**Password Guidelines**

What is a password? Your computer password is your personal key to a computer system. Passwords help to ensure that only authorized individuals may access computer systems. Passwords also help to determine accountability for all transactions and other changes made to system resources, including data. If you share your password with a colleague or friend, you may be giving an unauthorized individual access to the system. What if the individual gives your password to someone else? What if some of your files are deleted or otherwise rendered unusable? Are you willing to take the blame if an unauthorized individual uses your access privileges to damage the information on the system or to make unauthorized changes to data?

Authentication of individuals as valid users, via the input of a valid password is required to access any shared automated information system. Each user is accountable for the selection, confidentiality and changing of passwords required for their personal authentication purposes. Since you are responsible for picking your own password, it is important to be able to tell the difference between a good password and a bad one. Bad passwords jeopardize the information that they are supposed to protect. Good ones do not.

**Note: Do not use any of the password examples shown in this document.**

Following are some simple rules you should keep in mind about passwords.

* Passwords should be kept confidential and should never be shared.
* Passwords should not be written down.
* Never use the same password twice. When you are selecting a new password, choose one that is very different from your previous password.
* Passwords should be changed frequently. The shorter the life of a password, the better it is. Some systems force users to change their password at predetermined intervals.
* Passwords should be at least fourteen characters in length. Longer passwords are harder for others to guess. We have gone to fourteen for more security and to also make remembering a password easier. It is easier to remember (and type) a phrase than 8 random characters, numbers, and symbols.
* Passwords should not be obvious, predictable or trivial.
	+ **Obvious** passwords include names of persons, pets, relatives, cities, streets, your Logon ID, your birth date, car license plate, and so on.
	+ **Predictable** passwords include days of the week, months, or a new password that has only one or two characters different from the previous one.
	+ **Trivial** passwords include common words like 'secret', 'password', 'computer', etc.
* Your password should not be the same as your User/Logon ID, an anagram of your User/Logon ID or a palindrome of your User/Logon ID. If you have access to a number of systems that require the entry of a password, do not use the same password for both systems.
* A good password is relatively easy to remember but hard for somebody else to guess. There are a variety of techniques you can use to choose secure passwords.
* Following are examples of some examples of good passwords that are easy to remember:

isawaplanetoday

myhusbandisnice

ihavemonkeyarms

bigcatsdoeatmice

limeflavoredapples

* For further security, add in a random number to your password. Change an “o” to 0 or an “e” to a 3.
* Finally, please remember that there is no need to share IDs and passwords.