Policy # 01-06
Date Adopted: May 7, 2003
Revised: March 8, 2006

PASSWORDS

Division of Criminal Justice Services

Approved By:
Francis X. Aumand III
for the VIBRS Advisory Board

NOTE - This is a mandatory policy.

1. Purpose

1.1 Passwords represent the primary means of insuring system security. VIBRS system security is the responsibility of every user within the network. The first line of defense in system security is the selection of a good password. It has been estimated that 80% or more of all security breaches occur because of poorly chosen passwords or compromised passwords. Therefore, the purpose of this policy is to enforce the selection of passwords that follow the below standards as well as provide guidance on the selection of good passwords.

1.2 The passwords for access to the VIBRS Network are computer generated and given out by the VIBRS staff at the Division of Criminal Justice Services for new users.

2. Policies

2.1. Users must change their password every 120 days.

2.2. You cannot change your password until it is at least 100 days old. If you feel your password has been compromised, call the Help Desk to force a change for you.

2.3. Passwords cannot repeat any of your previous 3 passwords.

2.4. Password Complexity

2.4.1. Passwords must contain at least 8 characters.
2.4.2. Passwords cannot contain 3 or more contiguous characters of your username or full name.
2.4.3. Passwords must contain characters from at least 3 of the following four categories:

2.4.3.1. Uppercase alphabet characters (A through Z)
2.4.3.2. Lowercase alphabet characters (a through z)
2.4.3.3. Numbers (0 through 9)
2.4.3.4. Special characters, such as ! @ # $ % & * ( )

2.5. Do not reveal your password to anyone for any reason.

2.6. Do not use your VIBRS password for any purpose on the internet, such as using it for web mail accounts (i.e. yahoo.com, hotmail.com, gmail.com) or when purchasing from a web store.

2.7. Creating “good” passwords

2.7.1. Do not use anyone's name, pet’s name, place name or a fantasy character (from movies, books, cartoons, etc).
2.7.2. Do not use your phone number, social security number, employee ID, zip code or any other common number.
2.7.3. Do not use anything that may be easily guessed about you.
2.7.4. Do not use a word that can be found in the dictionary.
2.7.5. Do not use a pattern of letters found on the keyboard such as qwerty or 1234.
2.7.6. Do not use the first initial of your family members.
2.7.7. Do not use any of the above spelled backward, preceded or appended with a single digit.
2.7.8. Pick a password that is easy to remember so it does not have to be written down.
2.7.9. Examples of good passwords. These are no longer good passwords, do not use them.

2.7.9.1. Think of an easy phrase: “It’s Easy to Create Good Passwords!”. From this phrase, extract the first letters and special characters, substitute the number 2 in place of the word ‘to’ and vary the case of the letters. This results in the password: I’sE2cGp!

2.7.9.2. Alternate 3 or 4 consonants and vowels, put in a special character and then alternate 3 or 4 consonants again. wEda%SED, ROki$pAD, zik!POKI

2.8. If you wish to write down your password please use the following guidelines:

2.8.1. Do not attach your password to your terminal, keyboard, desk, etc.
2.8.2. Do not include your login name on the same piece of paper as your password.
2.8.3. Do not identify your password as being a password.
2.8.4. Camouflage your written password. If your password is oshP:635, a card in your Rolodex for a fictitious person might be: William Osh P:635-1234. Now that this idea has been written out here, it is not a good idea to use it. Be imaginative.