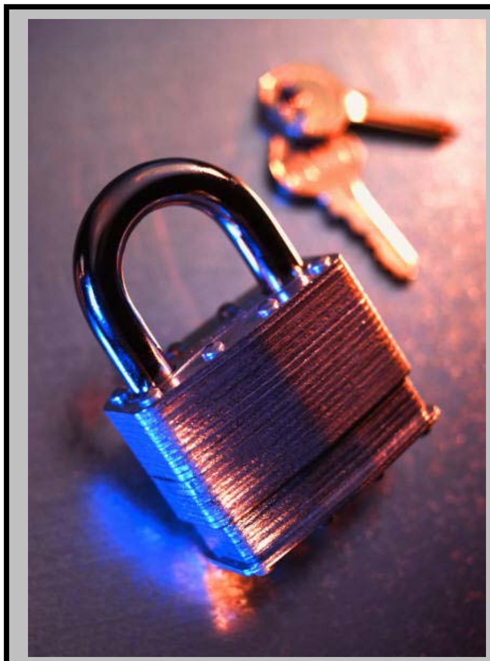


OSST

SECURITY MAINTENANCE

Agency for Workforce Innovation
Office of Workforce Program Development & Guidance

Table of Contents

OVERVIEW

Welcome to One Stop System Tracking (OSST) Security Maintenance area. A well-maintained Security System is important in order to uphold the confidentiality of customer information and allow proper access to the system. The OSST System uses secured access through the Internet to exchange information. Local regions will designate their Security Officers and only Security Officers will have access to the Security Maintenance System.

A copy of this manual can be found at AWI's Web Site at ***www2.myflorida.com/awi/pdg/osst/default.htm.***

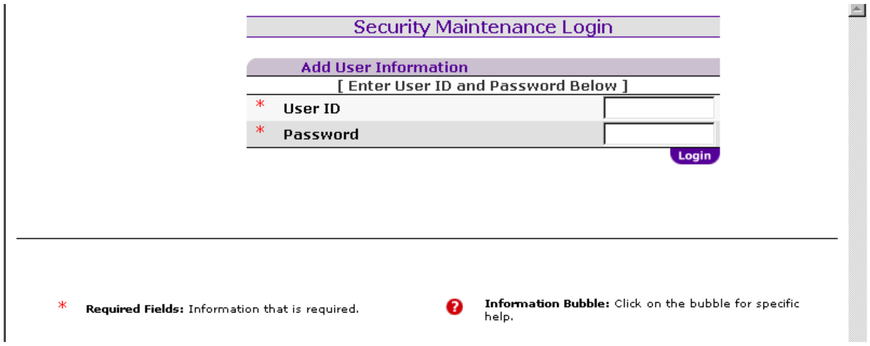
OSST Security Maintenance is designed to support regional Security Officers in the following functions:

- **Login** – It is suggested that the Security Maintenance training system be utilized for practice by Security Officers prior to attending Security Officer Training. This system allows the user an opportunity for trial and error and entries into this system do not affect the Security Maintenance area. The URL for the training environment is *https://sun13.state.fl.us/wagesct/wagestrain/casetracking/securitymaint/sm_login_dsp.cfm*. Only trained Security Officers should utilize the production Security Maintenance area. Information entered into the production environment must be authentic information only. The Security Maintenance area can be accessed using the following URL:
  https://www.myfloridajobs.com/wagesct/wagesprod/casetracking/securitymaint/sm_login_dsp.cfm
- **Maintain Units** - Includes defining new units; searching for and maintaining existing units so that cases can be assigned and tracked by Career Manager and Supervisor users.
- **Maintain Users** - Includes defining Career Manager and Supervisor users, contact information, their level of security access including which units they have security access within. The ability to search for and maintain existing user profiles is also included. Changing or resetting a user password is done from the OSST Case Tracking area at *https://www.myfloridajobs.com/casetracking/default.cfm*
- **Trigger Administration** – Explains the capability to turn on/off pre-defined correspondence triggers within OSST and how to upload regionally defined templates to use in the place of OSST defined correspondence.
- **On Line Help –** Provides help by reviewing the "contents", selecting specific topics from the "index" Help can also be obtained by entering a word(s) and using "search".
- **Log Off –** Provides instructions for proper log-off.

ACCESSING SECURITY MAINTENANCE

The security maintenance pages are accessed at a different URL than the OSST system. Only security officers will have user IDs and password access to the Security Maintenance screens.

LOGIN / LOGOFF



Security Maintenance Login

Add User Information

[Enter User ID and Password Below]

* User ID

* Password

* **Required Fields:** Information that is required.

Information Bubble: Click on the bubble for specific help.

LOGIN OSST SECURITY MAINTENANCE AT:

https://www.myfloridajobs.com/wagesct/wagesprod/casetracking/securitymaint/sm_login_dsp.cfm

Your user ID and password can be requested by contacting your current Regional Security Officer. For assistance with user IDs and passwords contact the OSST Help Desk at (850) 488-7228 ext. 2020.

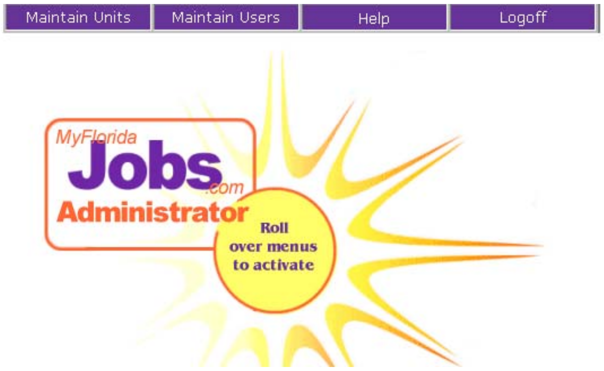
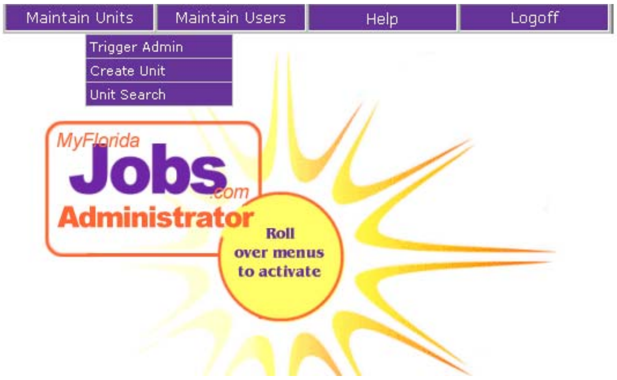
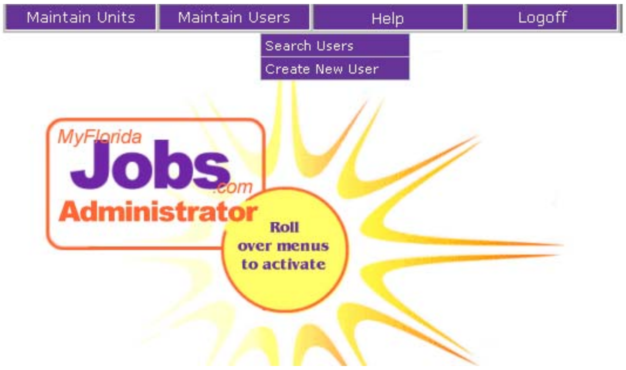
ENTER your User ID and Password.

CLICK Login

TO LOGOFF OF THE SECURITY MAINTENANCE AREA OF OSST:

CLICK on the Logoff button at the top of any page within Security Maintenance

From the Security Maintenance main page, security officers are able to access the following functions:

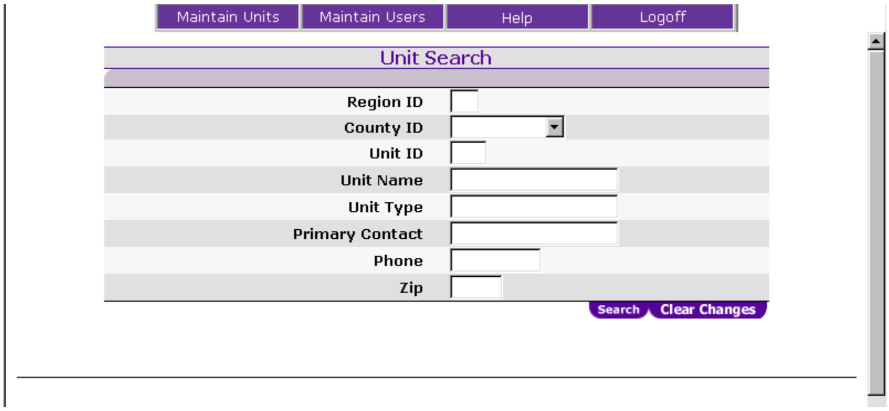
• Main Menu Navigation • Maintain Units • Maintain Users • Help • Logoff	 Maintain Units Maintain Users Help Logoff MyFlorida Jobs .com Administrator Roll over menus to activate
• Creating and Maintaining Units • Registering new units in the system • Entering unit contact information • Conducting unit searches • Viewing members of a specific unit • Correspondence Trigger Administration	 Maintain Units Maintain Users Help Logoff Trigger Admin Create Unit Unit Search MyFlorida Jobs .com Administrator Roll over menus to activate
• Creating and Maintaining Users • Registering new users in the system (including entering user contact information and setting user type) • Assigning user IDs and passwords • Editing user privileges • Associate a user with a provider	 Maintain Units Maintain Users Help Logoff Search Users Create New User MyFlorida Jobs .com Administrator Roll over menus to activate

Maintain Units

UNIT SEARCH

CONDUCTING A UNIT SEARCH

A unit search can be done by entering one or more parameters into the Unit Search function. These parameters include Region ID, County ID, Unit ID, Unit Name, Unit Type, Primary Contact, Phone and Zip code. **Associated Procedures: (Navigating from the Security Maintenance Main Page)** Position your mouse pointer over the 'Maintain Units' button at the top of the page. Click 'Unit Search'



ENTER search parameters – one or more of the following:

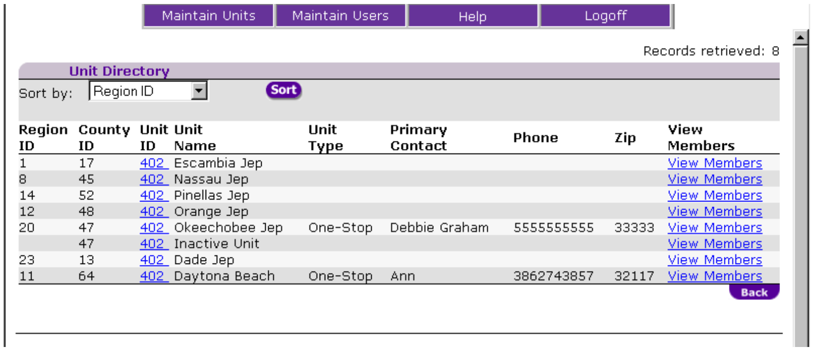
- Region ID – Identifying number of the Regional Workforce Board.
- County ID – From the drop down menu select the county in which the unit is located.
- Unit ID – Identifying number of the unit.
- Unit Name – Official title of the unit such as Alachua One Stop Center, Davie Career Center.
- Unit Type – FSET, One Stop, Summer Youth, Teen Parent, Transitional, Up front, WIA, Welfare Transition or Welfare to Work.
- Primary Contact – Name of the One Stop manager or supervisor of the unit.
- Phone and/or Zip – Main phone number or zip code for the unit.

