Information Security Password Policy

Policy Title	**Information Security Password Policy** **Part of Information Security Policy Framework**
Responsible Party	Chief Security Officer ("CSO")
Endorsed by	Information Security Policy Committee
Contact	Chief Security Officer, Stuart Zimmerman; (918) 858-6684
Effective Date	June 1, 2015
Last Update	July 1, 2021

I. Policy Statement

TMA Systems Information Security Password Policy ("Password Policy") describes the Company's requirements for acceptable password selection and maintenance to maximize security of the password and minimize the passwords misuse or theft.

Passwords are the most frequently utilized form of authentication for accessing computing resources. Due to the use of weak passwords, the proliferation of automated password-cracking programs, and the activity of malicious hackers and spammers, they are often also the weakest link in security data. Password use for anyone accessing or utilizing the Company's network or data must therefore adhere to the policy set forth in this document.

II. Policy

Long passwords are strong passwords!

Your password can be:

- A *passphrase* (password phrase or sentence), or
- A complex combination of characters.

Passphrase: The easiest way to create a secure password is to use a passphrase, a password consisting of a sentence or phrase. Passphrases may be easier to remember and more secure than a shorter, more complex password. A passphrase must:

- Be between 15 and 127 characters in length, consisting of letters and spaces, AND
- Contain at least 1 number OR 1 symbol, such as (!"# $%&'()*+,-./:;<=>?@[]^_`{|}~).
- ***Passphrase tips:***
    - Consider a passphrase of several (5 or more) random words strung together, e.g. strainer walking trusty comic giraffe.
    - Make up a sentence that is relevant to you but is stated in such a way that it is not easily guessable, e.g., jazz is a passion, pizza too.
    - Remember that incorrect grammar and misspellings are passphrase strengtheners.
    - **DON'T** use quotations, popular song lyrics or well-known lines from books, movies, plays, TV shows, etc. exactly as published. Individuals attempting to crack your password will try them. You can base your passphrase on one of these, but vary the text in a unique way, e.g., "not all those who wander are lost" (J.R.R Tolkein) could be modernized to "not all those who wander lost their GPS" (we're sure you can do better).
    - **DON'T** use something that is public knowledge or has been shared on social media, such as Facebook or Twitter.
    - **DON'T** use any sample passphrases or passwords shared as tips.

Complex Password: If you choose to set a shorter but complex password (less than 15 characters in length), your password must contain ALL of the following:

- A minimum of 8 characters,
- 1 uppercase letter,
- 1 lowercase letter,
- 1 number, AND
- 1 symbol, such as (!"# $%&'()*+,-./:;<=>?@[]^_`{|}~)
- ***Complex password tips:***
    - Base your password on things relevant to you, but not easily discoverable.
    - Consider using incomplete words, uncommonly misspelled words or number or letter substitutions.
    - Create a unique password for your Company account(s).

- **DON'T** use the kinds of passwords that are easy hacking targets, such as:
  - Common dictionary words.
  - Sequential letters or numbers (e.g. 1234567890, abcdefghij, qwertyuiop).
  - Trivial passwords (e.g. password, passwd,mypassword,p@ssw0rd).
  - Easily discoverable personal data (e.g. names, birthday, address, pets).
  - Things that you've posted on social media sites (e.g. Facebook, Twitter).
- **DON'T** ever leave a password blank or keep its default value intact.
- **DON'T** use the same password to secure your Company account(s) as you use (or have used) for other sites, e.g., online shopping, Facebook.
- **DON'T** reuse passwords.

Be creative! The best passphrases and passwords are ones that have never been used before.

Finally, remember: No one shall ever ask you to disclose your password!

III. Procedure

There is no content for this section.

IV. Who is affected by this Policy

All Company employees and consultants are affected by this policy.

V. Definitions

There is no content for this section.

VI. Related Policies

- **Information Security Policy Framework**
- **Information Security Policy**
- **Information Security Plan**
- **Information Security Incident Management**
- **Information Technology Policy**
- **Network Administrative Security Policy**
- **Data Encryption Policy**
- **Monitoring and Logging Policy**
- **Business Continuity Policy**
- **Disaster Recovery Policy and Plan**

VII. Update Log

June 1, 2015: Policy issued.
