

SECURITY MAINTENANCE: MODULE OVERVIEW

Module Overview:

Security Maintenance refers to the tasks of maintaining units and maintaining users. The content of the module focuses on:

- Creating and maintaining units
- Conducting unit searches
- Creating and maintaining user accounts
- Conducting user searches
- Resetting user passwords

NOTE: The estimated time to complete this module is as follows:

Presentation: 1 hour

Demonstration: 1 hour

Activity: 1 hour

Key Speaking Points:

1. **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.
 2. **Maintaining units:** Creating and maintaining units refers to entering unit contact information, conducting unit searches and viewing members of a specific unit.
 3. **Creating a new unit:** Creating a new unit requires the security officer to complete unit registration information (unit details) as well as unit contact information.
 4. **Conducting a unit search:** 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.
 5. **Viewing unit search results:** Unit search results can be viewed/sorted by any of the following parameters: Region ID, County ID, Unit Name, Unit Type, Primary Contact, Phone and Zip.
 6. **Conducting a user search:** A user search can be done by entering in one or many parameters into the User Search function. These parameters include <Need to insert>.
-

7. **Viewing user search results:** Unit search results can be viewed/sorted by several parameters, including: Region ID, County ID, Unit ID, Unit Name, Unit Type, Primary Contact, Phone and Zip.
8. **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.

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 assigns a user id and a password for the user. (Refer to Training Module for additional procedures).

9. **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.
-
-