Introduction to Module 8: System Security

System security consists of two major areas: Maintaining units and maintaining users. Units, user ids, and passwords will be created and assigned based on need.

- Maintain units contains the create units and unit search functions.

- Maintain users consists of user type search and adding new users.

Current units have been converted into OSST. Additional units will be created upon request from a regional workforce development board. Units consist of one or more supervisors, one or more career managers, and a caseload of customers.

User ids (changed to adapt to the new user id designations) have also been converted to OSST.

MyFlorida Jobs.com   **Module 8: Security Maintenance**

At the end of this module, you will be able to:

✓   **Create and maintain units**

✓   **Conduct unit searches**

✓   **Create and maintain user accounts**

✓   **Conduct user searches**

✓   **Resetting user passwords**

Accessing the Security Maintenance pages

The security maintenance pages will be accessed at a different url than the OSST system. Only security officers will have userid and password access to the Security Maintenance screens.

From the Security Maintenance main page, security officers will be able to access the following functions:
Creating and Maintaining Units

This includes:

- registering new units in the system
- entering unit contact information
- conducting unit searches
- viewing members of a specific unit

Creating and Maintaining Users

This includes:

- registering new users in the system (including entering user contact information and setting user type)
- assigning userids and passwords
- editing user privileges

Requesting a userid will still need to follow a standard process in each of the regions. For example, it will still be required to complete the necessary paperwork in order to have a user added to the system. The following is a suggested list of steps to follow in requesting a new userid:

- Determine a need for the user to have access to OSST
- Complete your regional security access request form
- Document the access levels that the user should have to determine the user's security profile
- Ensure that the user has been signed up to attend OSST training
- Create user in OSST using the 'Create User' functions

Creating a new unit

This function is accessed by positioning your mouse pointer over the 'Maintain Units' button at the top of the page and clicking the 'Create Unit' option. 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

CLICK 'Create Unit'

ENTER the district id

ENTER the region id

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 the Treasure Coast, Hillsborough County Workforce Board, Workforce Central Florida)

ENTER the unit id for the new unit

ENTER the unit name

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 that the unit is located)

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)

Conducting a Unit Search

This function is accessed by positioning your mouse pointer over the 'Maintain Units' button at the top of the page and clicking the 'Unit Search' option. A unit search can be done by entering in one or many 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.
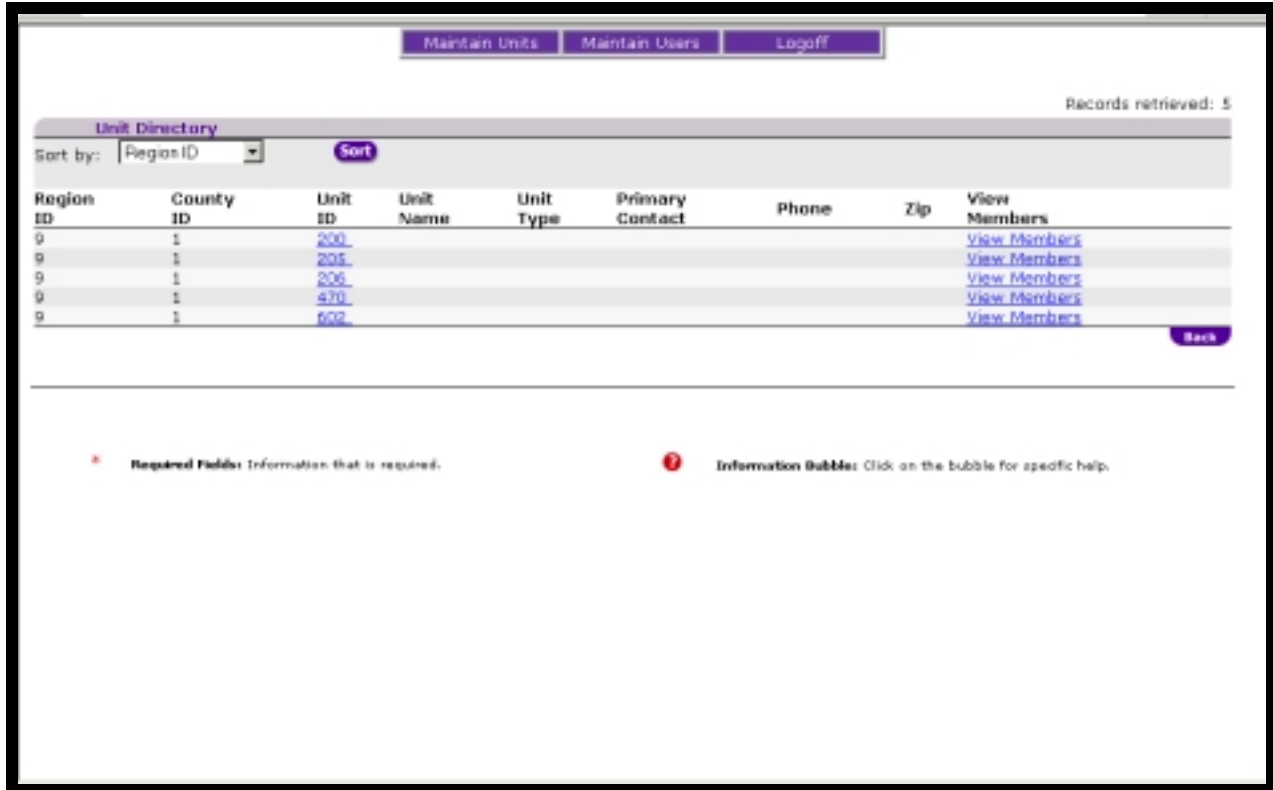
Associated Procedures: (Navigating from the Security Maintenance Main Page)

