PASSWORD BEST PRACTICES

To protect against security breaches, hacking attempts and rogue employees, it is recommended that all TLN libraries implement a password protection plan.

What not to do when choosing a password

- Do **not** choose a password based upon personal data like your name, your username, or other information that one could easily discover about you from such sources as searching the internet.
- Do **not** choose a password that is a word (English or otherwise), proper name, name of a TV shows, or anything else that one would expect a clever person to put in a "dictionary" of passwords.
- Do **not** choose a password that is a simple transformation of a word, such as putting a punctuation mark at the beginning or end of a word, converting the letter "l" to the digit "1", writing a word backwards, etc. For example, "password,123" is **not** a good password, since adding ",123" is a common, simple transformation of a word.
- Do **not** choose passwords less than 8 characters long and that that are made up solely of numbers or letters. Use letters of different cases, mixtures of digits and letters, and/or non-alphanumeric characters.

The best method for choosing passwords

The single best method for generating passwords is to do the following:

1. Make up a sentence you can easily remember. Some examples:
    - I have two kids: Jack and Jill.
    - I like to eat Dave & Andy's ice cream.
    - No, the capital of Wisconsin isn't Cheeseopolis!
2. Now take the first letter of every word in the sentence, and include the punctuation. You can throw in extra punctuation, or turn numbers into digits for variety. The above sentences would become:
    - Ih2k:JaJ.
    - IlteD&A'ic.
    - N,tcoWi'C!

As you can see, the passwords generated by this method can be fairly secure, but are easy to remember if the sentence you pick is one that is easy for you to remember.

Another password selection method

If you don't wish to use the above method, the following method also generates "reasonably secure" passwords (though not quite as good as the method above) that may be easier to remember:

1. Choose two unrelated words such as:
    - unix & fun
    - book & goat
    - august & brick
2. Join the words with a non-alphabetic character or two.
3. Make at least one change (for example, uppercase a letter or add another character) to one of the words (preferably not just at the very beginning or end of the password).

Some example passwords generated using this method:

- unix+fUn
- bo!ok29goat
- august,=bRICK

How long does my password have to be?

In general, the longer a password is, the harder it is for somebody to guess or brute-force it. Password selection trades off security with convenience and the ability to remember it. **Eight characters should be the absolute minimum length.** SCS Kerberos passwords may of practically unlimited length (the limit is at least several hundred characters). Windows 2000 and Windows XP support a maxiumum password length of 127 characters. There are a few cases where you might run into password length limitations:

- Some older Unix systems may only support passwords up to 8 characters, or ignore any letters after the first 8. This should not be a limitation if you login with your Kerberos password to Facilitized SCS hosts.
- Some applications for reading e-mail via POP may have trouble with long (greater than 8 character) passwords. This should only affect your choice of a .mail Kerberos instance password, not your main Kerberos password.
- Windows 98 and 95 only support passwords up to 14 characters long.

In a Windows environment, there are certain security advantages to be gained if your password is 15 characters or longer.

Can I write my password down?

You should avoid writing down your password or giving it to others. You should especially avoid writing it down and leaving it in a non-secured place such as on a post-it on your monitor or a piece of paper in your desk. If you absolutely must write something down, we suggest doing the following:

- Don't write down the entire password, but rather a hint that would allow you (but nobody else) to reconstruct it.
- Keep whatever is written down in your wallet or other safe place that only you have access to and where you would immediately notice if it was missing or someone else gained access to it.
- You may want to consider using a password protected password list. You may accomplish this by password protecting a Word file that contains your passwords or by using any number of open-source password protection software programs.

Why is this important?

It is very common for intruders to attempt to break-in to systems (both Unix and Windows) at SCS by trying to guess people's passwords. Sometimes they succeed, and when they do it is often because people chose very poor passwords (like "password" or "administrator"). These break-ins can result in a significant amount of downtime, lost work, and loss of privacy (for example, if there is credit card and other financial data on your machine). Intruders often also install keyboard sniffers that let them gather additional passwords and put more machines at risk. They can also conduct dictionary attacks against a host's password database, and literally try out tens of thousands of potential passwords per second, which is why words and simple variants of words are not good passwords.

Other things to consider

- It is recommended that each Library maintain a list of passwords and keep it in a secure location under lock and key or in a safe. The list can be saved to a computer with password protection enabled on the document. Only key people should have authorized access to the password list.
- You may want to change your passwords routinely. It is recommended that you do so at least every three months.
- Some websites, or systems, don’t allow special characters. When this is the case, try to use a variety of numbers and capital letters to make your password stronger.
- Change high level passwords when certain staff, or technical support, are no longer working at your Library.