Policy Title: _____Policy on Password Security___

Supercedes/Amends: _____

Prepared by: ____Richard Lindstrom_____Issued/Revised: __2/22/2008_

_____ Effective:___7_/_01_/_2008__

1.0 Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts private information. A password that is easy to guess or which goes unchanged could result in the compromise of Charles Drew University's network and the sensitive information stored there. To prevent this, all Charles Drew University network users (including contractors and vendors with access to Charles Drew University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all users of University information resources who have a user account (or any form of access that requires a password) on any system provided by the University, has access to the University network, or stores any non-public University information.

4.0 Policy

4.1 General

- All passwords must conform to the password guidelines for strong passwords described below.
  - This makes a password stronger, and less likely to be guessed or cracked.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. Campus systems that are capable of it will automatically require users to change passwords at this frequency.
  - This mitigates the risk of a password being obtained and used by an unauthorized person.
- Administrative (system level) passwords must be changed every 60 days.
  - This provides additional protection for critical administrative accounts.
- Default passwords and guest accounts will be changed or disabled on all systems.
  - This will prevent widely known access methods from being exploited.
- Users with administrative accounts that have system-level privileges granted through group memberships must have a unique password for each accounts held by that user.
  - This prevents unauthorized access to multiple systems if a password is acquired by an unauthorized person.
- Passwords must not be inserted into email messages or other forms of electronic communication.
  - Email can be forwarded or misdirected, and it is not safe to use it to send passwords.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

4.2 Password Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Charles Drew University. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Everyone should use only strong passwords for their accounts.

Poor, weak passwords have the following characteristics, and should not be used:

- The password contains less than six (6) characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Charles", "Drew", "University ", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the word spelled backwards.
    - Any word preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics, and must be used:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least six alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for University accounts as for other non- University access (e.g., Yahoo! Email account, online banking, etc.).

Do not share your passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Charles Drew University information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to your supervisor or subordinate
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
-

If someone demands a password, refer them to this document or have them call someone in the Information Systems Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Instant Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident to the Information Systems Department and change all passwords.

5.0 Enforcement

The Information Systems Department may periodically conduct password security audits. Any employee found to have violated this policy may be subject to disciplinary action and loss of access to University systems.