CLICK 'Search'

VIEWING UNIT SEARCH RESULTS

The Unit Search Results page is a listing of the results that met the initial search criteria .

- Click on Unit ID to see unit information.
- Click on View Members to see individuals associated with that unit.



Records retrieved: 8

Unit Directory

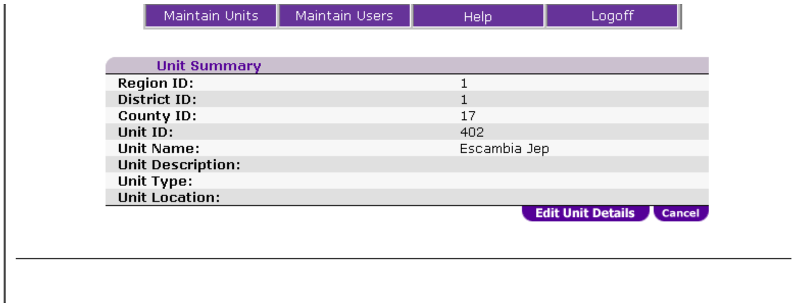
Sort by: Region ID

Region ID	County ID	Unit ID	Unit Name	Unit Type	Primary Contact	Phone	Zip	View Members
1	17	402	Escambia Jep					View Members
8	45	402	Nassau Jep					View Members
14	52	402	Pinellas Jep					View Members
12	48	402	Orange Jep					View Members
20	47	402	Okeechobee Jep	One-Stop	Debbie Graham	5555555555	33333	View Members
	47	402	Inactive Unit					View Members
23	13	402	Dade Jep					View Members
11	64	402	Daytona Beach	One-Stop	Ann	3862743857	32117	View Members

The results for Unit ID include the following information:

- Region ID
- County ID
- Unit ID
- Unit Name
- Unit Type
- Primary Contact
- Phone
- Zip

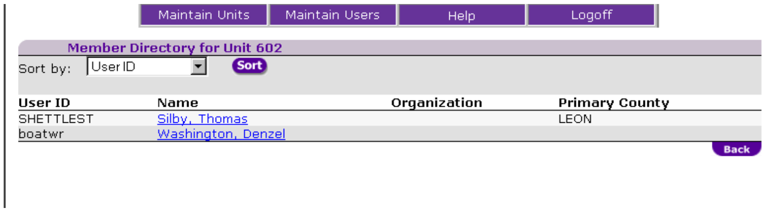
The results can be sorted and viewed by any of the above parameters.



Unit Summary

Region ID:	1
District ID:	1
County ID:	17
Unit ID:	402
Unit Name:	Escambia Jep
Unit Description:	
Unit Type:	
Unit Location:	

The results of View Members will show associates of the unit. Click on a member's name to go to that member's security profile page.



Member Directory for Unit 602

Sort by: User ID

User ID	Name	Organization	Primary County
SHETTLEST	Silby, Thomas		LEON
boatwr	Washington, Denzel		

CREATE A NEW UNIT

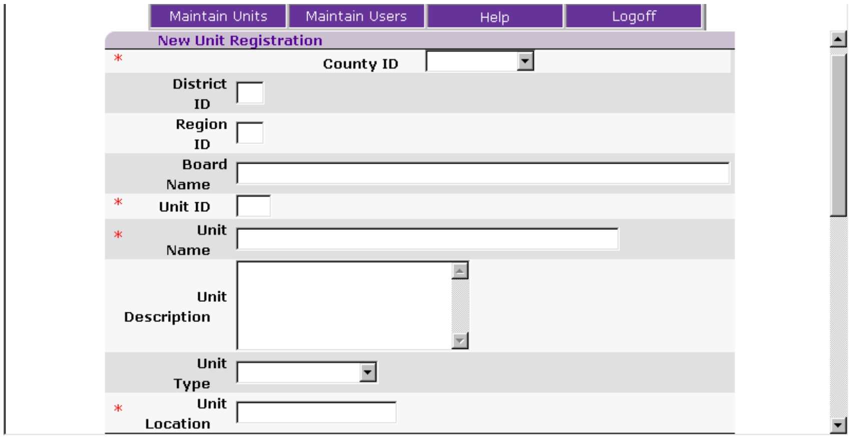
Error! Bookmark not defined.A unit is a physical location that is made up of a combination of Career Manager and Supervisor users. Regional Security Officers have the capability of defining units and the people assigned to those units in the Security Maintenance area of OSST. Creating a new unit requires the security officer to complete unit registration information (unit details) as well as unit contact information.

Associated Procedures: (Navigating from the Security Maintenance Main Page) Position your mouse pointer over the 'Maintain Units' button at the top of the page.

__NOTE:__ Unit numbers should be 700 and 800 series. After determining a number to use for a new unit do a Unit Search with the number to see if a unit already exists with that number. Manually created units may not interface with other systems such as FLORIDA or ODDS.

Unit numbers in the 500 and 600 series are reserved for FSET only and 400 series numbers are reserved for the Welfare Transition Program only. Numbers in the 100, 200 and 300 series are reserved for FTP historical purposes.

***A RED ASTERISK MARKS THE REQUIRED AREAS OF INFORMATION.**



CLICK 'Create Unit'

SELECT the county that the unit will be located in from the drop down list (based on the county selected, the district ID and region ID will be automatically populated)

ENTER the board name related to the new unit (e.g., Workforce Board of Hillsborough County, Workforce Board, Workforce Central Florida).

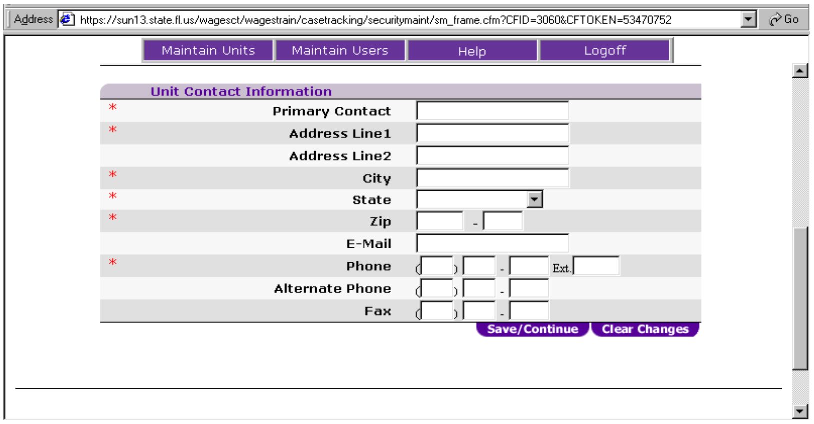
ENTER the unit ID number created for the new unit (it must be in a series of 700 or 800).

ENTER the name for the newly created unit.

ENTER a unit description (e.g., One-Stop Center, Refugee Unit).

SELECT a unit type from the drop down list.

ENTER the unit location (city or town where the unit is located).



Address https://sun13.state.fl.us/wagesct/wagestrain/casetracking/securitymaint/sm_frame.cfm?CFID=3060&CFTOKEN=53470752

Unit Contact Information

* Primary Contact	
* Address Line1	
Address Line2	
* City	
* State	
* Zip	-
E-Mail	
* Phone	( ) - Ext.
Alternate Phone	( ) -
Fax	( ) -

LOWER PAGE

ENTER the primary contact for the unit.

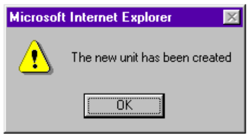
ENTER the address of the unit (including street address, city, state, and zip).

ENTER a primary contact's e-mail address (if applicable).

ENTER the primary phone number for the unit.

ENTER an alternate phone number for the unit (if applicable).

ENTER a fax number for the unit (if applicable.



Microsoft Internet Explorer

The new unit has been created

A message box will appear to inform you that the new unit has been created.

All units in existence prior to OSST Rollout will be converted from the WAGES system to the OSST system. Therefore it is not necessary to create new units unless they are needed for

Maintain Users

SECURITY PROFILE TYPES

CAREER MANAGER PROFILE

Career Manager profiles allow an individual to be granted read and write privileges to units defined within OSST. Career Managers always have a primary unit designation and may or may not have secondary units. Primary units indicate where an individual is most likely to perform their work. Secondary units may exist when a person has a need to work in more than one unit. A Career Manager's profile can also be associated with a specific provider.

ADMINISTRATIVE PROFILE

An individual with an Administrative Profile has Read-only access to OSST for the purpose of viewing application functionality and generating reports from within OSST. This type of access may be appropriate for personnel working for the administrative entity within a region, for example Regional Workforce Board Staff. This profile is created under a Career Manager profile.

SUPERVISOR PROFILE

This profile, which is selected at the time a user is defined, can be maintained (changed from Career Manager to Supervisor) from the Security Maintenance area of OSST. With a Supervisor profile, the individual when logged in to OSST, is able to see and access the caseloads of all Career Manager users associated with the same units, as defined within OSST Security Maintenance. This view is accessible via the OSST Desktop by clicking the hyperlink entitled *Workload.*_ A Supervisor's profile can also be associated with a specific provider.

Supervisors have the capability of assigning personal "To Do's" to Career Managers associated within their same units, editing/deleting case notes on cases associated with Career Managers within their same units and being designated as the Primary Supervisor when there is not one defined for their unit(s).

PRIMARY SUPERVISOR PROFILE

A Primary Supervisor will be selected by default by the system until a Security Officer defines one. Selection of the Receives Alerts checkbox defines a user as a Primary Supervisor. Once a Primary Supervisor is designated for a unit the Receives Alerts option is no longer available to any other users within that unit. The designation of Primary Supervisor means that all FLORIDA To Do's (formerly WAGES MIS Alerts) will come to that individual until the associated case is reassigned to another user of OSST. This profile is created under a Supervisor profile.

SECURITY OFFICER PROFILE

A supervisor can be identified as a Security Officer by clicking the Security Officer checkbox on the unit level profile. This action gives that individual the ability to login to the Security Administration area of OSST and reset user passwords from the OSST Login page. This Profile is created under a Supervisor profile.

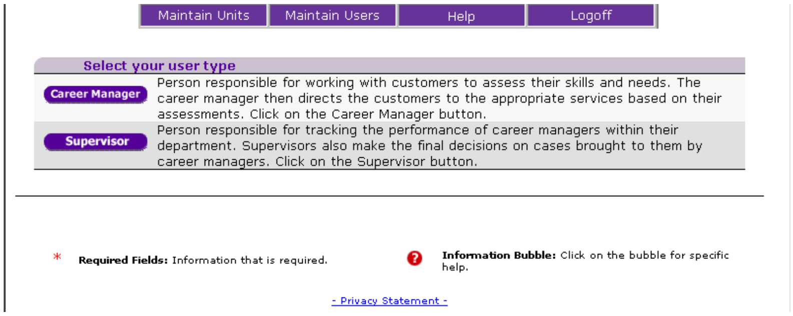
CREATING A NEW USER

Requesting a new user ID should follow a standard process in each of the regions. For example, it should be necessary to complete the associated paperwork in order to have a user added to the system. The following is a suggested list of steps to follow relative to creating a new user id:

- Determine the need for the user to have access to OSST.
- Complete the regional security access request form. (See example in Appendix)
- Document the access levels that the user is to have to determine the user's security profile.
- Ensure that the user has been signed up to attend or has attended OSST training.
- Create the user in OSST using the 'Create User' functions.

