Smeal College of Business - Password Policy: SCB-PW-01

1.0 Purpose

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 the Smeal College of Business computer network. As such, all Smeal College of Business employees (including contractors, temporary personnel, and vendors with access to Smeal College of Business systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish guidelines for creation of strong passwords, the protection of those passwords, and the frequency of change.

2.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of data communications access) on any system that resides at any Smeal College of Business facility, has access to the Smeal College of Business network through local or remote connectivity, or stores any non-public Smeal College of Business information.

Note: All faculty, staff and students are bound by ITS policies regulating their Penn State Access accounts. Those policies can be viewed at http://its.psu.edu/policies/password.html

3.0 Policy

3.1 General

- All system-level passwords (e.g., root, enable, Windows admin, application administration accounts, etc.) must be changed on at least a semester basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" under UNIX, or “Run As” under Windows must have a password different from passwords used with any other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- 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 user-level and system-level passwords must conform to the guidelines described below.

3.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at the College of Business. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should know how to construct strong passwords in order to protect their accounts.

Weak passwords have the following characteristics which should be avoided:

- The password contains less than eight 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.
    - The user’s ID, or subset thereof.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "College of Business", "SCB", "<Department Name>" 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 which must always 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 eight alphanumeric characters in length (more is better and is sometimes easier to remember).
- Are not a real 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 Smeal College of Business accounts as for other non Smeal College of Business access (e.g., personal ISP account, stock trading, benefits, on-line shops, ebay, web bill pay or personal banking accounts, etc.). Where possible, don't use the same password for various Smeal College of Business access needs. For example, select one password for the College administrative systems and a separate password for lab systems. Also, select a separate password to be used for a Windows account and a UNIX account.

Do not share Smeal College of Business passwords with anyone, including family, friends, or other co-workers. All passwords are to be treated as sensitive, confidential Smeal College of Business information.

Below are some simple rules for keeping your password (and therefore your account) secure:

- 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 manager
- 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 for use while on vacation

If someone demands a password, refer them to this document or have them call someone in the RIIT Group or University Security Department.

Avoid using the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape 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 PDAs, cell phones or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to the RIIT Group and change all passwords for your accounts immediately.

Password cracking or guessing may be performed on a periodic or random basis by the University Security Office, RIIT Group or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change their password.

C. Application Development Standards

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

- must support authentication of individual users, not groups.
- must not store passwords in clear text or in any easily reversible form.
- must provide for role management, such that one user can take over the functions of another without having to know the other's password.

D. Use of Passwords and Passphrases for Remote Access Users

Access to Smeal College of Business networks, computers or other devices via remote access must be made through an encrypted tunnel, established using either a one-time password authentication or a public/private key system with a strong passphrase. A VPN is an example of a public/private key system.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules mentioned above that apply to passwords also apply to passphrases.

4.0 Enforcement

The Smeal College of Business Research Instructional and Information Technology Group (RIIT Group) has been authorized by the Dean of the Smeal College of Business to enforce this policy.

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the College, or the University.

5.0 Definitions

Terms	**Definitions**
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).
TACACS+	Terminal Access Controller Access Control System authentication protocol
RADIUS	Remote Authentication Dial In User Service authentication protocol
X.509	An authentication protocol using the key Exchange Algorithm (KEA)
LDAP	An Internet standard protocol for accessing directory information. LDAP stands for Lightweight Directory

	Access Protocol
VPN	Virtual Private Network - provides a secure tunnel for transmitting data through an unsecured network

6.0 Revision History

06/04/2007 - Initial modification from COE policies, used with permission in conjunction with the Penn State IPAS project. http://www.ipas.psu.edu/