Password Policy

1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of George Wythe University's entire network. As such, all George Wythe University employees, volunteers, faculty, and staff (including contractors and vendors with access to George Wythe 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 personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any George Wythe University facility, has access to the George Wythe University network, or stores any non-public George Wythe University information.

4.0 Policy
4.1 General

- All user-level and system-level passwords must conform to the guidelines described below (see section 4.2).
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every twelve months
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- All system-level passwords (e.g., root, administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the administrator global password management database.
- Passwords must not be inserted into email messages or other forms of electronic communication. Except for new account creation, these systems must enforce a change after first use.

4.2 Guidelines
A. General Password Construction Guidelines
Passwords are used for various purposes at George Wythe University. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and VPN access. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following chdaracteristics:

- 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.
    - The words "George Wythe University", "gwc", "gwu", “liber” 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 above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- 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 fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- 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 George Wythe University accounts as for other non-George Wythe University access (e.g., personal ISP account, bank accounts, email, etc.) Maintaining three passwords that are changed at least yearly and meet these guidelines is strongly recommended. For example, select one password for George Wythe University administered systems, and select another for work related, but non-GWU administered systems (e.g., Amazon.com, online stores, libraries, etc.). Also select another for your own person non-work related passwords.

Do not share George Wythe University passwords with anyone, including administrative assistants, secretaries, or the individual that will fill your position when you leave. All passwords are to be treated as sensitive, Confidential George Wythe 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 the boss
- 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.

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.

Change passwords at least once every twelve months (except system-level passwords which must be changed quarterly).

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

Password cracking or guessing may be performed on a periodic or random basis by the Information Systems Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

5.0 Enforcement

6.0 Definitions

Terms	**Definitions**
Application Administration Account	Any account that is for the administration of an application (e.g., CAMS, QuickBooks, Scholar).
User Level	Any account that is standard access.
System Level	Any account that has access elevated above that of user-level.

8.0 More Information

For more information or clarification please contact tech@gwc.edu

8.0 Revision History

September 1, 2008 - v1.0 - Original Release