APPLICATION FOR ACCESS TO THE HR MANAGEMENT INFORMATION SYSTEM (HRIS)

HRIS Application Forms should be forwarded to the Manager, Information Systems, Human Resources (fax: 9748 or e-mail: lorraine.francke@mq.edu.au)

Family Name: _____ Other Names: _____

Faculty/Office: _____ Department: _____

Staff Number: _____ Extension No: _____

Email Address: _____ . _____ **@mq.edu.au**
(preferred name . last name)

Computing Liaison Officer (CLO): _____ Extension No: _____

ACCESS REQUIRED

Faculty/Office Code: _____ Dept./Discipline/Section Code (if applicable): _____

Level of Access required: ☐ View **OR** ☐ Change

AND: ☐ Timesheet Entry only (TSE) ☐ Faculty Staff access (SC9)

☐ Discoverer access

☐ Budget Module (BC1 - OFS staff only)
☐ Training Module (TD1 – OD staff only)
☐ Stats Module (ST1 - MIU staff only)
☐ Directory/Lookup (DS1 - Informatics staff only)
☐ EEO Module (EO1 - Equity staff only)
☐ HR staff access (HR1 - HR staff only)

APPROVAL

Head of Office or Faculty General Manager: _____ Date: ___ / ___ / ____

CONDITIONS OF USE

- I will use only those IT facilities for which I have been authorised;
- IT facilities may only be used for the purposes for which they have been provided and not be used for other projects, games 'hobby computing', private or consulting work;
- IT facilities must not be wasted or consumed by inappropriate or irresponsible use;
- I must not attempt to tamper with any IT facility in any way which might impede its use by others;
- I must not harass others, including using computing facilities to send obscene, abusive, fraudulent, threatening or unnecessarily repetitive messages;
- I will take every precaution to ensure that passwords, accounts and data are adequately secured;
- Any computer account allocated to me is for my exclusive use. I will not allow another person access.

I understand and agree to the above Conditions of Use.

Staff Member's Signature: _____ Date: ___ / ___ / ____

HR SYSTEMS USE ONLY

HRIS account created: _____ (inits) Date: ___ / ___ / ____

(Staff Member to keep this section)

Choosing good passwords

Australian Computer Emergency Response Team http://www.auscert.org.au/
http://www.auscert.org.au/Information/Auscert_info/Papers/good_password.html
Reproduced with Permission

How hard is it to choose a good password? Most people believe that choosing a good password is easy. After all, how is somebody going to guess my wife's maiden name?
In reality, people usually choose poor passwords. In 1990 [Klein 1990] an attempt to crack a large password database revealed over three hundred passwords in the first fifteen minutes! One fifth of all passwords were obtained in the first week and approximately one quarter were cracked by the end of the search. More than half of the cracked passwords were six characters or less and some accounts didn't even have a password.

An intruder only needs one password!

Choosing a good password is a trade-off between something that is difficult to guess versus something that is easy to remember. While *@G7x.m^l* is probably a good password, nobody will remember it and it is certain to appear as a sticky note attached to a terminal. Conversely, your first name is very easy to remember, but it is also trivial to guess.

Some simple rules of thumb

Some simple guidelines that will help you choose better passwords are:
• A password should be a minimum of eight characters long.
• Try to include some form of punctuation or digit.
• Use mixed case passwords if possible.
• Choose a phrase or a combination of words that make the password easier to remember.
• Do not use a word that can be found in *any* dictionary (including foreign language dictionaries).
• Do not use a keyboard pattern such as *qwertyui* or *oeuidhtn* (look at a Dvorak keyboard).
• Do not repeat any character more than once in a row like *zzzzzzzz*.
• Do not use all punctuation, all digit or all alphabetic.
• Do not use things that can be easily determined such as:
• Phone numbers.
• Car registration.
• Friends' or relatives' names.
• Your name or employment details.
• Any Date.
• **Never** use your account name as its password.
• Use different passwords for each machine.
• Change the password regularly and do not reuse passwords.
• Do not append or prepend a digit or punctuation mark to a word.
• Do not reverse words.
• Do not replace letters with similar looking numbers. For instance, all of the letters *i* should not be blindly replaced by the digit *1*.

