Password Policy
COE–PWP–ADG02

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 College of Engineering's computer network. As such, all College of Engineering employees (including contractors, temporary personnel, and vendors with access to College of Engineering 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 standards 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 College of Engineering facility, has access to the College of Engineering network through local or remote connectivity, or stores any non-public College of Engineering information.

Note: All faculty, staff and students are bound by ITS policies regulating their Penn State Access Accounts 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, NT admin, application administration accounts, etc.) must be changed every 90 days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 120 days. 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, unless the email or other transmission method is securely encrypted.
- 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.
- General day-to-day User accounts must run least privilege and not have administrative rights. See policy COE_LUP_01 for details.

3.2 Guidelines
A. General Password Construction Guidelines
Passwords are used for various purposes at the College of Engineering. Some of the more common uses include: system administration, 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 be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:
- The password contains less than nine characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
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 nine 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 College of Engineering accounts as for other non College of Engineering access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various College of Engineering access needs. For example, select one password for the Engineering 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 College of Engineering passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential College of Engineering information.

Here is a list of "don'ts":

- 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
- Don't store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

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

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

Password integrity testing may be performed on a periodic or random basis by the University Security Office, NCTS 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.
• Should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the College of Engineering Networks via remote access is to be encrypted traffic, 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:

"4Sc0re&7YrsAgo!"
NOTE: Do not use this example as a password!

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

4.0 Enforcement
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

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Administration Account</td>
<td>Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Controller Access Control System authentication protocol</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial In User Service authentication protocol</td>
</tr>
<tr>
<td>X.509</td>
<td>An authentication protocol using the key Exchange Algorithm (KEA)</td>
</tr>
<tr>
<td>LDAP</td>
<td>An Internet standard protocol for accessing directory information. LDAP stands for Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network - provides a secure tunnel for transmitting data through an unsecured network</td>
</tr>
</tbody>
</table>

6.0 Revision Date
Last updated: 1/5/2016