After the Security Officer receives and reviews a security access request form, the Security Officer should conduct a search in OSST to determine if there is currently an account open for the user. After determining whether an account currently exists for the user, the Security Officer can begin the process of assigning a user ID and password or sending the request form back to the supervisor with a reason for denial.

To begin adding a user, position your mouse pointer over the 'Maintain Users' button at the top of the page and click on the 'Create User' option. The first step in creating a new user is selecting the user type. There are two user types for OSST: Career Manager and Supervisor. A Career Manager is defined as "a person responsible for working with clients to assess their skills and needs. The Career Manager then directs the clients to the appropriate services based on their assessments." A Supervisor is defined as "a person responsible for tracking the performance of Career Managers within their department. Supervisors also make the final decisions on cases brought to them by Career Managers." After selecting user type, the Security Officer is then prompted to create a user ID and a password for the user.



Select your user type

Career Manager: Person responsible for working with customers to assess their skills and needs. The career manager then directs the customers to the appropriate services based on their assessments. Click on the Career Manager button.

Supervisor: Person responsible for tracking the performance of career managers within their department. Supervisors also make the final decisions on cases brought to them by career managers. Click on the Supervisor button.

* **Required Fields:** Information that is required.

Information Bubble: Click on the bubble for specific help.

- Privacy Statement -

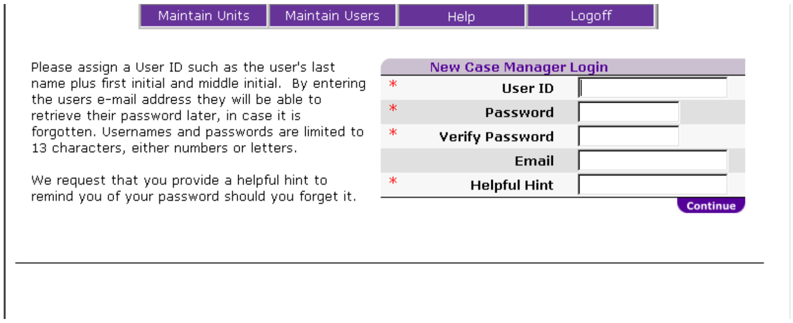
SELECT the user type (case manager or supervisor)

❖ Career Managers

- Administrative

❖ Supervisor

- Primary Supervisors
- Security Officers



Please assign a User ID such as the user's last name plus first initial and middle initial. By entering the users e-mail address they will be able to retrieve their password later, in case it is forgotten. Usernames and passwords are limited to 13 characters, either numbers or letters.

We request that you provide a helpful hint to remind you of your password should you forget it.

New Case Manager Login

* User ID

* Password

* Verify Password

Email

* Helpful Hint

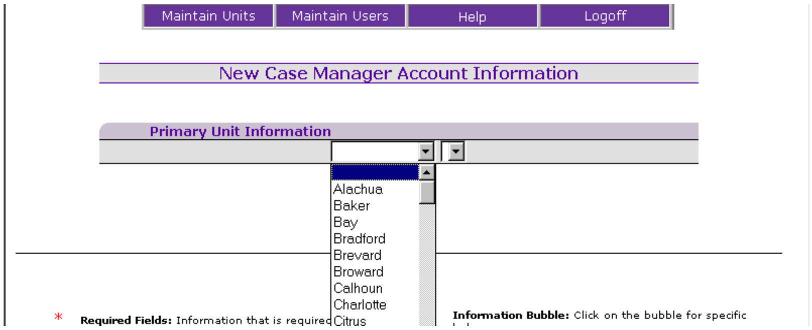
ASSIGN the user ID – Generally last name and the first and middle initial.

ASSIGN the user a password.

VERIFY the user's password by re-entering it. Users should be advised to change their password when they login the first time.

ENTER the user's e-mail address.

ENTER a helpful hint as a prompt for the user's password.

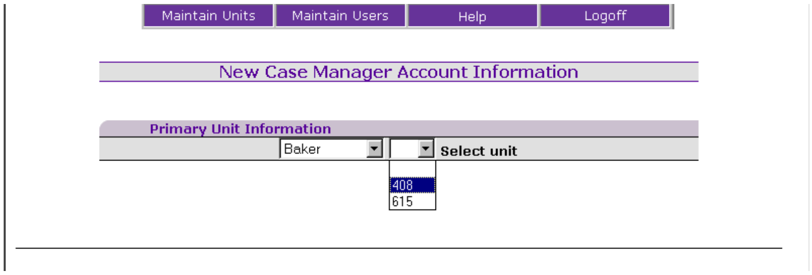


New Case Manager Account Information

Primary Unit Information

* **Required Fields:** Information that is required

Information Bubble: Click on the bubble for specific



New Case Manager Account Information

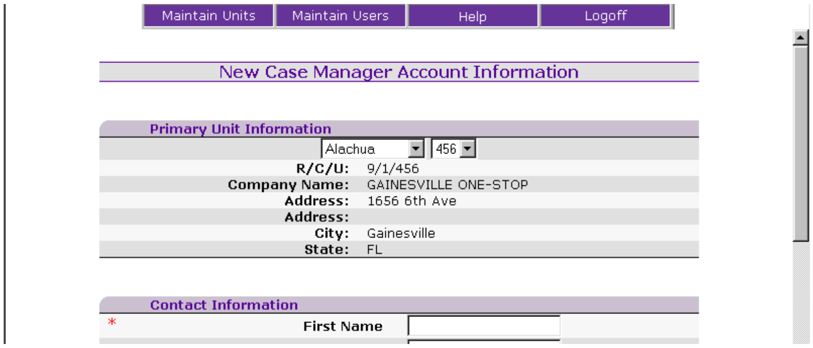
Primary Unit Information

Baker Select unit

SELECT primary unit information County name and unit number. After the county is selected the screen will automatically refresh and a drop down menu with unit numbers will become available. The Security Officer will have access to only those counties and units within his/her assigned region(s).

ENTERING ACCOUNT INFORMATION FOR A NEW USER

This page will prompt you to enter information related to the user's primary unit and contact information. The Region/County/Unit (R/C/U) name and address is automatically populated.



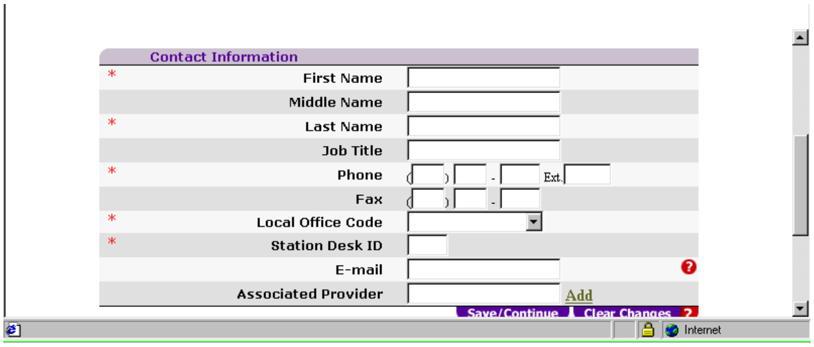
New Case Manager Account Information

Primary Unit Information

	Alachua 456
R/C/U:	9/1/456
Company Name:	GAINESVILLE ONE-STOP
Address:	1656 6th Ave
Address:	
City:	Gainesville
State:	FL

Contact Information

* First Name	



Contact Information

* First Name	
Middle Name	
* Last Name	
Job Title	
* Phone	( ) - Ext.
Fax	( ) -
* Local Office Code	
* Station Desk ID	
E-mail	
Associated Provider	Add

ENTER the user's first, middle and last name.

ENTER the user's job title.

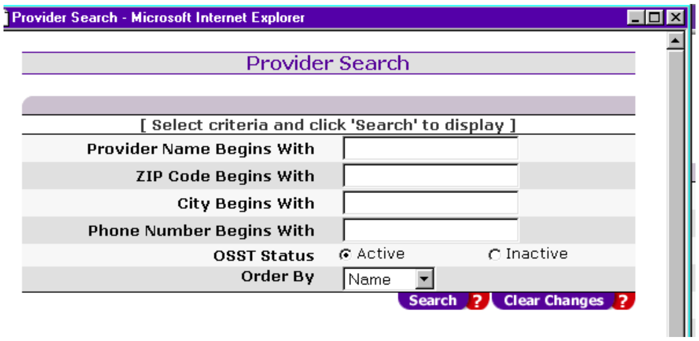
ENTER the user's phone number.

ENTER the user's fax number

SELECT the local office code from the drop down menu. This should be the user's primary unit.

ENTER the user's station desk ID number. Use the same station desk ID number previously assigned to the user.

ENTER the provider to which the user is associated with if applicable



Provider Search - Microsoft Internet Explorer

Provider Search

[Select criteria and click 'Search' to display]

Provider Name Begins With	
ZIP Code Begins With	
City Begins With	
Phone Number Begins With	
OSST Status	● Active ○ Inactive
Order By	Name

TO PERFORM AN ASSOCIATED PROVIDER SEARCH:

CLICK on "Add" to the right of the Associated Provider box

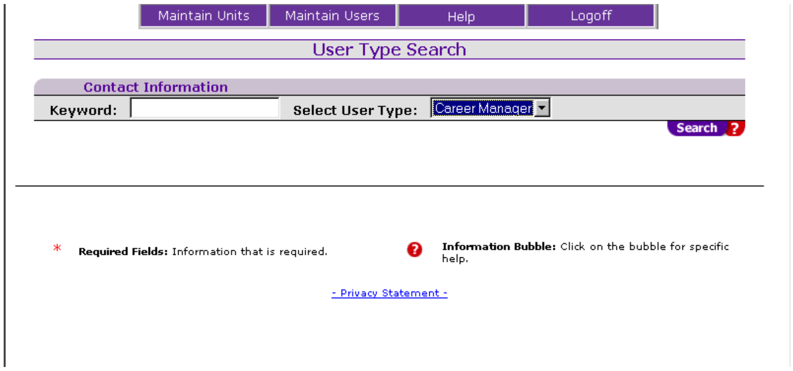
ENTER the search criteria in the Provider Search box.

THE SEARCH CRITERIA CAN BE:

- The first letter of the provider's name.
- The beginning of the zip code.
- The first letter of the city where the provider is located.

The OSST Status is active by default. Inactive can be selected if provider has not been activated in the OSST system. The provider information must be in Case Tracking for a search to locate the provider. If no information is found on a provider, go to Case Tracking and enter the necessary information.

SEARCH FOR A USER



User Type Search

Contact Information

Keyword: 　Select User Type: Career Manager

* Required Fields: Information that is required.

