## Creating Strong and Safe Passwords Information Sheet

All Computer Systems users will be asked to create multiple passwords for different systems making it difficult to create and remembering strong passwords. This information sheet provides some tips for creating and remembering passwords to assist you in storing information securely.

In 2012 the Australian Communications Consumer Action Network issued consumers with the following advice about creating strong and safe passwords:

**Do’s:**

* Use long passwords – they’re harder to crack. Aim for eight or more characters.
* Use variety – the greater variety of characters in your password, the better. A strong password will include a combination of lower and upper case letters, a special character (e.g. $, #, \*), and a numeral.
* Change your passwords regularly – set an automatic reminder to change them every few months.

**Don’ts:**

* Don’t use the same password for more than one account. If hackers are able to obtain your online password for one account, they can run software to try the same email/password combination for all your other accounts.
* Avoid using common words that can be found in any English or foreign dictionary.
* Avoid words spelled backwards, common misspellings and abbreviations, e.g. koolpassword, retupmoc.
* Don’t use sequences or repeated characters, e.g. 123ABC, qwerty.
* Don’t use any of your personal information, even if it’s easy to remember, e.g. your name, yours or your families birthdays, street name or your passport number.

**Tip’s**

Some creative solutions to keeping track of all your passwords:

* Create a short phrase that you’re likely to remember**.**
* For example, John Smith will make 30 cakes on Friday. Now, simply take the first character from each word to create your password, where the example would become JSwm30coF. Notice how there is a mixture of upper case, lower case, numerals, and just to be sure, you can put a special character at the end, to create JSwm30coF\*.
* Another example, Alex Harris can eat 10 hot dogs only on Thursdays, will become AHce10hdooT. Once again, adding a random, special character will add to the strength of your password, so this password becomes #AHce10hdooT. These types of passwords are extremely strong, as they are very long and don’t use common English words.
* Consider using password-management software. Depending on which software you choose, the basic idea is that the software will generate and manage your passwords for all your sites across all your computers. Staff members are encouraged to make sure that any password-management site they use is secure by reading their privacy policy. Some examples include LastPass, RoboForm Pro, or Sticky Password.