Password Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Thiel College's resources. All users, including College students, employees, contractors, vendors, guests, and others with access to Thiel College systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. 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. Scope

The scope of this policy includes all individuals or groups 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 Thiel College facility, has access to the Thiel College network, or stores any nonpublic Thiel College information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must meet or exceed the strong password standard articulated by the following **Password Construction Guidelines**.

Password Construction Guidelines:

Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example ,!$%^ *()_+|~-=\`{}[]:";'>?,/) chosen from a list provided by the Office of Information Services (OIS).
- Cannot contain your first name, last name, email, or user ID.
- Cannot be one of your last 5 passwords.

Poor, or weak, passwords have the following characteristics:

- Contain fewer than twelve characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, season, months, years, sports teams, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.

- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

Never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, other phrase, or a random collection of words that only you can remember.

4.1.2 Users must not use the same password for Thiel College accounts as for other personal accounts (for example, personal ISP account, bank account, merchant account, and so on).

4.1.3 User accounts that have system-level administrative privileges must have a unique password from all other accounts held by that user.

4.2 Password Change

4.2.1 All system-level passwords (for example, root, enable, admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least annually. The recommended change interval is every 90 days.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Thiel College information.

4.3.2 Passwords must not be inserted into email messages or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, "my family name").

4.3.6 Do not share Thiel College passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

4.3.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

5. Policy Compliance

5.1 Compliance Measurement

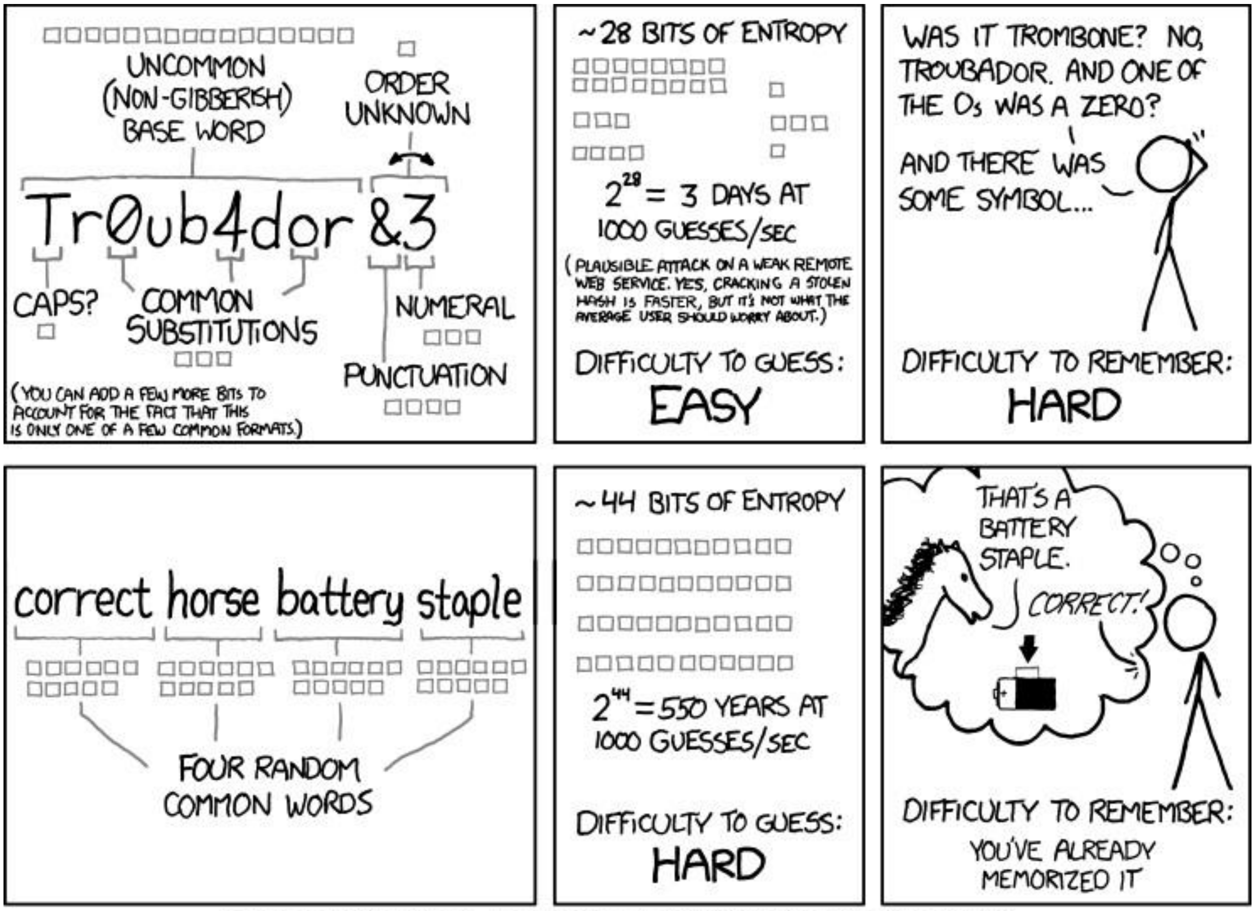
The Office of Information Services (OIS) will verify and promote compliance to this policy through various methods, including but not limited to, reports, internal and external audits, and feedback to individuals and campus departments.

5.2 Exceptions

The Directory of Information Systems must approve any exception to the policy in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.