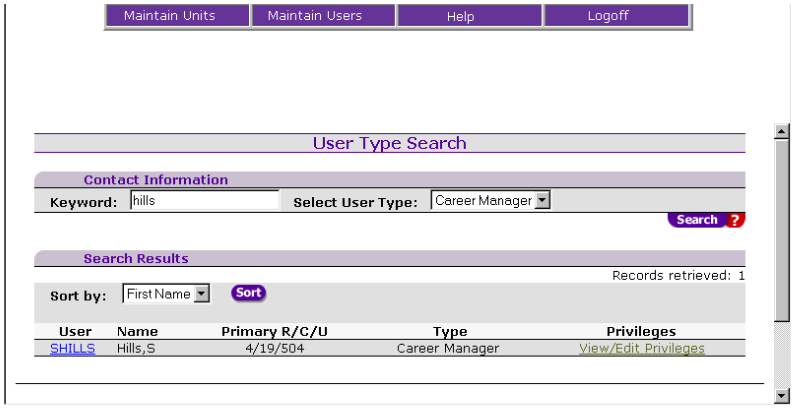
Information Bubble: Click on the bubble for specific help.

- Privacy Statement -

VERIFYING ACCOUNT INFORMATION FOR A NEW USER

After entering the user's primary unit information and contact information, the Security Officer will be prompted by the User Search screen.   Enter a keyword to search. A keyword is the last name, first name or user ID of the user.

The purpose of this function is to conduct a search to verify that the user has been added to the system. Additionally, from this screen the security officer can link to 'View/Edit Privileges' for a new user or edit user information by clicking on the user's ID.



User Type Search

Contact Information

Keyword: hills　Select User Type: Career Manager

Search Results

Records retrieved: 1

Sort by: First Name

User	Name	Primary R/C/U	Type	Privileges
SHILLS	Hills,S	4/19/504	Career Manager	View/Edit Privileges

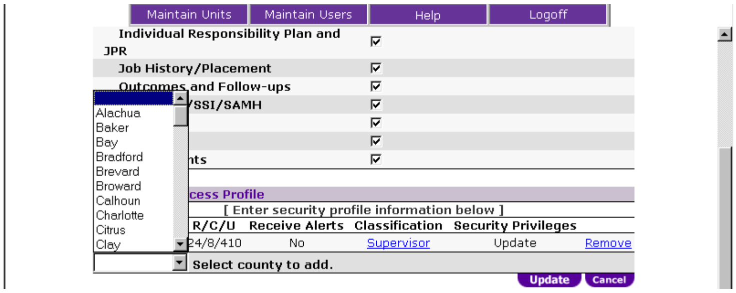
USER INFORMATION WHICH CAN BE EDITED:

- Name
- Job title
- Phone
- Fax
- E-mail
- Local office
- Station Desk ID
- Associated provider

SECURITY PROFILE PRIVILEGES

PRIMARY/SECONDARY UNIT DESIGNATION

A Primary Unit is defined as the unit where a user will perform most responsibilities. Secondary Units are all other units to which the user has security access. For example, a region consisting of three counties with one unit in each county will grant access to a user in one of those counties and designate it as the primary unit. Other units added to the user's profile, like the other two units/counties in the example above, are automatically considered secondary units even though the security rights may be set exactly the same in all units.



Individual Responsibility Plan and JPR ☑

Job History/Placement ☑

Outcomes and Follow-ups ☑

/SSI/SAMH ☑

☑

☑

nts ☑

cess Profile

[Enter security profile information below]

R/C/U	Receive Alerts	Classification	Security Privileges	
24/8/410	No	Supervisor	Update	Remove

Select county to add.

TO ADD A UNIT TO A USER PROFILE:

FIND the user by following the 'Search Users' procedure.

SELECT the county in which the unit exists. The page will refresh to indicate which units currently exist in that region/county. If the unit is not listed, it does not exist. To add a new unit, follow the Create Unit procedure.

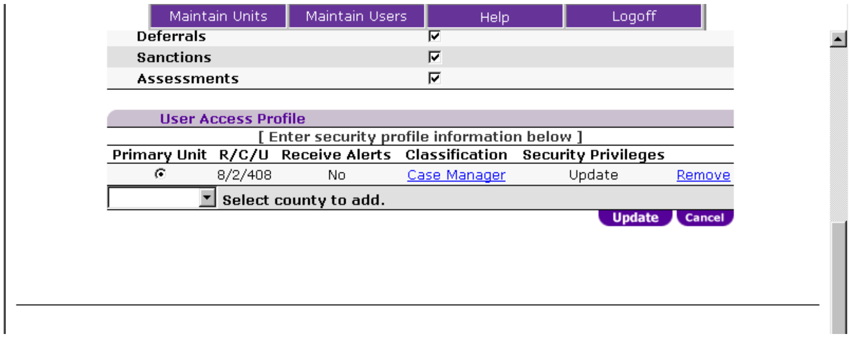
SELECT the unit to which the user is to be given access.

SELECT the User type for the user within that unit. Options are: Career Manager and Supervisor.

CHECK the Update Authority checkbox if the user should have update rights to cases in that unit.

CHECK the Security Officer checkbox if the user should be a Security Officer. If no Primary Supervisor exists and this individual should be the one to receive FLORIDA To Do's for unassigned cases, check the Receives Alerts checkbox. **NOTE:** This action updates the Receive Alerts column from No to Yes. An individual must be a Supervisor before he/she can be identified as a Primary Supervisor.

CLICK the 'Update' button to save the changes to the profile.



Deferrals	☑
Sanctions	☑
Assessments	☑

User Access Profile

[Enter security profile information below]

Primary Unit	R/C/U	Receive Alerts	Classification	Security Privileges	
●	8/2/408	No	Case Manager	Update	Remove

Select county to add.

TO CHANGE A PRIMARY UNIT DESIGNATION

FIND the user by following the ‘Search Users’ procedure.

CLICK the ‘View/Edit Privileges’ hyperlink.

CLICK the radio button next to the unit to be designated as the user’s primary unit.

CLICK the ‘Update’ button to save the changes to the profile.

GRANTING SECURITY RIGHTS

OSST provides the capability of defining a user's security access within a primary and one or more secondary units where work is accomplished. Security access has a few key components as described here:

UNIT ACCESS - The units an individual has access to for case management purposes.

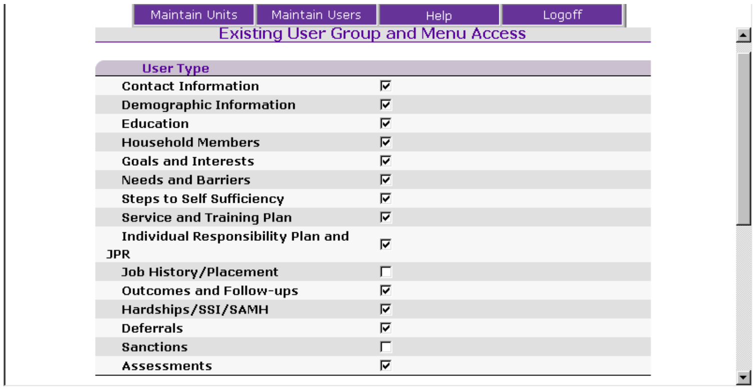
READ/UPDATE ACCESS - The ability within assigned units to either read (view only) or update (view and maintain) cases.

BUSINESS FUNCTION ACCESS - Beyond read/update access, OSST enables security rights to be set for specific business functions. For example, a user who works as an administrative assistant may be given rights to update contact and demographic information but there may not be a need for that individual to request a sanction for cases in the unit. This example is accommodated by OSST, however, the rights are globally set across all assigned units for the individual. Therefore, removal of sanction-write access will apply to all units to which the individual has access.

TO GRANT A USER SECURITY RIGHTS:

FIND the user by following the 'Search Users' procedure.

CLICK the 'View/Edit Privileges' hyperlink.

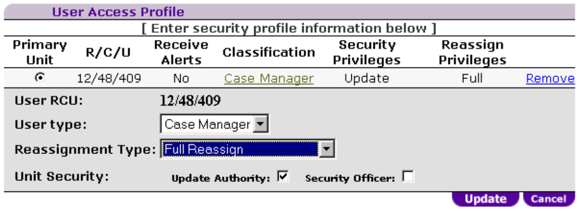


Existing User Group and Menu Access

User Type	
Contact Information	☑
Demographic Information	☑
Education	☑
Household Members	☑
Goals and Interests	☑
Needs and Barriers	☑
Steps to Self Sufficiency	☑
Service and Training Plan	☑
Individual Responsibility Plan and JPR	☑
Job History/Placement	□
Outcomes and Follow-ups	☑
Hardships/SSI/SAMH	☑
Deferrals	☑
Sanctions	□
Assessments	☑

On the Existing User Group and Menu Access page, check the business functions for which the individual will have global update authority in all the units where update authority exists. On the Existing User Group and Menu Access page, uncheck the business functions for which the individual will not have global read authority in the units where read/update authority exists. The Security Officer can edit the user authority for only the users in the units for his/her region.

On the User Access Profile section of the page ensure the classification is appropriate. To change, click on the classification hyperlink and select the appropriate user type for that specific unit from the user type drop down list box.



User Access Profile

[Enter security profile information below]

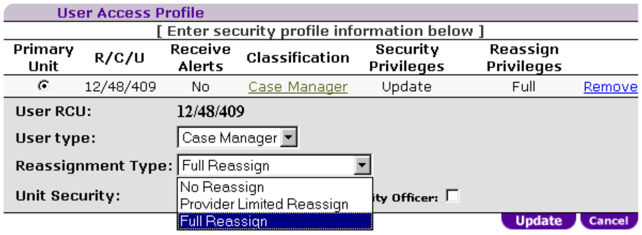
Primary Unit	R/C/U	Receive Alerts	Classification	Security Privileges	Reassign Privileges	
●	12/48/409	No	Case Manager	Update	Full	Remove

User RCU: 12/48/409

User type: Case Manager

Reassignment Type: Full Reassign

Unit Security: Update Authority: ☑ Security Officer: □



User Access Profile

[Enter security profile information below]

Primary Unit	R/C/U	Receive Alerts	Classification	Security Privileges	Reassign Privileges	
●	12/48/409	No	Case Manager	Update	Full	Remove

User RCU: 12/48/409

User type: Case Manager

Reassignment Type: Full Reassign

Unit Security: ity Officer: □

SELECT one of the three options for Reassignment Type from the drop down list. A Full Reassign type may reassign any cases within the unit. The Provider Limited Reassign type may reassign only the cases in a unit of the provider to which that user is associated. A user must be associated with a Provider before the system will allow the Provider Limited Reassign option. No Reassign denies any case reassignment privileges for that unit.

CHECK the Update Authority checkbox if the user should have update rights to cases in that unit.

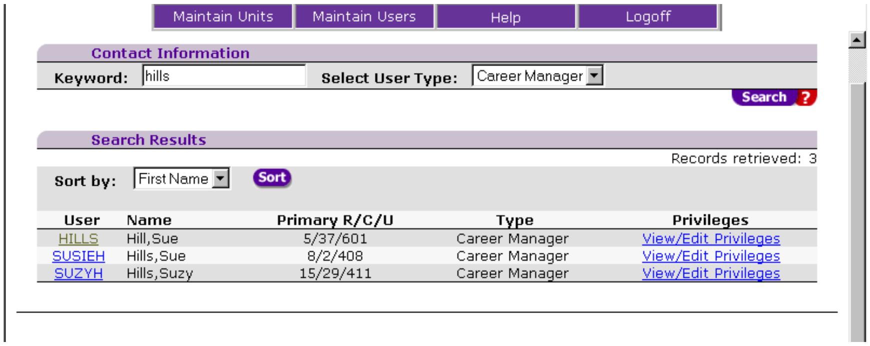
CHECK the Security Officer checkbox if the user should be considered a Security Officer. The user type must be supervisor before being assigned security officer privileges.

