

GUIDANCE: GOOD PASSWORDS

1. Users must choose passwords that are difficult-to-guess. This means that passwords must NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used. Where such systems software facilities are available, users must be prevented from selecting easily-guessed passwords by either using a password crack program or requiring passwords with minimum length (6) and opportunity to mix numbers, special characters, and capital letters.

Users can choose easily-remembered passwords that are at the same time difficult for unauthorized parties to guess if they:

- (a) string several words together (the resulting passwords are also known as "passphrases"),
 - (b) shift a word up, down, left or right one row on the keyboard,
 - (c) bump characters in a word a certain number of letters up or down the alphabet,
 - (d) transform a regular word according to a specific method, such as making every other letter a number reflecting its position in the word,
 - (e) combine punctuation or numbers with a regular word,
 - (f) create acronyms from words in a song, a poem, or another known sequence of words,
 - (g) deliberately misspell a word (but not a common misspelling), or
 - (h) combine a number of personal facts like birth dates and favorite colors.
2. Users must not construct passwords that are identical or substantially similar to passwords they have previously employed. Where systems software facilities are available, users must be prevented from reusing previous passwords (minimum 3, maximum 6).
 3. Users must not construct passwords using a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users must NOT employ passwords like "zOSjan1" in January, "zOSfeb1" in February, etc.
 4. Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers

without access control, in documentation of system or application, or in other locations where unauthorized persons might discover them.

5. Passwords must not be written down and left in a place where unauthorized persons might discover them.
6. Passwords must never be shared or revealed to anyone else besides the authorized user. To do so otherwise exposes the authorized user to responsibility for actions that the other party takes with the disclosed password. This standard does not prevent the use of default passwords--typically used for new user-ID assignment or password reset situations--which are then immediately changed when the user next logs-onto the involved system.
7. Aside from initial password assignment and password reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user, the password must be immediately changed.