

PWS APP G - ACCOUNT MGMT PLAN

DTCI User Account Management

1. The Defense Transportation Coordination Initiative (DTCI) Program Management Office (PMO) will control government user access to the Menlo ONE TMS website. This action is necessary to protect the integrity of government transportation information and systems. The ONE TMS provides registration for system user access through the website (URL) and passes the information to the DTCI PMO for validation and approval.
2. For access, the supervisor fills out the user registration form for employees requiring access with the following fields. (Fields in *Italic* are mandatory.) The system will edit input to ensure e-mail addresses, phone numbers, and required fields are complete before accepting the application.
 - *User Role (Ordering Officer, Reporting, Tracking, Claims, Carrier Issues)*
 - *User ID*
 - *Citizenship (default is US)*
 - *Prefix (Mr, Ms, Rank, etc.)*
 - *User first name and middle initial*
 - *User last name*
 - *User commercial phone number*
 - User DSN
 - *User e-mail address (validate structure)*
 - *Organization name*
 - Organization Office
 - *Supervisor prefix (Mr, Ms, Rank, etc.)*
 - *Supervisor first name*
 - *Supervisor last name*
 - *Supervisor commercial phone number*
 - Supervisor DSN
 - *Supervisor e-mail address (validate structure)*
 - *A text box describing why the user needs access to the DTCI system*
3. Once all edit checks are complete and the form is ready, the supervisor submits information via the website.
4. The Menlo team collects all requests on a daily basis, reviews for completeness, and forwards them to the DTCI A&P team (at ustc-dtci-a&p@ustranscom.mil) for validation and approval. Questions concerning status of an account request should be directed to the DTCI A&P Team at (618) 622-2212.
5. The DTCI A&P reviews the requests. If necessary, staff may contact the individual or the individual's supervisor to validate information or verify the need for access to the system. The DTCI A&P lead will notify the supervisor of any disapproved accounts with the reason for the rejection.
6. The approved accounts are returned to the Menlo team for activation.

7. The ONE TMS assigns a user ID and password. The user ID will be constructed of the last name with the first and middle initials. Duplicate names will be appended with consecutive numbers to create a unique User ID. The user ID will not be case sensitive; either WeyerhouserWI or weyerhouserwi will be accepted.
8. Passwords are required to be changed to a strong password as soon as issued for security. A strong password requires a minimum of 9 characters containing 2 upper case characters, 2 lower case characters, 2 numerals, and 2 special characters (!,@,#,\$,%,&).
9. As required by the government user passwords will expire every 60 days. The ONE TMS will notify users upon login when their passwords are [10] days away from expiration and inquire if they would like to change them. A password change will be forced on the last day.
10. Accounts will be flagged as inactive if not used for 45 days. Accounts will be deleted after 90 days. User may request reactivation by contacting the coordinator's help desk. The coordinator will reactivate the account in a manner similar to that described in steps 4 through 7. Accounts that have been deleted require a complete application and processing through the PMO.
11. DOD shippers and other activities will notify the coordinator of the user accounts that will require deactivation due to retirement, transfer, termination, etc and the date to close the account.
12. Users may edit their profiles by logging into the system.
 - User first name and middle initial
 - User last name
 - User commercial phone number
 - User e-mail address
 - Option to delete the user account
13. The Menlo team will make the changes available to the PMO for information purposes.
14. When needed, the PMO security officer will have permission to query the coordinator system for a list of current account holders.