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 the University of Evansville's entire corporate network. As such, all University of Evansville employees (including contractors and vendors with access to University of Evansville systems) 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 Faculty, Staff, Administrators, or other personnel 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 University of Evansville facility, has access to the University of Evansville network, or stores any non-public University of Evansville information.

4.0 Policy

4.1 General

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at a minimum every twelve (12) months.
- Passwords must be a minimum of 8 characters in length and consist of a combination of at least 3 of the 4 following items:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Symbols.
- Passwords may not be reused for a period of 2 years.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.
- Users will be notified of impending password expiration starting 14 days prior to actual password expiration.

4.2 Guidelines

A. **General Password Construction Guidelines**
Passwords are used for various purposes at the University of Evansville. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and local router logins. Poor, weak passwords have the following characteristics:
   - The password contains less than seven 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.

- Computer terms and names, commands, sites, companies, hardware, software.
- 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 fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not words 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 University of Evansville accounts as for other non-University of Evansville access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various University of Evansville access needs.

Do not share your University of Evansville passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential University of Evansville 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 asks for your password, refer them to this document or have them call the Office of Technology Services.

Do not use the "Remember Password" feature of applications (e.g., IE, FireFox, 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 Palm Pilots or similar devices) without encryption.

Change passwords at least once every 12 months. If an account or password is suspected to have been compromised, report the incident to the Office of Technology Services and change all passwords immediately.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary actions as outlined in the university faculty, staff and administrator manuals.

Revision 1 – Feb. 11, 2010
Revision 2 – April 22, 2010-forced strong password policy
Revision 3 – April 26, 2010-cleaned up scope by including user groups
Revision 4 – August 19, 2010 – changed time frame to 12 months and length to 8 characters, changed enforcement to refer to employee manual