Cracking passwords

The principle behind password cracking is quite simple: take a large word list, encrypt each word and check if the encrypted string matches the user's password. Word lists that are used frequently include English and other language dictionaries, common names, pet names, television and movie characters, character patterns on keyboards (for example, *qwerty*) and jargon or slang terms.
To allow for the case that the user has not chosen a word in your word list, an intruder can and usually will apply a large number of simple rules to each word in the word list and check if any of these encrypt to the user's passwords. Typical rules include appending and prepending digits and other punctuation characters to words, reversing words, capitalising words, converting words to all upper or all lower case, substituting letters or digits for other letters and naturally many combinations of these. Since computers are fast, applying these rules and encrypting the resulting guess doesn't take much time and a lot of guesses can be made in a very short time. In addition, a CD based database is supposed to have been produced that contains every word in a large dictionary plus many rule based permutations of these words encrypted in every possible manner. This reduces password cracking to a simple (and fast) database lookup.

How long is a good password?

The simple answer to this is that in general the longer the password the better. Assuming that you're using a reasonable selection of characters for your password, say letters and numbers, then the following table presents the number of passwords possible for the various choices of length. It also includes an estimate of how much time would be required to crack the password using a brute force attack.
The *cracking time* field is derived from a report in September 1993 that claimed the record for the speed of cracking passwords. The claim was that 6.4 million passwords per second could be tested.

Number of passwords for each length

Length	Number of Passwords	Number of passwords	Cracking Time
1	62	Not nearly enough	Try this by hand
2	3844	Three thousand	Almost no time
3	238328	One quarter of a million	Less than one second
4	14776336	Fourteen million	Two seconds
5	916132832	Almost one billion	Two and a half minutes
6	56800235584	Fifty six billion	Two and a half hours
7	3521614606208	Three and a half trillion	One week
8	218340105584896	Two hundred trillion	One year
9	13537086546263552	Thirteen quadrillion	Seventy years
10	839299365868340224	Eighty three quadrillion	Forty centuries

Having said that longer is better, it is important to note that many machines artificially restrict the length of the password usually by silently truncating what you enter to their maximum length. Since this length is often eight characters under Unix, the rest of this article will assume that an 8 character password is being used.

What characters should a good password contain?

The previous section assumed passwords consisted of upper and lower case letters and digits. What happens if this character set is increased or decreased? The next table shows some of the options for 8 character passwords:

Number of eight character passwords

Type of Password	Number of Characters	Number of passwords	Cracking Time
7-bit ASCII	128	72057594037927936	350 years
Printable Characters	95	6634204312890625	Thirty three years
Letters and Numbers	62	218340105584896	One year
Letters only	52	53459728531456	Ninety six days
Lowercase/one uppercase	26/special	1670616516608	Three days
Lowercase only	26	208827064576	Nine hours
English words: 8 letters or more	special	250000	Less than one second

So clearly, the richer the character set being used, the harder it will be to crack passwords. You should attempt to include as a minimum both upper and lower case characters and if possible, you should also include some digits, punctuation symbols and/or control codes in your password.

Examples of how to construct good passwords

So now that typical bad passwords have been discussed, how is a good password constructed? Try combining two or more words together or taking the first (or second or last) letter of each word in an easily remembered phrase. Then mangle the result by adding capitals, digits and punctuation characters. As an extra measure, control characters can also be introduced.

Some examples of using multiple words with punctuation

Here is a pair of good examples of using multiple words:
• gOt%L0st! - got lost! • heLP4me$ - help for me (money) And here is a bad one: • T0gether - to get her

Some examples of using a phrase

Here is a pair of good examples of using phrases:
• rsKf0myH - Raindrops keep falling on my head.• wru2rxy? - Who are you to ask why.

References

KLEIN 1990 Klein, D., *"Foiling the Cracker": A Survey of, and Improvements to, Password Security*,
Proceedings of the UNIX Security Workshop II, Portland, August 1990.