WTO PASSWORD POLICY.

1 Guidelines for users: How to choose a good pass phrase

This guideline explains the content of the authentication policy and provides some assistance in the creation of a sufficiently strong pass phrase.

2 Introduction

The WTO Information Technology Security Policy requires that all information used in support of WTO operations should be protected in a manner commensurate with its sensitivity, value and criticality. In particular, it states that access to all resources shall be granted only to authorized users. It also stipulates the need for more transparency and calls for the explicit accountability for all information technology systems and all data stored in or transmitted through them.

Authorization and accountability require that all users can be uniquely identified and unambiguously authenticated. Access to the WTO internal network therefore requires that you

- Identify yourself with your User Name (i.e. your name), and
- Authenticate yourself by typing a secret pass phrase that is only known to you. (The term “pass phrase”• is used instead of the more familiar “password”• to emphasize the possibility and necessity to construct “complex”• phrases)

As it is fairly trivial to “guess”• a user name, the pass phrase is the single most important protection for your user account.

If your pass phrase is known to anyone else, this person will be able to assume your identity and access all data and services with your privileges.

3 How to choose a good pass phrase

Your pass phrase should be difficult to guess, but easy for you to remember (and type!). The longer it is and the more random it appears, the harder it will be to guess.

4 A good pass phrase should *not*:

- Be simply a word that can be found in a dictionary (of any language).
- Be trivial like “ABC”• .
- Include any information about you that can be easily guessed by a determined adversary.
    - Your first, middle, or last name in any form (as-is, reversed, capitalized, doubled, etc.).
    - Your spouse's, girlfriend's, boyfriend's or child's name.
    - Your (or anybody else's) nickname
    - Birthdates
    - Telephone numbers
    - Licence plate numbers
    - ID numbers
    - Bank account numbers
    - The brand of your automobile
    - The name of the street you live on
    - ...
- contain the string “WTO”• .
- embody a computer name, a user identifier or any parts of those.
- consist of keys next to each other on the keyboard, e.g.: qwerty(z), mnbvcx or 12345.
- be made up of well known acronyms or abbreviations.
- be modified by pre- or suffixing a number or any other (special) character (**password1**, **0password**, **.password$**, **%password**, ...)

5 A good pass phrase should:

- Be at least 8 characters long.
- Consist of lower case and upper case alphabetic characters as well as of numbers and/or special characters.
- Not include any character that cannot be found on the most common keyboards (e.g. to logon from a different computer or check e-mail from an Internet cafe).
- Be easy to memorize, simply because it should not be written down.
- Nevertheless, be as complex as possible.

In the current infrastructure a minimum level of complexity is enforced by the requirement that a pass phrase contains characters from at least three different of the following categories:

1.English upper case letters: **ABCDEFGHIJKLMNOPQRSTUVXYZ**
2.English lower case letters: **abcdefghijklmonpqrstuvwxyz**
3.Westernized Arabic numerals: **0123456789**
4.Non-alphanumeric (“special characters”•):**{}[],.<>;:'"?/\`~!@#$%^&*()_-+=**

Pass phrases that do not follow these rules will not be accepted by the authentication system.

A blank character (the “space bar”•) is allowed in a pass phrases, however, it does not fall into any of the four categories.

6 How to create a good pass phrase

A good pass phrase should be easy for you to remember. You will be using it every day, so spending a few minutes to create a good pass phrase is certainly worth the time. The best advice for creating secure pass phrases is:

> "Utter nonsense makes the most sense."•

As an example, you could use grossly misspelled words or sentences, or a combination of seemingly unrelated words. Another common method is to replace letters with numbers: *zero* instead of "O"• ,*one* instead of "L"• , *three* instead of "E"• , or *seven* instead of "T"• .
The use of fantasy words or phrases is also a reliable method for creating "random"• strings that are easy for you to remember but hard to guess for others. Small children are an extremely good source for these types of pass phrases (as long as you don't pick fantasy terms from very popular sources like Harry Potter.)

A simple way to create a pass phrase that fulfils these requirements would be to use two words, at least one of which begins with a CAPITAL LETTER, and separate them by a hyphen ("-"•) or underscore ("_"•): "**Pass-phrase"•** , "**pass_Phrase"•** , "**Pass_Phrase"•** , "**Good-morning"•** , ...

If the pass phrase contains another "special character"• or a number, you can also use the "space"• (blank) character for separation: "**Pass phrase1"•** , "**pass Phrase1"•** , "**Pass Phrase1"•** , "**Lausanne 154"•** , "**fax: 5791"•** , "**Good morning!"•** , ...

A different method to construct a good pass phrase is to create a simple sentence of at least 8 words and choose letters from each word to make up a pass phrase. You might take the initial or final letters, or use multiple letters per word, e.g. for different syllables. You should put some letters in upper case to make the pass phrase harder to guess, and at least one number and/or special character should be inserted as well.
An example of such a composition might be using the phrase is *"It's noon and I am hungry!"*• to create the pass phrase **I's12&Iah!**, which is hard for anyone else to guess but easy for you to remember.

By all means use a foreign language if you know one. You could even mix words from several languages. However, do not just use a single word or a name from a foreign language. Try being creative!

7 How to maintain a good pass phrase

After you have chosen a good pass phrase you need to take some steps to ensure that it remains a personal secret that can uniquely authenticate you.

- **Keep your WTO pass phrase different from any other pass phrase.**
  This will ensure that your WTO account will still be protected even if other pass phrases are compromised.
- **Change your pass phrase frequently and do not reuse old pass phrases.**
  The current system requires all users to change their pass phrase at least twice a year (every 180 days to be precise). You will be reminded to do so for thirty days prior to

the expiration date of your pass phrase. The authentication system is configured not to accept a recently used pass phrase.

- **Do not tell anyone what your pass phrase is.**
  You should not share your pass phrase with anyone — not even staff of ITSD. Only you alone should know your own pass phrase. Do not tell a person verbally, by electronic mail or by any other means. Passing your pass phrase through e-mail is dangerous, since it could be easily intercepted, and other people besides the intended receiver could read your email as well.
- **Do not record your pass phrase online.**
  Recording your pass phrase in your PC would be dangerous as well, since someone could look for it while your PC is unattended. Although a screen-saver that locks the workstation can offer some protection, it is not recommended.
- **Do not write down your pass phrase.**
  Pass phrases should not be written down, for someone could find it and try it out on your account.
- **Do not allow anyone to watch while you type your pass phrase.**
  Make sure nobody is around when you are typing in your pass phrase. If there is anybody, ask them to turn their back on you when you are doing this. Do not underestimate the power of glancing!
- **Do not give out your private information too quickly.**
  Whenever you are being asked for your private information over the phone, internet or other means, make sure you have confirmed the identity of the requester before any information is surrendered. If you have any doubts as to the identity or the legitimacy of the request, do not give out any information and inform the Service Desk about this incident.