POSITION your mouse pointer over the 'Maintain Units' button at the top of the page

CLICK 'Unit Search'

ENTER search parameters

CLICK 'Search'

Viewing Unit Search Results

The Unit Search Results page is a listing of the results that met the initial unit search criteria. The results 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. There is also a link to 'View the Members' of each listed unit.

Conducting a User Search

This function is accessed by positioning your mouse pointer over the 'Maintain Users' button at the top of the page and clicking the 'User Search' option. A unit search can be done by entering in one or many parameters into the User Search function. These parameters include

Associated Procedures: (Navigating from the Security Maintenance Main Page)

POSITION your mouse pointer over the 'Maintain Users' button at the top of the page

CLICK 'User Search'

ENTER search parameters (include a keyword, such as the person's last name and select the user type)

CLICK 'Search'

Viewing User Search Results

The User Search Results page is a listing of the results that met the initial unit search criteria. The results include the following information:

- User id
- User Name
- Primary R/C/U
- Link to edit user privileges

The results can be sorted and viewed by any of the above parameters.
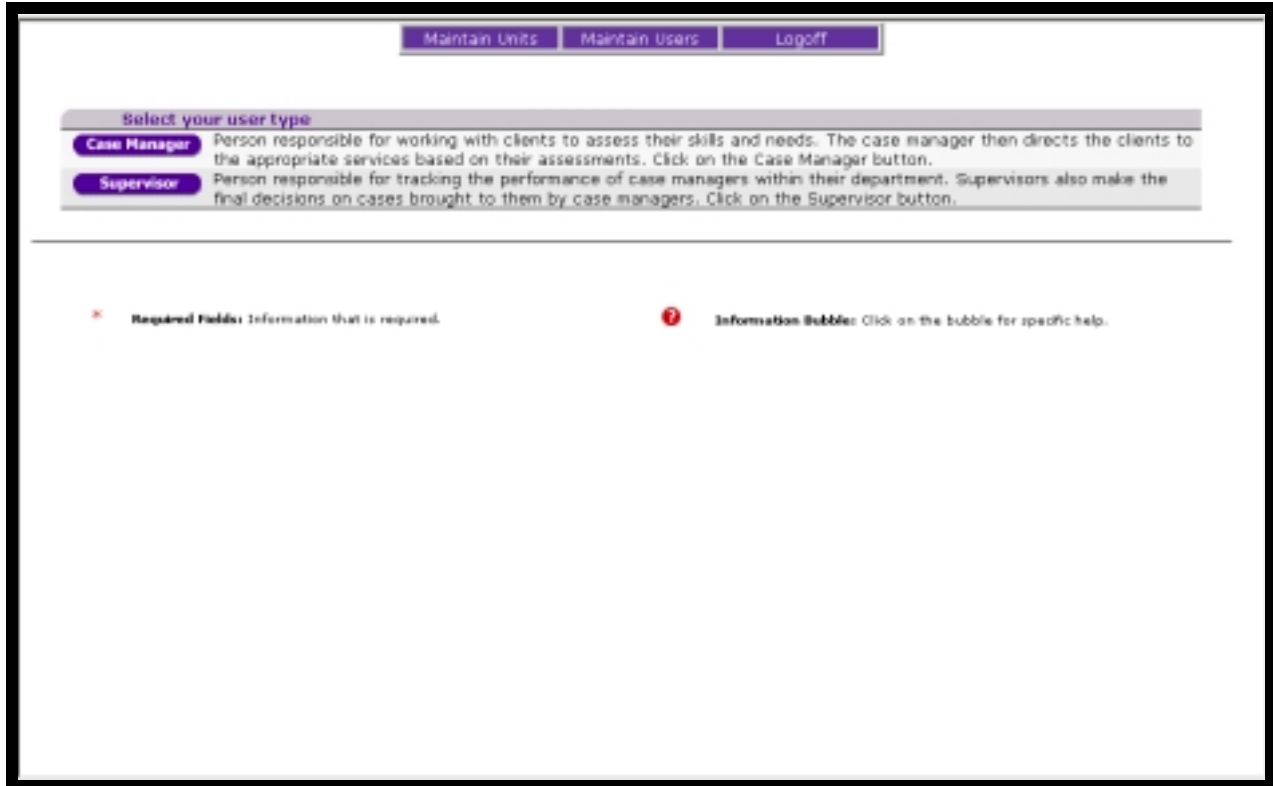
Creating a new user

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 userid 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 clicking the 'Create User' option.

