Contract concerning the utilization of SLU's computer resources

This contract has been drawn up between the undersigned and SLU through the IT Unit in order to regulate the use of SLU's computer resources.

Rights

1. This contract gives the undersigned the right, **within the framework of his/her activity** at SLU, to utilize SLU's computers, network, modem pool and other network-related resources.

2. The undersigned will be assigned a **personal** user ID that gives him/her access to computers, servers, e-mail, etc.

Obligations

The regulations governing the use of SLU's computer network are to be complied with.

This means, but is not limited to, the following:

1. The undersigned shall at all time use his/her own user ID in combination with a well-construed password and the settings for connection advised by the IT Unit/IT coordinator. The undersigned agrees never to loan out his/her user ID/password to any other person.

   (Enclosure: "What is a good password?")

2. The undersigned may use another user's file space allocation but only after obtaining the consent of the user (see point 5.3).

3. The undersigned may not loan out or transfer any of SLU's computer or network resources to a third party/outsider (including a spouse or child). Services may not either be distributed via the Internet (e.g., file archives, film archives, music archives, program archives, commerce, information publication) that are not part of SLU's operations and activities.

4. Copyright to software and data is to be respected.

5. The undersigned is obliged to report the occurrence, or suspected occurrence of security incidents/breaches to the IT Unit.

Sanctions

1. In the case of suspicion of misuse, the undersigned's user ID may be shut down and his/her files may be locked while an investigation is conducted.

2. Where an actual breach of this contract has occurred, the undersigned will be blocked from using SLU's computers and other network resources.

3. Inappropriate or indecent use of the computers in the computer network may result in disciplinary actions for employees in accordance with Sweden's Public Employment Act.

4. Repeated cases of misuse will be reported to SLU's Disciplinary Offences Board.

Misuse of computers may also be a criminal offence under Swedish or foreign law, which can result in legal action.

The undersigned hereby confirms that he/she has read and accepted the above.

□ Student □ Employee

Date ………………..………………………………….. Place…………………………………………………..

If employee:
Faculty/Equiv……………………………………….. National registration no………………………………

Signature..………………………………………………………………………………………………..

Name in block letters……………………….…………………………………………….……………

This contract has been drawn up in two originals, one of which the IT Unit (or where applicable, the Department's IT Coordinator) will archive.

What is a good password?

A secure (=difficult to guess) password should meet the following criteria:

1. *It should be 7-8 characters long (it is deemed possible that all words up to 6 characters could be generated and tested by machine/computer within a reasonable time period, and many systems do not test more than 8 characters).*

2. *Do not use a password that has any direct link to yourself, your family or your workplace and which others know of, for example, your national registration number, phone number, car registration number, your initials, user ID or other easily accessible information.*

3. *Do not use letters only. Include at least one number. You should also include at least one upper case and one lower case letter.*

4. *It should not be possible to find the word in any glossary or dictionary, and it should not either be a simple joining of two words.*

5. *Personal names (by themselves or joined together) should be avoided for the same reasons.*

6. *Do not either use simple keyboard patterns such as QWERTYU or 1qaz2wsx.*

7. *If the password contains parts of a word, replace, remove or add one or more characters to break it up. However, using an ordinary word or name with one character replaced, removed or added does not provide sufficient security and neither does reversing the order of the letters in a word or name.*

8. *Do not use the Swedish characters å ä ö in the password.*

It is obvious too that you should avoid allowing the computer to store your user ID and password for automatic log-in.

Based on the need for a password to be reasonably difficult to guess or to test for to discover while at the same time being relatively easy to remember, we recommend the following methods:

A. *Form the password from the first letters of each word in a phrase from a poem, book title, literary quote, song text, hymn verse, line from a play, nursery rhyme, slogan, saying or just a sentence. (The result should of course not be a recognisable word found in any dictionary as mentioned previously. Avoid also very well known or familiar quotations.) Make one or more of the letters upper case and include a number. For example, you could take the saying "It's an ill wind that blows nobody any good" to form the password iaiWtb2nag.*

B. *Another possibility is to select a string of 7-8 characters (without spaces) from such a phrase or saying, starting anywhere in the phrase. Here too, you should make one or more of the characters upper case or add a number. For example, you could form the password aNil3lwi or lowS8nob from the above saying.*

You should put some time and effort into constructing a secure password. Being able to keep a good password for a long time is obviously far better than having to change bad passwords often. (If you suspect that any unauthorized person might have found or guessed your password, it must naturally be changed immediately.)

It is of course NOT appropriate to write down your password and keep the paper on which it is written close to your computer workstation (under a desktop mat or taped to the wall, for example).

You should take the time to plan a new password carefully – not make it up on the spur of the moment. If you have a good rule of thumb for how to form your password, this in itself becomes a key to being able to easily recall the password so that you will not need to write it down.