College of Agricultural Sciences --- Password Policy: ITP-002

1.0 Purpose

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

2.0 Scope

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 Agricultural Sciences facility, has access to the College of Agricultural Sciences network through local or remote connectivity, or stores any non-public College of Agricultural Sciences information.

Note: All faculty, educators, 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 Background

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 Agricultural Sciences computer network. Further, passwords are one-half of a user's digital credentials. These credentials are in essence a digital fingerprint. Any actions taken under a properly authenticated account are presumed to be the actions of the individual assigned that account. As such, it is in the users best interest to ensure they and only they can properly authenticate their account by using a secure password and maintaining the privacy of that password. All College of Agricultural Sciences employees (including contractors, temporary employee, and vendors with access to College of Agricultural Sciences systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

4.0 Policy

4.1 General

1. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least annually. The recommended change interval is every six months.
2. All user-level passwords for individuals processing credit cards must be changed every 90 days.
3. 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.
4. Passwords must not be inserted into email messages or other forms of electronic communication.
5. 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).
6. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on a quarterly basis. System-level passwords should be changed immediately when an employee with access to these passwords no longer is responsible for said systems.
7. All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes in the College of Agricultural Sciences. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail, 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.

Strong passwords have the following characteristics:

1. Contain both upper and lower case characters
2. Have digits and punctuation characters as well as letters
3. Are at least eight alphanumeric characters long.
4. Are not a word in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.

Poor, weak passwords have the following characteristics:
1. The password contains less than eight characters
2. The password is a word found in a dictionary (English or foreign)
3. The password is a common usage word such as:
    a. Names of family, pets, friends, co-workers, fantasy characters, etc.
    b. The user's ID, or subset thereof.
    c. Computer terms and names, commands, sites, companies, hardware, software.
    d. The words "College of Agricultural Sciences", "CAS", "<Department Name>" or any derivation.
    e. Birthdays and other personal information such as addresses and phone numbers.
    f. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    g. Any of the above spelled backwards.
    h. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

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 to 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 Agricultural Sciences accounts as for other non College of Agricultural Sciences or Penn State access accounts (e.g., personal ISP account, option trading, benefits, etc.).
Do not share College of Agricultural Sciences passwords with *anyone*, including administrative assistants, secretaries or even family members – especially children. All passwords are to be treated as sensitive, Confidential College of Agricultural Sciences information.
Here is a list of **"don'ts"**:
1. Don't reveal a password to anyone
2. Don't reveal a password in an email message
3. Don't talk about a password in front of others
4. Don't hint at the format of a password (e.g., "my family name")
5. Don't reveal a password on questionnaires or security forms
6. Don't share a password with family members
7. Don't reveal a password to co-workers to use while you are away on vacation
8. Don't use the "Remember Password" feature of applications (e.g., Internet Explorer).
9. Don't write down passwords and store them anywhere in your office
10. Don't store passwords in a file on ANY computer system (including mobile devices such as Blackberrys, Treos, Palm Pilots or similar devices) without encryption.

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

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

Password cracking or guessing may be performed on a periodic or random basis by the University Security Office, AgIT 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

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

1. Support authentication of individual users, not groups.
2. Do not store passwords in clear text or in any easily reversible form.
3. Provide for role management, such that one user can take over the functions of another without having to know the other's password.
4. Support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

5.0 Enforcement

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

6.0 Supporting Documents

NA

7.0 Revision History

Last updated: 12/14/2009