CHECK the Receives Alerts checkbox if the individual will be receiving FLORIDA To Do's for unassigned cases in units where no Primary Supervisor exists. **Note**: This action updates the Receive Alerts column from No to Yes. An individual must be a Supervisor before being identified as a Primary Supervisor.

CLICK THE 'UPDATE' button to save the changes to the profile.

REMOVING SECURITY RIGHTS

There will be situations where a user should no longer have access to cases within a unit. For example, a Career Manager may move to another unit or no longer work for a unit. OSST Security Maintenance allows unit access to be removed. Users who no longer work for any unit must be removed from all units, effectively removing them from the system. It is important to remember to remove security officer privileges of users who are no longer assigned that duty. However, if a user is rehired, the same user ID cannot be reused. The reason for this is to maintain the integrity of any historical records created by that user. The user is never fully eliminated from the system even though access to read/update cases in units is revoked. In the case where a previously existing user was removed and needs to have security rights reinstated, a new user ID and password must be created using the Create New User procedure. If a user is removed from a unit, any cases assigned to that user will automatically be reassigned to the Primary Supervisor who will have to reassign those cases to other Career Managers.



Contact Information

Keyword: hills   Select User Type: Career Manager

Search Results

Records retrieved: 3

Sort by: First Name

User	Name	Primary R/C/U	Type	Privileges
HILLS	Hill,Sue	5/37/601	Career Manager	View/Edit Privileges
SUSIEH	Hills,Sue	8/2/408	Career Manager	View/Edit Privileges
SUZYH	Hills,Suzy	15/29/411	Career Manager	View/Edit Privileges

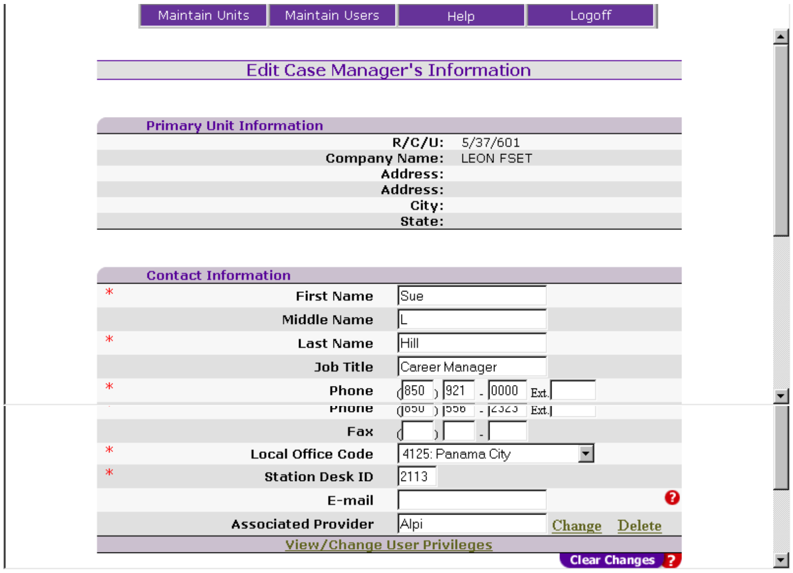
TO REMOVE SECURITY RIGHTS FOR A USER IN A SPECIFIC UNIT:

FIND the user by following the 'Search Users' procedure.

CLICK the 'View/Edit Privileges' hyperlink.

CLICK the 'Remove' hyperlink on the record of the unit for which security rights need to be entirely revoked.

CLICK the 'Update' button to save the changes to the profile.



Edit Case Manager's Information

Primary Unit Information

R/C/U:	5/37/601
Company Name:	LEON FSET
Address:	
Address:	
City:	
State:	

Contact Information

*	First Name	Sue
	Middle Name	L
*	Last Name	Hill
	Job Title	Career Manager
*	Phone	(850) 921 - 0000 Ext.
	Phone	(850) 556 - 2323 Ext.
	Fax	( ) -
*	Local Office Code	4125: Panama City
*	Station Desk ID	2113
	E-mail	
	Associated Provider	Alpi

EDITING USER PRIVILEGES

The menu access page allows the security officer to edit the areas within OSST where a user is permitted update access. From this page, a security officer can also update a user's access profile (primary, secondary R/C/U) and information.

CLICK on field in 'Contact Information' - delete and add correct information.

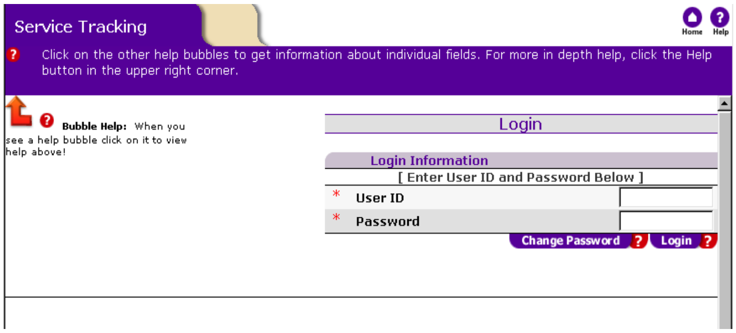
CLICK 'Change' or 'Delete' to edit the "Associated Provider' information. Clicking on 'Change' will bring up the provider search screen. 'Delete' will remove the associated provider.

CLICK 'View/Change User Privileges' to get to the screen with user privileges. Check and uncheck appropriate boxes on user privileges.

RESETTING USER PASSWORDS

Users have the ability to change their own passwords. This is done from the OSST Service Tracking Login screen. If a user forgets his/her password, there is functionality that allows the security officer to reset the password. Resetting a user's password is not done within the Security Maintenance pages.

Instead, a security officer accesses this functionality through the OSST login screen using his/her security user ID and password.



Click on the other help bubbles to get information about individual fields. For more in depth help, click the Help button in the upper right corner.

Bubble Help: When you see a help bubble click on it to view help above!

Login Information

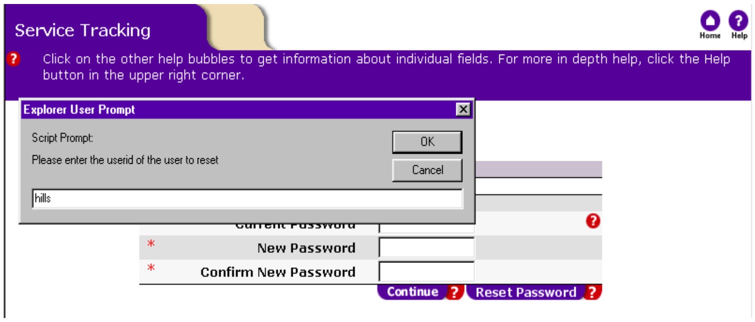
[Enter User ID and Password Below]

* User ID	
* Password	

FROM YOUR BROWSER, GO TO:

https://www.myfloridajobs.com/casetracking/default.cfm

ENTER your user ID and password and click 'Reset Password' tab. **<u>DO NOT LOGIN</u>**



Click on the other help bubbles to get information about individual fields. For more in depth help, click the Help button in the upper right corner.

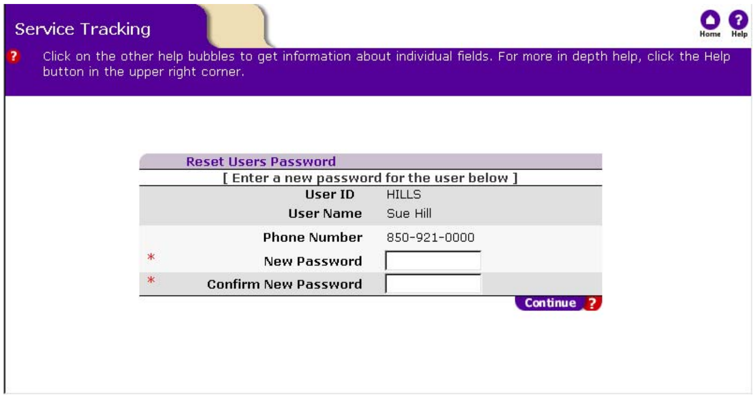
Script Prompt:

Please enter the userid of the user to reset

hills

Current Password	
* New Password	
* Confirm New Password	

ENTER the user ID for the password that needs to be changed in the space on the 'Explorer User Prompt' box and click 'OK'.



Click on the other help bubbles to get information about individual fields. For more in depth help, click the Help button in the upper right corner.

Reset Users Password

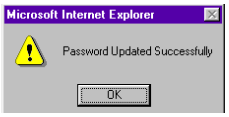
[Enter a new password for the user below]

User ID	HILLS
User Name	Sue Hill
Phone Number	850-921-0000
* New Password	
* Confirm New Password	

ENTER a new password and confirm it by re-entering the same password.

CLICK the 'Continue' tab.

The user should be advised to change the password the first time he/she logs on.



Password Updated Successfully

A Pop-up message will advise that the password has been changed.

HELPFUL TIPS:

Tip 1: The process to request that a user password be reset may vary according to the local region's procedures (e.g. phone call vs e-mail based request).

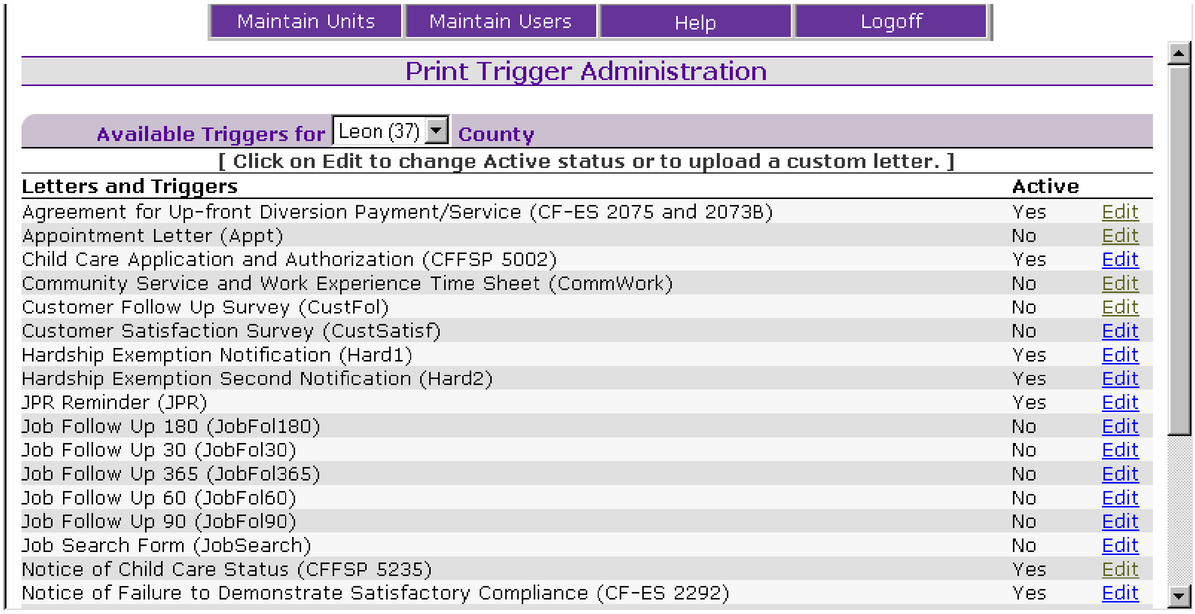
Tip 2: After resetting a password, encourage the user to change the password after logging in for the first time.

