Password Policy

Policy Number: PSU-NK-ITS-005
Date: December 4, 2012
Page Count: 5

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 New Kensington Campus Data Network. As such, all Penn State New Kensington employees (including contractors, temporary personnel, and vendors with access to any/all New Kensington campus technology systems) are responsible for taking the appropriate steps, as outlined below, to select and secure personal passwords. The purpose of this policy is to establish standards for the creation of strong passwords, the protection of those passwords, and the frequency of change.

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 or in any New Kensington campus facility, has access to the New Kensington Campus Data Network through local or remote connectivity, or stores any non-public campus 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/be-safe/password-policy/

Definitions:
Application Administration Account - Any account that is for the administration of an application (e.g., Server Root Access, Web Server administrator).

VPN – (Virtual Private Network) – A technology used to allow a user or network to connect in a secure and virtual manner via open or public communication channels. A VPN grants a remote user (e.g. working from home) secure access to local network services as if he/she were sitting in his/her office.

New Kensington Data Network – The technology infrastructure, hardware, and software installed at the campus which is used to facilitate the flow of digital information between (but not limited to) computers, printers, servers, mobile devices, the Internet, etc. This includes both the wired and wireless networks at Penn State New Kensington.

NK ITS Department – The department that oversees IT resources at Penn State New Kensington to include the System Administrator, IT Specialist and IT Director.
Security Operations and Services (SOS) - a group of individuals that are part of Penn State Information Technology Services (ITS) that is responsible for protecting the Penn State community from threats to our IT resources.

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

Policy:

General

- All passwords must be changed at least every twelve (12) months. The recommended change interval is every three 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.
- Passwords must be kept secure at all times and not shared with other individuals.
- 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.

Guidelines:

General Password Construction Guidelines

Passwords are used for various purposes at Penn State New Kensington. 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 be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- 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 "New Kensington campus," "NK," "<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:

- 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 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!

**Password Protection Standards**

Do not use the same password for Penn State New Kensington accounts as well as for other non-Penn State New Kensington access (e.g., personal ISP account, option trading, benefits, etc.). Select a separate password to be used for a Windows account and a UNIX account if applicable.

Do not share your password with anyone, including administrative assistants, NK ITS Department personnel, or Police Services. All passwords are to be treated as sensitive, confidential university information.

Here is a list of "do not’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 a supervisor
- 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 to the NK ITS Department personnel.
• Do not use the "Remember Password" feature of applications (e.g., Outlook, AOL Instant 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 Palm Pilots or similar devices) without 128-bit or higher encryption.

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

Password cracking or guessing may be performed periodically by Security Operations and Services (SOS) or NK ITS Department personnel. If a password is guessed or cracked during one of these scans, the user will be required to change their password.

Application Development Standards
Internal 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 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.

Use of Passwords and Passphrases for Remote Access Users
Access to the New Kensington Data Network via remote access, requires the encryption of all traffic. This can be established by 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.

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

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

**Cross Reference:**
Other policies that should also be referenced:

**University Polices**
AD20 - Computer and Network Security

**Campus Policies**
PSU-NK-ITS-000 – End User Computer Agreement
PSU-NK-ITS-004 – Acceptable Use and Security Policy

**Policy History:**
November 16, 2012 – Policy Ratified by Chancellor Kevin Snider