CAPITAL UNIVERSITY
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 Capital University's entire university network. As such, all Capital University computer and network account holders 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 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 Capital University facility, has access to the Capital University network, or stores any non-public Capital University information.

4.0 Policy

4.1 General

4.1.1 User-level accounts

- All user-level passwords (e.g., email, Colleague, desktop computer, etc.) must be changed at least every 90 days.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level passwords must conform to the guidelines described in the Appendix.

4.1.2 System Administration Accounts

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) are changed based on a frequency defined for the specific system, but at a minimum must be changed on at least an annual basis. Where practical, system-level passwords will be changed quarterly.
- All production system-level passwords must be documented and secured in the Capital University IT-administered and encrypted global password management database.
- 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.
- 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).
- All system-level passwords must conform to the guidelines described in the Appendix.

4.2 Password Maintenance

4.2.1 Forgotten Passwords – all users are required to maintain and protect their own account passwords. If a user has forgotten their password, they must contact the IT Helpdesk during normal hours of operation to have the password reset.

4.2.2 Account Locks – if an incorrect password is entered ten (10) times within ten (10) minutes, the system will automatically lock the account for thirty (30) minutes.

4.2.3 Compromised Passwords - If a password is suspected to have been compromised, report the incident to the IT Helpdesk and immediately change all passwords.

4.2.4 Password Resets – Per the Capital University User Account Policy, account access is terminated for users who are no longer in good standing with the university, and passwords will be immediately changed by the IT Department to prevent continued account access.

4.2.5 Password Validation - Password audits may be performed periodically by the Information Technology Department to assure adherence to password complexity standards. Audits will not reveal actual passwords, but will alert when a non-secure password exists. Users will be notified if their password does not pass a complexity standard audit.

5.0 Enforcement

Accounts that have not had their password changed within the required change timeframe will be disabled until the user has been contacted by IT and given an opportunity to update their account. Violation of this policy may result in disciplinary action consistent with the Acceptable Use Policy and other University policies, including provisions in relevant handbooks (student, faculty, administrator, and support staff).

6.0 Definitions

Terms	Definitions
Keyed hash	A keyed hash is a type of message authentication code (MAC) calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key.
SNMP	Simple Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects.
SNMP Community String	A SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the management station (the SNMP manager) and the device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent.
sudo	A unix command, the sudo command stands for "superuser do". It prompts for a personal password and confirms the request to

execute a command by checking a file, called sudoers, which the system administrator configures. Using the sudoers file, system administrators can give certain users or groups access to some or all commands without those users having to know the root password. It also logs all commands and arguments so there is a record of who used it for what, and when.

7.0 Revision History

5/27/08	Draft submitted to legal for review.
6/2/08	Comments received from legal.
6/3/08	Approved by President's Cabinet.

Appendix

A. General Password Construction Guidelines

Passwords are used for various purposes at Capital University. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Capital University systems do not currently have support for one-time tokens (i.e., dynamic passwords which are only used once), therefore, everyone should be aware of how to select strong passwords.

Most Capital University passwords are **required** to have these complexities:

- Minimum length of seven (7) characters
- The current and past seven (7) passwords are not eligible for re-use
- Passwords will expire 90 days after each change
- You may only change your password once a day
- Passwords are case-sensitive (TmB1w2R! is different than tmb1w2r!)
- May not contain your name or username
- Passwords must contain three (3) or more of the following:
    - At least one upper-case letter
    - At least one lower-case letter
    - At least one numeric digit
    - At least one special character, such as:
      ! # $ ^ * - _ = ; : ´ " ( ) { } [ ] | ` ~
        - Avoid using the following characters: @ % & ? / \ + since they may not work with all university systems

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 seven alphanumeric characters long (b0rn2W!n).
- 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!

Poor, weak passwords have the following characteristics:

- The password contains less than seven characters (unless the system is restricted to less than seven, such as NIS+)
- 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 “Capital University ", "bexleyoh", "coloh", “columbusoh” 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)

B. Password Protection Standards

Do not use the same password for Capital University accounts as for other non-Capital University access (e.g., personal ISP account, Facebook or MySpace, online banking, benefits, etc.).

Do not share Capital University passwords with anyone, including roommates, student workers, family members, co-workers, administrative assistants or consultants. All passwords are to be treated as sensitive, confidential Capital 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 Technology Department.

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

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including smart phones, PDAs, or similar devices) unless that file is encrypted.

Change passwords at least once every 90 days.

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

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support AD integration / Kerberos, TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.