Tip 3: The user should contact the Security Officer directly to have a password reset.

Correspondence Trigger Administration

CREATING AND UPLOADING LOCAL CORRESPONDENCE

Local correspondence can be created and uploaded to replace any of the letters that are currently printed when a trigger is encountered in OSST. Uploading replacement correspondence changes the correspondence *county-wide*. Replacement correspondence cannot be done on a unit by unit basis.



Print Trigger Administration

Available Triggers for Leon (37) County

[Click on Edit to change Active status or to upload a custom letter.]

Letters and Triggers	Active	
Agreement for Up-front Diversion Payment/Service (CF-ES 2075 and 2073B)	Yes	Edit
Appointment Letter (Appt)	No	Edit
Child Care Application and Authorization (CFFSP 5002)	Yes	Edit
Community Service and Work Experience Time Sheet (CommWork)	No	Edit
Customer Follow Up Survey (CustFol)	No	Edit
Customer Satisfaction Survey (CustSatisf)	No	Edit
Hardship Exemption Notification (Hard1)	Yes	Edit
Hardship Exemption Second Notification (Hard2)	Yes	Edit
JPR Reminder (JPR)	Yes	Edit
Job Follow Up 180 (JobFol180)	No	Edit
Job Follow Up 30 (JobFol30)	No	Edit
Job Follow Up 365 (JobFol365)	No	Edit
Job Follow Up 60 (JobFol60)	No	Edit
Job Follow Up 90 (JobFol90)	No	Edit
Job Search Form (JobSearch)	No	Edit
Notice of Child Care Status (CFFSP 5235)	Yes	Edit
Notice of Failure to Demonstrate Satisfactory Compliance (CF-ES 2292)	Yes	Edit

The letters that currently exist in OSST (and their associated triggers) are listed in the following table:

Correspondence Letter/Trigger Descriptions

Letters		Page	Triggers
1	Agreement for Up-front Diversion Payment/Service (CF-ES 2075 and 2073B)	**Services**	When a case manager adds an Upfront Diversion Service.
2	Appointment Letter (Appt)	**Training/Activities**	When a case manager adds an activity or training.
3	Child Care Application and Authorization (CFFSP 5002)	**Services**	When a case manager creates a welfare transition, or transitional child care service
4	Community Service and Work Experience Time Sheet (CommWork)	**Services**	When a case manager schedules a client for Community Service Work Experience or Work Experience.
5	Customer Follow Up Survey (CustFol)	**N/a**	No trigger, accessible through search functions.

6	Customer Satisfaction Survey (CustSatisf)	**N/a**	No trigger, accessible through search functions.
7	FSET Employment Verification (EmpVerFSET)	**N/a**	No trigger, accessible through search functions.
8	FSET Failure to Comply (4165)9	**Sanctions**	Triggers when a request for sanction of an FSET client is processed.
9	FSET Job Search Report (4133)	**N/a**	No trigger, accessible through search functions.
10	FSET Opportunities and Obligations (OandOFSET)	**Training**	Triggers when a case manager adds an Orientation Activity in an FSET Unit.
11	FSET Orientation (4159)	**Training**	Triggers when a case manager adds an Orientation Activity in an FSET Unit.
12	FSET Referral (4163)	**Training**	Triggers when a referral to JEP is added in an FSET Unit.
13	Hardship Exemption Notification (Hard1)	**Hardships**	When a case manager creates hardship entry entering first hardship date and appointment date
14	Hardship Exemption Second Notification (Hard2)	**Hardships**	When a case manager creates hardship entry entering second hardship date and appointment date.
15	JPR Reminder (JPR)	**N/a**	No trigger, accessible through search functions.
16	Job Follow Up 180 (JobFol180)	**Job Placement**	When a 180 day follow-up is added on a job placement.
17	Job Follow Up 30 (JobFol30)	**Job Placement**	When a 30 day follow-up is added on a job placement.
18	Job Follow Up 365 (JobFol365)	**Job Placement**	When a 365 day follow-up is added on a job placement.
19	Job Follow Up 60 (JobFol60)	**Job Placement**	When a 60 day follow-up is added on a job placement.
20	Job Follow Up 90 (JobFol90)	**Job Placement**	When a 90 day follow-up is added on a job placement.
21	Job Search Form (JobSearch)	**Training**	When a case manager creates job search activity.
22	Notice of Child Care Status (CFFSP 5235)	**Services**	When a case manager ends a welfare transition, or transitional child care service.
23	Notice of Failure to Demonstrate Satisfactory Compliance (CF-ES 2292)	**Sanctions**	When a case manager creates a sanction requesting a penalty.
24	Notice of Failure to Participate and Possible Sanction (CF-ES 2290)	**Sanctions**	When a case manager creates a sanction requesting a pre-penalty.
25	Relocation Form (Rel)	**Services**	When a case manager creates a relocation service from the Services page.
26	Request for Assessment (Assessment)	**Assessments**	When an assessment is created.
27	Request for Medical Verification (MedVer)	**Deferrals**	Create deferral using reason medical deferral (less than 90 days) or medical deferral (90 days or more).
28	School Attendance Time Sheet (SchoolTime)	**Training**	Create employment related education, vocational education (primary), GED /high school (transitional) training
29	Service with Expense (ServExp)	**Services**	When a service is created with expense greater than 0.
30	Training with Expense (TrainExp)	**Services**	when a training entry is created with expense greater than 0.
31	Transitional Letter (Trans)	**Demographics**	When changing a client to TS status.
32	Transitional Services Reminder at Placement (TransJob)	**Job Placement**	When a job placement is created for a transitional client.

Because the correspondence administration is included on the Security Maintenance screens, local correspondence can only be uploaded by a Security Officer.

Any of the letters in the table above can be replaced with local correspondence templates by following these steps:

STEP 1: CREATE A LETTER IN MICROSOFT WORD.

Information that is generic to all customers or all units can be entered by typing the letter text in the same way a normal document is prepared; however, when entering information that is specific to a customer or a case manager (such as First Name, Last Name, or Case Manager's phone number), the variables within the following table should be used. There are 83 variables defined. These variables map to the customer and unit data stored in OSST and are the only variables that can be used when creating local correspondence. When you type the variables into the letter text, be sure to type them exactly as they appear in this table (% signs included).

	Variable	Definition
1	%DATE%	Date (System date will populate the letter if this variable is used)
2	%FNAME%	Customer's First Name
3	%LNAME%	Customer's Last Name
4	%MI%	Customer's Middle Initial
5	%ADDRESS1%	Customer's First line of his/her living address
6	%ADDRESS2%	Customer's Second line of his/her living address (e.g., Apt #)
7	%CITY%	Customer's City of residence (as listed in his/her primary contact information)
8	%STATE%	Customer's State of residence (as listed in his/her primary contact information)
9	%ZIPCODE%	Customer's zipcode (as listed in his/her primary contact information)
10	%RFA%	Customer's RFA (Request for Assistance) Number
11	%SSN%	Customer's Social Security Number
12	%DOB%	Customer's Date of Birth
13	%SEX%	Customer's gender
14	%RACE%	Customer's race
15	%INFRACTION1%	Pre-Penalty Reason for a Sanction
16	%INFRACTIONDATE1%	Pre-Penalty Date for a Sanction
17	%INFRACTION2%	Request for Penalty Reason for a Sanction
18	%INFRACTIONDATE2%	Request for Penalty Date for a Sanction

19	%SANCLEVEL%	Customer's Sanction Level
20	%DATEPLUS10%	Ten Days from Current Date
21	%DATEPLUS90%	Ninety Days from Current Date
22	%CHILD1%	Name of child #1
23	%CHILDSSN1%	Social Security Number for child #1
24	%CHILDDOB1%	Date of Birth for child #1
25	%CHILDSEX1%	Gender of child #1
26	%CHILDRACE1%	Race of child #1
27	%CHILD2%	Name of child #2
28	%CHILDSSN2%	Social Security Number for child #2
29	%CHILDDOB2%	Date of Birth for child #2
30	%CHILDSEX2%	Gender of child #2
31	%CHILDRACE2%	Race of child #2
32	%CHILD3%	Name of child #3
33	%CHILDSSN3%	Social Security Number for child #3
34	%CHILDDOB3%	Date of Birth for child #3
35	%CHILDSEX3%	Gender of child #3
36	%CHILDRACE3%	Race of child #3
37	%CHILD4%	Name of child #4
38	%CHILDSSN4%	Social Security Number for child #4
39	%CHILDDOB4%	Date of Birth for child #4
40	%CHILDSEX4%	Gender of child #4
41	%CHILDRACE4%	Race of child #4
42	%CHILD5%	Name of child #5
43	%CHILDSSN5%	Social Security Number for child #5
44	%CHILDDOB5%	Date of Birth for child #5
45	%CHILDSEX5%	Gender of child #5
46	%CHILDRACE5%	Race of child #5
47	%CHILD6%	Name of child #6
48	%CHILDSSN6%	Social Security Number for child #6
49	%CHILDDOB6%	Date of Birth for child #6
50	%CHILDSEX6%	Gender of child #6
51	%CHILDRACE6%	Race of child #6
52	%CHILD7%	Name of child #7
53	%CHILDSSN7%	Social Security Number for child #7
54	%CHILDDOB7%	Date of Birth for child #7
55	%CHILDSEX7%	Gender of child #7
56	%CHILDRACE7%	Race of child #7
57	%CHILD8%	Name of child #8
58	%CHILDSSN8%	Social Security Number for child #8
59	%CHILDDOB8%	Date of Birth for child #8
60	%CHILDSEX8%	Gender of child #8

61	%CHILDRACE8%	Race of child #8
62	%CHILD9%	Name of child #9
63	%CHILDSSN9%	Social Security Number for child #9
64	%CHILDDOB9%	Date of Birth for child #9
65	%CHILDSEX9%	Gender of child #9
66	%CHILDRACE9%	Race of child #9
67	%CHILD10%	Name of child #10
68	%CHILDSSN10%	Social Security Number for child #10
69	%CHILDDOB10%	Date of Birth for child #10
70	%CHILDSEX10%	Gender of child #10
71	%CHILDRACE10%	Race of child #10
72	%UNIT%	Unit Number
73	%UNITNAME%	Unit Name
74	%UNITADDRESS1%	First line of Unit Address
75	%UNITADDRESS2%	Second line of Unit Address (if necessary)
76	%UNITCITY%	City where unit is located
77	%UNITSTATE%	State where unit is located
78	%UNITZIPCODE%	Zipcode where unit is located
79	%UNITFAX%	The customer's case manager's fax number
80	%UNITPHONE%	The customer's case manager's primary phone number
81	%UNITCONTACT%	The customer's case manager
82	%HARD1DATE%	Date that the first Hardship Appointment was mailed
83	%HARD2DATE%	Date that the second Hardship Appointment was mailed

STEP 2: SAVE THE DOCUMENT AS AN .RTF FILE.

