Password Requirements & Tips

Comply with Password Requirements

When you create, change, or reset your SAIC password, the following requirements must be met:

Passwords

- Must be **between 8 to 14** characters
- **Must contain at least 3 of the 4 character types:**
    1. **lowercase alphabetic** (a-z)
    2. **UPPERCASE alphabetic** (A-Z)
    3. **numeric** (0-9)
    4. **special** - Special characters are all characters not defined as letters or numerals on your keyboard (i.e., ` ~ ! _ # $ ^ * ( ) , etc.)

  Note: The special character "&" is problematic for some SAIC applications. It is recommended that you do not use this symbol in your password. The special characters "(", and ")" may be problematic in rare combinations and should be used with caution.
- Must **not be a variation of your name or username**
- Must be **different from a password used in the last 15 months**
- Must **not contain spaces**

Improve Password Security

Here are some additional ways you can help ensure that your passwords are secure:

- Avoid using words that can be found in a dictionary in your password.
- Don't include personal identifiers, such as names of relatives, the car you drive, etc. in your password. • Avoid using the same password across multiple systems.

Develop a Strategy to Help You Remember Your Password

Developing a strategy for creating passwords can help to make it easier for you to remember your password. Here are some strategies to try:

Phrase association. Many people find that using an acronym derived from a familiar phrase helps them to remember their password.

- **Nitt4@GM** "Now is the time for all Good Men" with the @ character acting as an 'a'
- **Iw2ba*Td** "I want to be a star Today" with the '*' representing the word 'star'
- **Hw11,1B!** "He who laughs last, laughs Best!" with a number '1' in lieu of the letter 'l')

Letter/number combination. Consider reusing your password scheme with each new password, but changing the actual characters that you use. Is there a red-letter date on

your calendar you don't want to miss? Every 90 day period usually has at least one such date for you. Mom's birthday? Your anniversary? Why not trigger your memory daily by using that upcoming event into your password? For example:

- **0618=ABl** could help you remember June 18 is Aunt Betty Lou's birthday
- **Gba!!1202** could help a grandparent remember the new 'grand baby arrives' in December 2002

Letter/number association. Think of a series you've memorized at some point in your life. Maybe you had to learn the U.S. presidents in sequential order; the chemical elements; the books of the Bible; the planets in our solar system. Create a pattern of 3-4 alpha characters based on this series, then add special characters and numbers which have an association you can remember. Following a series you've already got committed to memory makes it easy to pick your next password when expiration day arrives. Rotate or alter the pattern just slightly to keep you on your toes. For example:

- **33-45FdR** Franklin D. Roosevelt was in office from 1933-1945
- **HsT45-53** Harry S. Truman was in office from 1945 to 1953
- **DdE(R)53** Dwight D. Eisenhower (Republican) was elected in 1953

Keyboard pattern. Devise a pattern on your keyboard which includes alpha, numeric, and special character keys. For example, rest your hands on the home keys. Starting with an N and moving up gives you Nji9. Repeat the pattern with your left hand to give you vfr$. Put it together and you have **Nji9vfr$**. When this password expires, shift your hands to the right of the home keys. Repeat your pattern and you have **Mko0bgt%**. People who can visualize a pattern on their keypad (parallel lines, diagonals, the shape of a letter z, etc.) may find variations on this strategy especially useful.

No matter what password strategy you use, keep both the strategy and the password to yourself. Your password is your online identity and a hacker's key to valuable information. Protect it accordingly. Never write it down and never let others watch you key it in. Think of it as your toothbrush: use it daily, change it regularly, and don't share it with your friends!

Password Policy Changes FAQ

1. **Why are you increasing password complexity? What difference does it make if I put in a special character/number or use upper and lower case?** Password cracking attempts rely on the "brute-force" method, simply trying every possible combination of characters until the correct combination is found. Adding numbers, special characters, and varying the case of a password adds an exponential number of possibilities, dramatically increasing the amount of time needed to bruteforce a password.

   At one time, a password comprised of 8 letters and one number was considered to be adequate. However, advances in computer technology have dramatically decreased the

time it takes to brute-force a password. Adding numbers, special characters, and varying the case of a password adds an exponential number of possibilities, greatly increasing the amount of time needed to brute-force a password. Password strength is our first line of defense in protecting our information at SAIC. It is important to adhere to industry best practice when since not only does SAIC rely on the strength of our passwords but our customer information that we control is also dependent on our security.

2. **What are special characters? Do all of the special characters work?**

   Special Characters are the characters on your keyboard other than numbers or letters, such as $, @, ^, &, +, etc. Windows supports all special characters in passwords.

3. **What should I do if I am locked out of my SAIC account?**

   Please visit Unlock Your Account for instructions.