

Password, authentication and security Policy

First Medical Transcription Corporation offer's several Medical & healthcare related services through their web site named firstMT.com. In this document firstMT.com represent the website as well as First Medical Transcription Corporation.

Passwords and user authentications 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 firstMT.com's entire operational network. As such, all firstMT.com employees (including contractors and vendors with access to firstMT.com systems), clients, associates, affiliates, sub-contractors and all other concern parties are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong user authentication, passwords, the protection of those passwords, and the frequency of change.

The scope of this policy includes all 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 firstMT.com facility, has access to the firstMT.com network, or stores any non-public firstMT.com information.

General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the centrally administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six 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" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of non-secure electronic communication.
- 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

A. General Password Construction Guidelines

Passwords are used for various purposes at firstMT.com. Some of the more common uses include: user level accounts, web accounts, email accounts, FTP 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.
 - Computer terms and names, commands, sites, companies, hardware, software.

- o The words "firstMT.com", "firstMT", " First Medical Transcription Corporation " or any derivation.
- o Birthdays and other personal information such as addresses and phone numbers.
- o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- o Any of the above spelled backwards.
- o 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!

B. Password Protection Standards

Do not use the same password for firstMT.com accounts as for other non-firstMT.com access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various firstMT.com access needs. For example, select one password for the web based systems and a separate password for FTP systems. Also, select a separate password to be used for an incoming account and a outgoing account.

Do not share firstMT.com passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential firstMT.com 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 demands a password, refer them to this document or have them call firstMT.com's support line.

Do not use the "Remember Password" feature of applications (e.g., 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 six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

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

Password cracking or guessing may be performed on a periodic or random basis by firstMT.com or its delegates, in order to maintain security on individual account and eliminate vulnerabilities. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers for firstMT.com 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 some sort of 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.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the firstMT.com Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. 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:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

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

Enforcement

Any user, clients, affiliate, employee, consultant, sub-contractor and concern parties found to have violated this policy may be subject to disciplinary action, up to and including termination of services.

Revision History

*firstMT.com password policy.
First Medical Transcription Corporation
22 W 19th Street, 5th Floor
New York, NY 10011*

Last Updated: 2/17/2005 2:44:13 PM