When the letter is completed, save the file as an .rtf file. From within Microsoft Word, this is done by clicking 'File,' then 'Save As' on your tool bar. A pop up box will appear. In the 'Save As Type' drop down box , select 'Rich Text Format (*.rtf).' Click 'Save.'

STEP 3: LOGIN TO THE SECURITY MAINTENANCE SCREENS TO ACCESS TRIGGER MAINTENANCE.

LOGIN to the Security Maintenance screens.

MOUSE over the 'Maintain Units' option at the top of the screen and select 'Trigger Admin.' This launches the 'Print Trigger Administration' screen.

STEP 4: UTILIZE THE PRINT TRIGGER ADMINISTRATION PAGE.

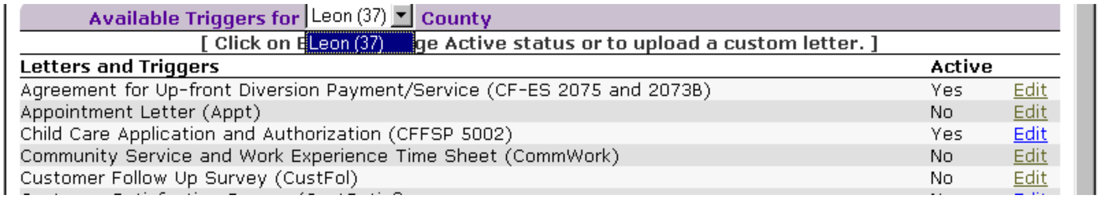
This screen allows the Security Officer to view all potential points within OSST at which a letter can be generated. This screen provides a view of the letters within a particular *county* in OSST. From this screen, a Security Officer can also link to edit the active status and the letter associated with any of the listed triggers. Any updates that are made to these triggers are based on the *county* (not a region, not a specific unit). This means that if a letter should be uploaded for an entire Region, the Security Officer must ensure that each county for that Region has been updated to trigger that specific letter.

Currently there are 26 trigger points defined in the application. When OSST goes live in any region, eleven common letters are defaulted when a trigger is generated. The remaining fifteen triggers (if the region decides to associate a letter with that trigger) must be tied to local correspondence. Any of the 26 trigger points (including those where a common letter is defined) can be replaced with local correspondence.

If a letter/trigger is listed with an Active Status of 'No,' this means that either the trigger has been turned ‘OFF’ or a letter does not currently exist for this trigger. If a letter/trigger is listed with an Active Status of 'Yes,' this means that a letter does currently exist for this trigger (either the default letter or the locally defined letter) and that it has been set to be active.

STEP 5: EDIT A TRIGGER.

Before you edit any of the listed triggers, make sure that you have selected the county in which you are editing triggers from the drop down box.

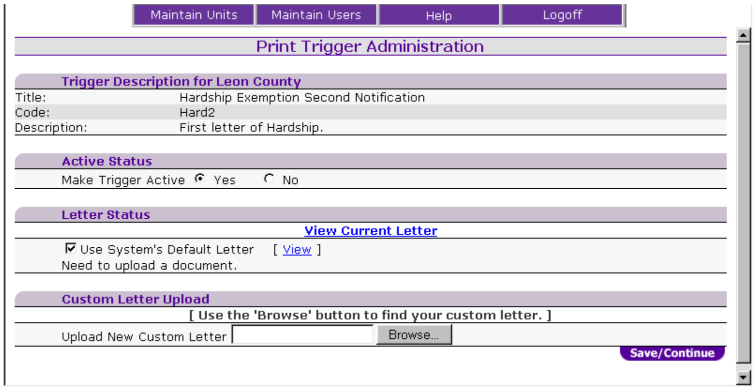


Available Triggers for Leon (37) County

[Click on E Leon (37) ge Active status or to upload a custom letter.]

Letters and Triggers	Active	
Agreement for Up-front Diversion Payment/Service (CF-ES 2075 and 2073B)	Yes	Edit
Appointment Letter (Appt)	No	Edit
Child Care Application and Authorization (CFFSP 5002)	Yes	Edit
Community Service and Work Experience Time Sheet (CommWork)	No	Edit
Customer Follow Up Survey (CustFol)	No	Edit

From the 'Print Trigger Administration' main page, click the 'Edit' link next to the specific letter/trigger that is to be edited. Clicking Edit brings up the detail for that specific letter/trigger. The page is divided into four sections: a Trigger Description section, an Active Status section, a Letter Status section and a Customer Letter Upload section.



Print Trigger Administration

Trigger Description for Leon County

Title:	Hardship Exemption Second Notification
Code:	Hard2
Description:	First letter of Hardship.

Active Status

Make Trigger Active ● Yes ○ No

Letter Status

View Current Letter

☑ Use System's Default Letter [View]
Need to upload a document.

Custom Letter Upload

[Use the 'Browse' button to find your custom letter.]

Upload New Custom Letter ▭ Browse...

Save/Continue

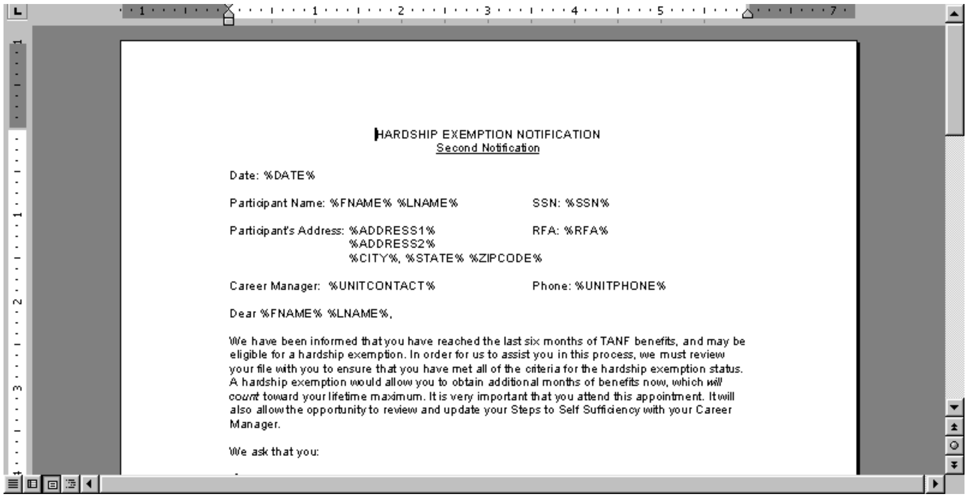
- Trigger Description: Provides the title of the letter and a description of when it is triggered.

- Active Status: To activate the current trigger click the 'Yes' radio button. To inactivate the current trigger click the 'No' radio button.

- Letter Status: If a default letter exists, you will have an option to check a box for "Use System's Default Letter." If a default letter does not exist and a custom letter has not been uploaded, the message "Need to upload a document" will appear. If both a system default letter and a custom letter exist, check which one should be used as the trigger letter. The 'Letter Status' section also allows viewing of the current letter that is generated for this particular trigger.

- Custom Letter Upload: Clicking the Browse button allows navigation through the files on the computer to locate the .rtf file that is to be uploaded for the custom letter. After locating the custom letter in your files, double click on it. The document will the appear in the “Upload New Custom Letter” box. Click the “Save/Continue” tab. Check the box next to “Use Custom Letter” and be sure the trigger is active. This will change the letter for one county only. The custom letter must be uploaded for each county in a region if same letter needs to be utilized by the entire region.

- Letter can be viewed by clicking on ‘view’.



HARDSHIP EXEMPTION NOTIFICATION
<u>Second Notification</u>

Date: %DATE%

Participant Name: %FNAME% %LNAME%   SSN: %SSN%

Participant's Address: %ADDRESS1%   RFA: %RFA%
%ADDRESS2%
%CITY%, %STATE% %ZIPCODE%

Career Manager: %UNITCONTACT%   Phone: %UNITPHONE%

Dear %FNAME% %LNAME%,

We have been informed that you have reached the last six months of TANF benefits, and may be eligible for a hardship exemption. In order for us to assist you in this process, we must review your file with you to ensure that you have met all of the criteria for the hardship exemption status. A hardship exemption would allow you to obtain additional months of benefits now, which *will count* toward your lifetime maximum. It is very important that you attend this appointment. It will also allow the opportunity to review and update your Steps to Self Sufficiency with your Career Manager.

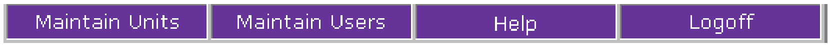
We ask that you:

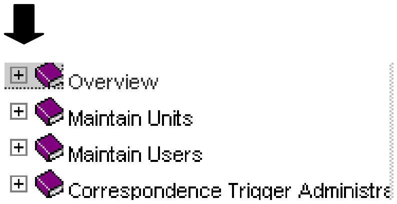
STEP 6: SAVE YOUR CHANGES.

When all changes have been completed, click 'Save/Continue.'

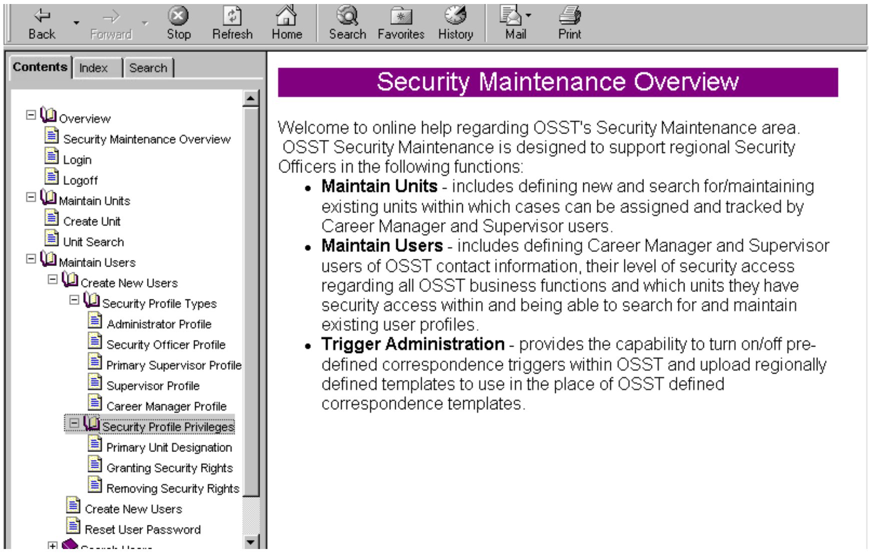
On-Line Help

On line help offers three different ways to search for information. To access on-line help click the help button at the top of any screen.