The first step in creating a new user is selecting the user type. There are two user types for OSST: case manager and supervisor.
- A case manager is defined as "a person responsible for working with clients to assess their skills and needs. The case 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 case managers within their department. Supervisors also make the final decisions on cases brought to them by case managers."

After selecting user type, the security officer is then prompted to create a user id and a password for the user.

Creating a User id and Password for a New User

This page will prompt you to assign the user a User ID and an initial pssword for OSST. A suggestion is to assign a user id such as his/her last name plus first initial and middle initial.

Associated Procedures:

I. Creating a New User

POSITION your mouse pointer over the 'Maintain Users' button at the top of the page

CLICK 'Create User'

SELECT the user type (case manager or supervisor)

ASSIGN the user id

ASSIGN the user's password

CONFIRM the user's password

ENTER the user's e-mail address

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

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.

Associated Procedures:

I. Entering Account Information

SELECT the county in which the user's primary unit is located

SELECT the user's primary unit

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

CLICK 'Save/Continue'

Verifying Account Information for a New User

After entering in the user's primary unit information and contact information, the user will be prompted with the User Search screen. The purpose of this is to conduct a search and verify the user has been added to the system.
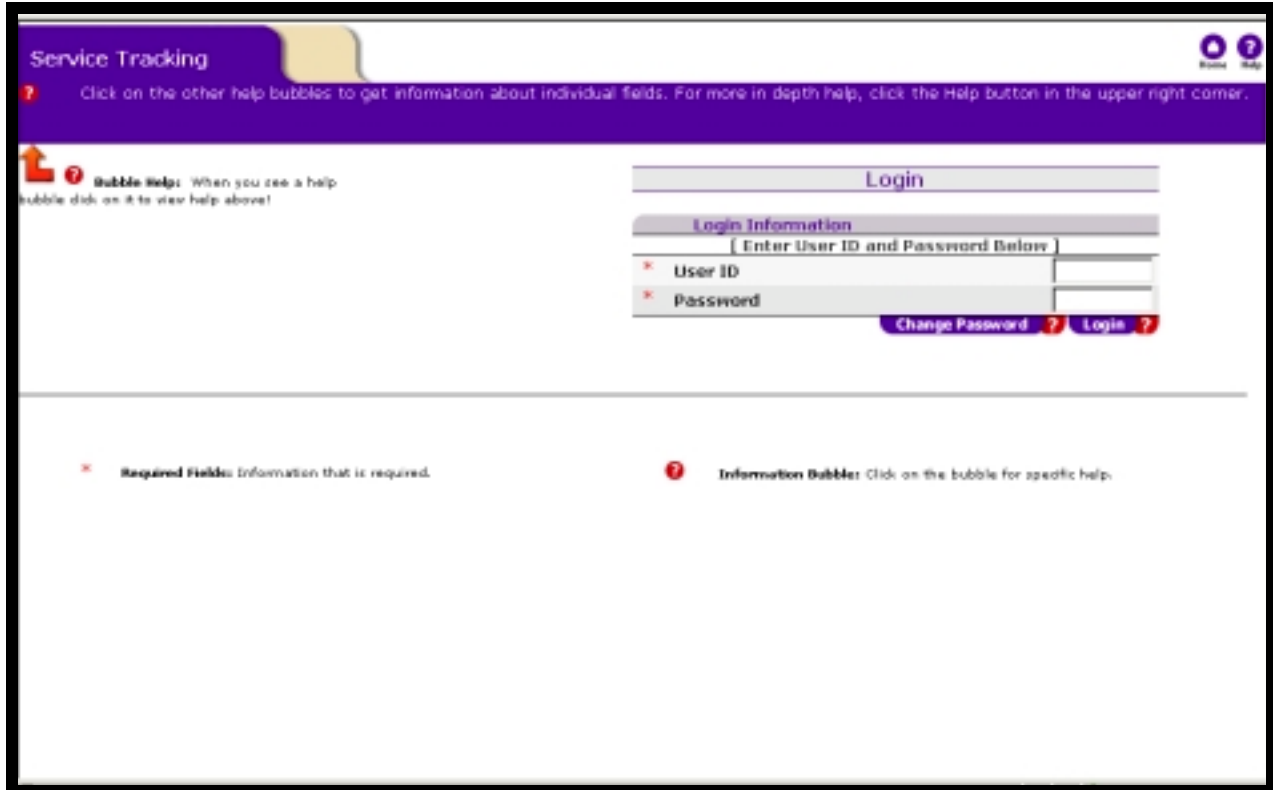
Additionally, from this screen, the security officer can link to 'View/Edit Privileges' for a new user.
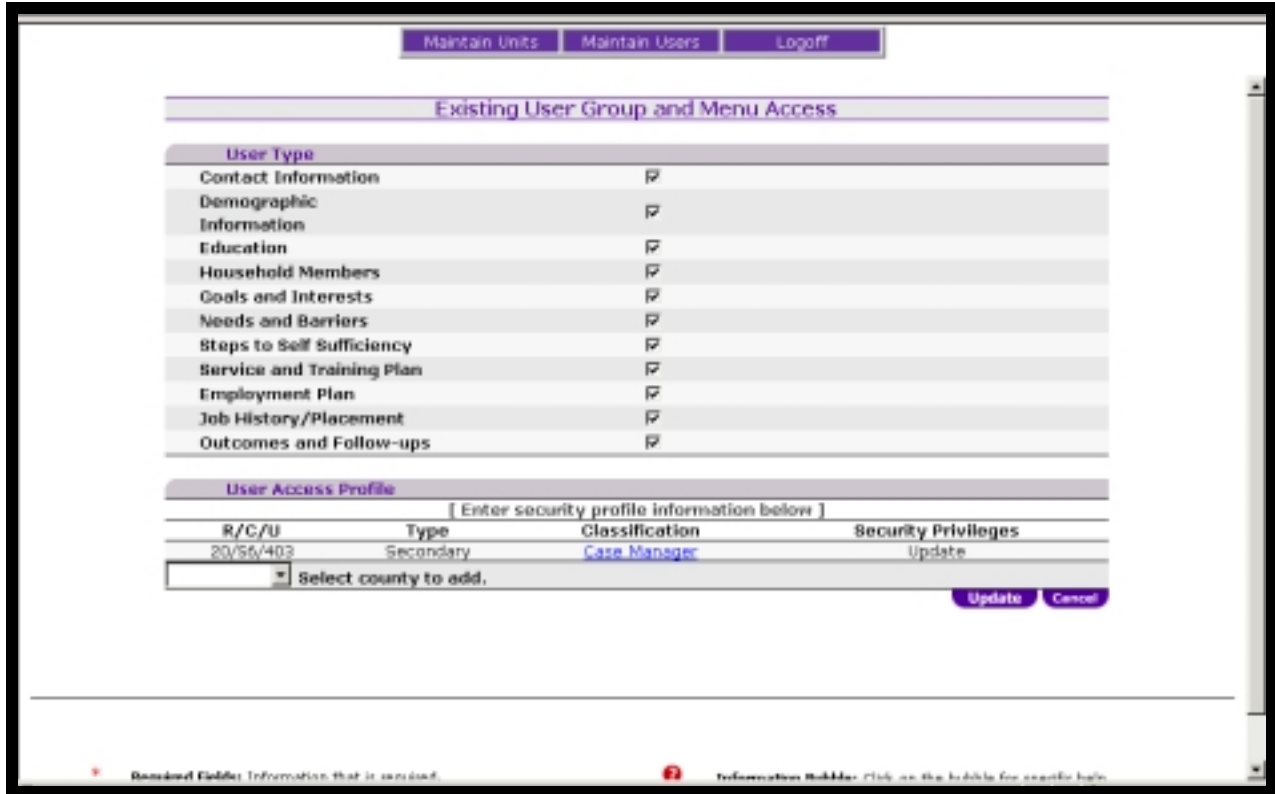
Editing User Privileges

The menu access page allows the security officer to edit which areas within OSST 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).

Resetting a user's password

Users have the ability to change their own passwords. This is done from the OSST Login screen. In the case that 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.

Associated Procedures:

I. Resetting a user's password (security officer must access through OSST login screen, and must enter your security user id and password into the OSST user id and password fields)

ENTER to your security user id and password

CLICK 'Change Password'

OVERWRITE the displayed user id with the user id of the user whose password you wish to change

ENTER the user's new password

REENTER the user's new password to confirm the change

CLICK 'Continue'

Helpful Tips:

Tip 1: The process to have a user password reset may vary according to local region processes (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: Passwords are not reset for a third party. The user must request to have the password reset (if a supervisor makes the request they will not be given the new password).

Now it's your turn to practice using the system! Here are the scenarios:

- Adding /Editing Unit Detail
- Conducting a Unit Search
- Viewing/Sorting Unit Search Results
- Conducting a User Search
- Adding a User
- Adding/Editing a User's Security Profile
- Resetting a User's password