

Password Requirements

- Passwords must be 8 characters in length.
- Must contain at least one number (i.e. 0, 1, 2, ... 9)
- Must contain at least one alphabetic character (i.e. a, b, c, ... z)
Note: Passwords are not case sensitive; all characters are converted to upper case before processing.
- Must contain at least one of the following special characters #, \$, or @
Note: No other special characters are valid in passwords.
- May not contain the first three to six consecutive characters of your name as it appears in the security database. For example: John Barrymore cannot use joh, john, bar, barr, barry, or barrym anywhere in the password.
- May not contain your user ID.
- Security maintains a history of each user's most recent five (5) passwords and does not allow the reuse.
- Personal user ID passwords must be changed at least every 60 days.

Examples of Passwords

User's name in database = John Smith, User's ID = JS00211

Valid Password Examples

\$ismksc9 (contains numeric character, special character, and alpha characters)

b\$o#ca22 (contains numeric characters, special characters, and alpha characters)

m@129apy (contains numeric characters, special character, and alpha characters)

Invalid Passwords

Moneybag (contains alpha characters only)

Moneyba2 (contains alpha and numeric characters only)

cev#ga2 (less than 8 characters)

\$2749638 (contains numeric characters and special character only)

js00211# (contains user's User ID)

john#007 (contains part of user name, "john")

#2smi\$56 (contains part of user name, "smi")

Password Tips

Entering Passwords

Be careful entering your eight-character password on the TPX and TSO sign-in screens. The input field for the password is eight characters and the cursor will automatically advance to the “New Password” field. If you accidentally type a character in that field and press Enter, the system assumes you are trying to change your password and prompt you to re-enter your new password for verification. Choose F3 to escape the sign-in screen and start over.

Choosing a Good Password

- Avoid obvious passwords. Do not use names of children, spouses, pets, favorite sports teams, birthdays, or similar personal things that others are also likely to know.
- Do not use anything that can be found in a dictionary. If you want to use a word, mix in special characters and numbers, or even intentionally misspell the word, such as #guvnor1 or @2gether.
- Make up an acronym on a song, a sentence, poem, or rhyme then mix in special characters and numbers to a length of 8 characters, as in the following examples.

“I Saw Mommy Kissing Santa Clause...” ism\$9ksc

“The Check Is In The Mail” 5#tciitm

“My Dog Fido Drools A Lot” mdfdal@7

- Do not use any of these examples...make up your own schemes!

Safeguarding Your Password

- NEVER tell your password to anyone, including co-workers.
- NEVER share your user ID and password with others. You alone are responsible for what is done with your user ID.
- Do not write your password down. A written password is more easily discovered than one committed to memory.

Be careful when typing in your password. Make sure no one is looking over your shoulder.