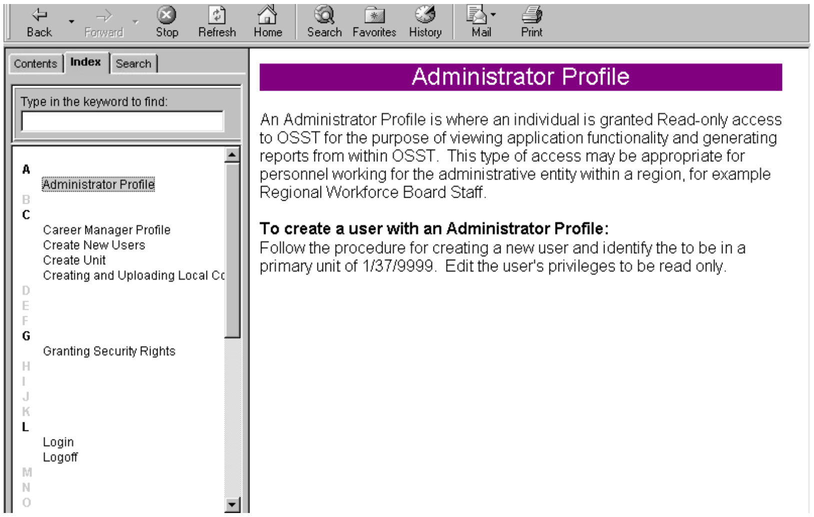
TO SEARCH FOR INFORMATION ON THE CONTENTS TAB:
CLICK the plus sign [+] beside the book icon and a drop



Security Maintenance Overview

Welcome to online help regarding OSST's Security Maintenance area. OSST Security Maintenance is designed to support regional Security Officers in the following functions:

- **Maintain Units** - includes defining new and search for/maintaining existing units within which cases can be assigned and tracked by Career Manager and Supervisor users.
- **Maintain Users** - includes defining Career Manager and Supervisor users of OSST contact information, their level of security access regarding all OSST business functions and which units they have security access within and being able to search for and maintain existing user profiles.
- **Trigger Administration** - provides the capability to turn on/off pre-defined correspondence triggers within OSST and upload regionally defined templates to use in the place of OSST defined correspondence templates.



Administrator Profile

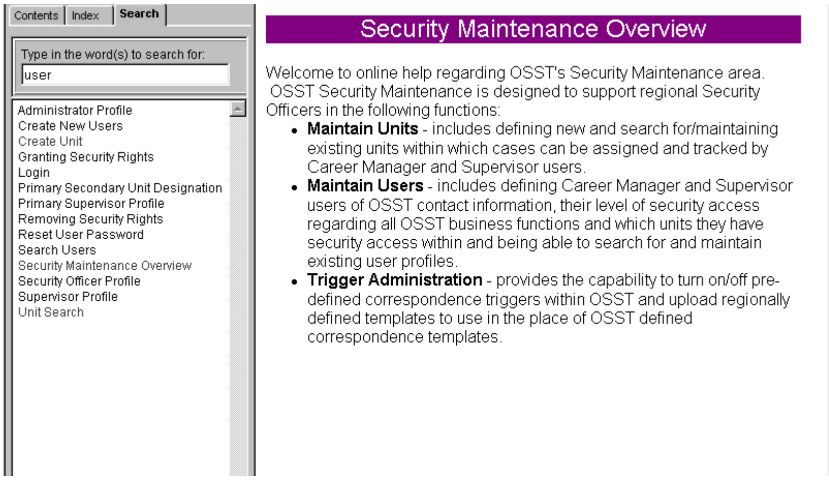
An Administrator Profile is where an individual is granted Read-only access to OSST for the purpose of viewing application functionality and generating reports from within OSST. This type of access may be appropriate for personnel working for the administrative entity within a region, for example Regional Workforce Board Staff.

To create a user with an Administrator Profile:
Follow the procedure for creating a new user and identify the to be in a primary unit of 1/37/9999. Edit the user's privileges to be read only.

TO SEARCH FOR INFORMATION ON THE INDEX TAB:

The Index tab will list all subjects in alphabetical order.

CLICK the subject in the list and the information will appear in the detail box on the right.



Security Maintenance Overview

Welcome to online help regarding OSST's Security Maintenance area. OSST Security Maintenance is designed to support regional Security Officers in the following functions:

- **Maintain Units** - includes defining new and search for/maintaining existing units within which cases can be assigned and tracked by Career Manager and Supervisor users.
- **Maintain Users** - includes defining Career Manager and Supervisor users of OSST contact information, their level of security access regarding all OSST business functions and which units they have security access within and being able to search for and maintain existing user profiles.
- **Trigger Administration** - provides the capability to turn on/off pre-defined correspondence triggers within OSST and upload regionally defined templates to use in the place of OSST defined correspondence templates.

TO SEARCH FOR INFORMATION ON THE SEARCH TAB:

ENTER a keyword and hit the enter key and a list of subjects will appear.

CLICK on a subject and the information will appear in the details box on the right

Appendix

- Useful URLs
- OSST Security Agreement
- Chapter 815, Florida Statutes

Useful URLs

TRAINING

https://sun13.state.fl.us/wagesct/wagestrain/casetracking/default.cfm

SECURITY

https://sun13.state.fl.us/wagesct/wagestrain/casetracking/securitymaint/sm_login_dsp.cfm

SKILL MATCH

https://sun13.state.fl.us/wagesct/wagestrain/default.cfm

WELFARE TRANSITION PROGRAM

http://www2.myflorida.com/awi/wtp/default.htm

OSST HOME PAGE

http://www2.myflorida.com/awi/pdg/osst/default.htm

WFI/OSMIS

http://workforceflorida.com/wages/wfi/partners/osmis/index.html

OSST PRODUCTION

https://www.myfloridajobs.com/casetracking/default.cfm

OSST Security Agreement Form

Contact Information:	**Primary Unit Information:**
First Name	Region
Middle Name	County
Last Name	Unit
Job Title	Org. Name
Phone	Address
Fax	Address
Local Office Code	City
Station Desk ID	State, Zip
E-mail	

Menu Access	Allow	Menu Access	Allow
Contact Information		Individual Responsibility Plan & JPR	
Education		Job History / Placement	
Household Members		Out comes and Follow up	
Goals and Interests		Hardships/SSI/SAMH	
Needs and Barriers		Deferrals	
Steps to Self Sufficiency		Sanctions	
Service and Training Plan		Assessments	

User Access Profile

Region/County/Unit ______________________________

Receive Alerts (Yes or No) ______________________________

Classification (Case Manager or Supervisor)______________________________

Security Privileges ______________________________

OSST Security Agreement **Name**______________________________________

Your local Workforce Development Board has authorized you to have access to sensitive data through the use of the One Stop Service Tracking (OSST) and computer related media (such as printed reports, system inquiry, on-line update, etc).

Computer crimes are a violation of disciplinary standards and the commission of computer crimes may result in felony criminal charges. The Florida Computer Crimes Act, Chapter 815, Florida Statues addresses the unauthorized modification, destruction, disclosure, or taking of information resources.

Employees of AWI, one-stop centers, RWB and their subcontractors in the performance of their duties and in the course of delivering the core service, receive and have access to information obtained from employers, job applicants and unemployment compensation claimants. The information received includes job applicant registrations, job orders, employer reports, unemployment compensation claims and related records. The information is collected for such purposed as labor exchange, determination of an unemployment compensation claim and in compliance with State and federal reporting requirements. This information is confidential, as required by federal law and by § 443.1715(1), Florida Statutes, which reads in part:

> …..Except as otherwise provided by law, public employees receiving such information must retain the confidentiality of such information.

Section 443.1715(1), Florida Statutes, also provides that any employee or individual receiving or releasing confidential information that violates any provision of this subsection commits a misdemeanor of the second degree punishable as provided in Florida Statutes, sections 775.082 or s. 775.083. The effect of this language is to extend penalties to any person who receives confidential information and who releases it improperly. This would pertain to persons who legally receive confidential information.

I understand that a security violation may result in criminal prosecution according to the provision of Chapter 815, F.S. and may also result in disciplinary action against me.

The minimum security requirements are: Personal passwords are not to be disclosed. Information is not to be obtained for my own or another person's use.

I have read the above statements and have been provided a copy of the Computer Related Crimes Act, Chapter 815, F. S. By my signature I acknowledge that I have received, read and that I understand Chapter 815, F. S. and have received any necessary clarification from my supervisor.

____

Requestor's Signature/Date **Supervisor's Signature/Date**

____

Security Officer's Signature/Date

CHAPTER 815
COMPUTER-RELATED CRIMES

815.01 Short title.--The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."

History.--s. 1, ch. 78-92.

815.02 Legislative intent.--The Legislature finds and declares that:

(1) Computer-related crime is a growing problem in government as well as in the private sector.

(2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.

(3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.

(4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

History.--s. 1, ch. 78-92.

815.03 Definitions.--As used in this chapter, unless the context clearly indicates otherwise:

(1) "Intellectual property" means data, including programs.

(2) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

(3) "Computer" means an internally programmed, automatic device that performs data processing.

(4) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(5) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or computer software.

(6) "Computer network" means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

(7) "Computer system services" means providing a computer system or computer network to perform useful work.

(8) "Property" means anything of value as defined in [1]s. 812.011 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.

(9) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(10) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

History.--s. 1, ch. 78-92.

[1]**Note.**--Repealed by s. 16, ch. 77-342.

815.04 Offenses against intellectual property; public records exemption.--

(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(3)(a) Data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 which resides or exists internal or external to a computer, computer system, or computer network which is held by an agency as defined in chapter 119 is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

(b) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(4)(a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

History.--s. 1, ch. 78-92; s. 1, ch. 94-100; s. 431, ch. 96-406.

815.045 Trade secret information.--The Legislature finds that it is a public necessity that trade secret information as defined in s. 812.081, and as provided for in s. 815.04(3), be expressly made confidential and exempt from the public records law because it is a felony to disclose such records. Due to the legal uncertainty as to whether a public employee would be protected from a felony conviction if otherwise complying with chapter 119, and with s. 24(a), Art. I of the State Constitution, it is imperative that a public records exemption be created. The Legislature in making disclosure of trade secrets a crime has clearly established the importance attached to trade secret protection. Disclosing trade secrets in an agency's possession would negatively impact the business interests of those providing an agency such trade secrets by damaging them in the marketplace, and those entities and individuals disclosing such trade secrets would hesitate to cooperate with that agency, which would impair the effective and efficient administration of governmental functions. Thus, the public and private harm in disclosing trade secrets significantly outweighs any public benefit derived from disclosure, and the public's ability to scrutinize and monitor agency action is not diminished by nondisclosure of trade secrets.

History.--s. 2, ch. 94-100.

Note.--Former s. 119.165.

815.05 Offenses against computer equipment or supplies.--

(1)(a) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits an offense against computer equipment or supplies.

(b)1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

2. If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(2)(a) Whoever willfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offense against computer equipment or supplies.

(b)1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

2. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is greater than $200 but less than $1,000, then the offender is guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

3. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is $1,000 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

History.--s. 1, ch. 78-92; s. 192, ch. 91-224.

815.06 Offenses against computer users.--

(1) Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.

(2)(a) Except as provided in this subsection, an offense against computer users is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) If the offense is committed for the purposes of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

History.--s. 1, ch. 78-92.

815.07 This chapter not exclusive.--The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter.

History.--s. 1, ch. 78-92.